Distr.: General 18 January 2019

English only

Economic Commission for Europe

Inland Transport Committee

Working Party on Road Transport

Group of Experts on European Agreement Concerning Work of Crews of Vehicles Engaged in International Road Transport (AETR)

Twentieth session

Geneva, 18 February 2019

Annex 1C

Submitted by European Commission

This document submitted by the European Commission contains the tables of equivalence between Annex IC in Regulation (EU) 2016/799 and the AETR. It comprises Annex IC and its Appendices 1 to 16.

LIST OF PROPOSED CHANGES TO ANNEX 1C FOR AETR V0.2 20190116

Point or article	Text Annex IC	Proposed text for AETR	Comments
TITLE/TABLE OF CONTENTS			To be updated as needed, according to the validated changes
General	Recording equipment	Is called control device in the AETR. Options: Recording equipment definition to be added in the introduction and replace control device with recording equipment. Both expressions to be	To be discussed
		defined as synonyms and use both of them as it corresponds. Continue to use recording equipment in Appendix 1C.	
INTRODUCTI	First generation digital tachograph system is deployed since 1 May 2006. It may be used until its end of life for domestic transportation. For international transportation instead, 15 years after the entry into force of this Commission Regulation, all vehicles shall be equipped with a compliant second generation smart tachograph, introduced by this Regulation. This Annex contains second generation recording equipment and tachograph cards requirements. Starting from its introduction date, second generation recording equipment shall be installed in webiless registered.	First generation digital tachograph system is deployed on the territory of the Contracting Parties since xx xx xxxx. It may be used until its end of life for domestic transportation. For international transportation instead, after June 15th 2034, all vehicles shall be equipped with a compliant second generation smart tachograph, introduced by this Agreement. First generation tachograph system complies with Appendix 1B to this Agreement, while second generation tachograph system complies with this Appendix. This Appendix contains second	Starting date of deployment of the first generation digital tachograph on the territory of the AETR Contracting Parties to be discussed.
	installed in vehicles registered for the first time, and second	generation recording equipment and tachograph cards requirements.	

	generation tachograph cards shall be issued. In order to foster a smooth introduction of the second generation tachograph system, - second generation tachograph cards shall be designed to be also used in first generation vehicle units, - replacement of valid first generation tachograph cards at the introduction date shall not be requested. This will allow drivers to keep their unique driver card and use both systems with it. Second generation recording equipment shall however only be calibrated using second generation workshop cards. This Annex contains all requirements related to the interoperability between the first and the second generation tachograph system. Appendix 15 contains additional details about how the co-existence of the two systems shall be managed.	Starting from its introduction date, second generation recording equipment shall be installed in vehicles registered for the first time, and second generation tachograph cards shall be issued. In order to foster a smooth introduction of the second generation tachograph system, - second generation tachograph system, - second generation tachograph cards shall be designed to be also used in first generation vehicle units, - replacement of valid first generation tachograph cards at the introduction date shall not be requested. This will allow drivers to keep their unique driver card and use both systems with it. Second generation recording equipment shall however only be calibrated using second generation workshop cards. This Appendix contains all requirements related to the interoperability between the first and the second generation tachograph system. Sub-appendix 15 contains additional details about how the co-existence of the two	
		additional details about how the co-existence of the two systems shall be managed.	
1	1 Definitions In this Annex: a) "activation" means:	1 Definitions In this Appendix: a) "activation" means:	
1, f)	f) "calibration" of a smart tachograph means updating or confirming vehicle parameters	f) "calibration" of a smart tachograph means updating or confirming vehicle parameters	

	to be held in the data	to be held in the data	
	memory. Vehicle parameters	memory. Vehicle parameters	
	include vehicle identification	include vehicle identification	
	(VIN, VRN and registering	(VIN, VRN and registering	
	Member State) and vehicle	Contracting Party) and vehicle	
	characteristics (w, k, l, tyre	characteristics (w, k, l, tyre	
	size, speed limiting device	size, speed limiting device	
	_		
	setting (if applicable), current	setting (if applicable), current	
	UTC time, current odometer	UTC time, current odometer	
	value); during the calibration	value); during the calibration	
	of a recording equipment, the	of a recording equipment, the	
	types and identifiers of all	types and identifiers of all	
	type approval relevant seals in	type approval relevant seals in	
	place shall also be stored in	place shall also be stored in	
	the data memory;	the data memory;	
	any update or confirmation of	any update or confirmation of	
	UTC time only, shall be	UTC time only, shall be	
	considered as a time	considered as a time	
	adjustment and not as a	adjustment and not as a	
	calibration, provided it does	calibration, provided it does	
	not contradict Requirement	not contradict Requirement	
	409;	409;	
	,		
	calibrating a recording	calibrating a recording	
	equipment requires the use of	equipment requires the use of	
	a workshop card;	a workshop card;	
1, g)	g) "card number" means:	(g) "card number" means:	
	a 16 alpha-numerical	a 16 alpha-numerical	
	characters number that	characters number that	
	uniquely identifies a	uniquely identifies a	
	tachograph card within a	tachograph card within a	
	Member State. The card	Contracting Party. The card	
	number includes a card	number includes a card	
	consecutive index (if	consecutive index (if	
	applicable), a card	applicable), a card	
	replacement index and a card	replacement index and a card	
	renewal index;	renewal index;	
	a card is therefore uniquely	a card is therefore uniquely	
	identified by the code of the	identified by the code of the	
	issuing Member State and the	issuing Contracting Party and	
4 1)	card number;	the card number;	
1, 1)	I) "company card" means: a tachograph card issued by	I) "company card" means:	
	the authorities of a Member	a tachograph card issued by the authorities of a Contracting	
		_	
	State to a transport undertaking needing to	Party to a transport undertaking needing to	
	THE THE THE TO	undertaking needing to	
	operate vehicles fitted with a	operate vehicles fitted with a	
	operate vehicles fitted with a tachograph, which identifies	operate vehicles fitted with a tachograph, which identifies	
	operate vehicles fitted with a tachograph, which identifies the transport undertaking and	operate vehicles fitted with a tachograph, which identifies the transport undertaking and	
	operate vehicles fitted with a tachograph, which identifies	operate vehicles fitted with a tachograph, which identifies	

the	data, stored in the	the data, stored in the	
	ograph, which have been	tachograph, which have been	
locke		locked by that transport	
	ertaking;	undertaking;	
	ontinuous driving time" is	n) "continuous driving time" is	The AETR defines splits in
·	puted within the	computed within the	driving periods of four and a
	rding equipment as1:	recording equipment as ³ :	half hours (in Article 7).
	continuous driving time is	the continuous driving time is	
·	puted as the current	computed as the current	
	mulated driving times of a	accumulated driving times of a	
parti	cular driver, since the end	particular driver, since the end	
of his	s last AVAILABILITY or	of his last AVAILABILITY or	
BREA	AK/REST or UNKNOWN ²	BREAK/REST or UNKNOWN ⁴	
perio	od of 45 minutes or more	period of 45 minutes or more	
(this	period may have been	(this period may have been	
split	according to Regulation	split according to this	
(EC)	N°. 561/2006). The	Agreement). The	
comp	putations involved take	computations involved take	
into	account, as needed, past	into account, as needed, past	
activ	ities stored on the driver	activities stored on the driver	
card.	. When the driver has not	card. When the driver has not	
inser	ted his card, the	inserted his card, the	
comp	putations involved are	computations involved are	
base	d on the data memory	based on the data memory	
recor	rdings related to the	recordings related to the	
curre	ent period where no card	current period where no card	
was i	inserted and related to	was inserted and related to the	
the r	elevant slot;	relevant slot;	
1, o) o) "c	ontrol card" means:	o) "control card" means:	
a tao	chograph card issued by	a tachograph card issued by	
the a	authorities of a Member	the authorities of a Contracting	
State	e to a national competent	Party to a national competent	
conti	·	control authority which	
ident	tifies the control body and,	identifies the control body and,	
	onally, the control officer,	optionally, the control officer,	
· ·	which allows access to the	and which allows access to the	
data	stored in the data	data stored in the data	
mem	nory or in the driver cards	memory or in the driver cards	

¹ This way of computing the continuous driving time and the cumulative break time serves into the Recording Equipment for computing the continuous driving time warning. It does not prejudge the legal interpretation to be made of these times. Alternative ways of computing the continuous driving time and the cumulative break time may be used to replace these definitions if they have been made obsolete by updates in other relevant legislation.

² UNKNOWN periods correspond to periods where the driver's card was not inserted in a recording equipment and for which no manual entry of driver activities was made.

³ This way of computing the continuous driving time and the cumulative break time serves into the Recording Equipment for computing the continuous driving time warning. It does not prejudge the legal interpretation to be made of these times. Alternative ways of computing the continuous driving time and the cumulative break time may be used to replace these definitions if they have been made obsolete by updates in other relevant legislation.

⁴ UNKNOWN periods correspond to periods where the driver's card was not inserted in a recording equipment and for which no manual entry of driver activities was made.

	and, optionally, in the	and, optionally, in the	
	workshop cards for reading,	workshop cards for reading,	
	printing and/or	printing and/or	
	downloading;	downloading;	
	It shall also give access to	It shall also give access to	
	the roadside calibration	the roadside calibration	
	checking function and to	checking function and to	
	data on the remote early	data on the remote early	
	detection communication	detection communication	
	reader.	reader.	
1, p)	p) "cumulative break	p) "cumulative break	The AETR defines splits in
- <i>/</i> - <i></i>	time" is computed within the	time" is computed within the	driving periods of four and a
	recording equipment as1:	recording equipment as1:	half hours (in Article 7).
	the cumulative break from	the cumulative break from	
	driving time is computed as the	driving time is computed as the	
	current accumulated	current accumulated	
	AVAILABILITY or BREAK/REST	AVAILABILITY or BREAK/REST	
	or UNKNOWN2 times of 15	or UNKNOWN2 times of 15	
	minutes or more of a particular	minutes or more of a particular	
	driver, since the end of his last	driver, since the end of his last	
	AVAILABILITY or BREAK/REST	AVAILABILITY or BREAK/REST	
	or UNKNOWN2 period of 45	or UNKNOWN2 period of 45	
	minutes or more (this period	minutes or more (this period	
	may have been split according	may have been split according	
	to Regulation (EC) N°.	to according to this	
	561/2006).	Agreement.	
		_	
	The computations involved	The computations involved	
	take into account, as needed,	take into account, as needed,	
	past activities stored on the	past activities stored on the	
	driver card. Unknown periods	driver card. Unknown periods	
	of negative duration (start of	of negative duration (start of	
	unknown period > end of	unknown period > end of	
	unknown period) due to time	unknown period) due to time	
	overlaps between two	overlaps between two	
	different recording	different recording	
	equipments, are not taken into	equipments, are not taken into	
	account for the computation.	account for the computation.	
	When the driver has not	When the driver has not	
	inserted his card, the	inserted his card, the	
	computations involved are	computations involved are	
	based on the data memory	based on the data memory	
	recordings related to the	recordings related to the	
	current period where no card	current period where no card	
	was inserted and related to the	was inserted and related to the	
	relevant slot	relevant slot	
1, s)	s) "downloading" means:	s) "downloading" means:	The AETR defines what rules
	the copying, together with	the copying, together with	must be complied with, instead
	the digital signature, of a	the digital signature, of a	of Regulation (EC) N°.
	part, or of a complete set,	part, or of a complete set,	561/2006).
	of data files recorded in the	of data files recorded in the	
	data memory of the vehicle	data memory of the vehicle	
	data memory of the venicle	data memory of the venicle	

	unit or in the memory of a	unit or in the memory of a	
	tachograph card, provided	tachograph card, provided	
	that this process does not	that this process does not	
	alter or delete any stored	alter or delete any stored	
	data;	data;	
	Manufacturers of smart	Manufacturers of smart	
	tachograph vehicle units	tachograph vehicle units	
	and manufacturers of	and manufacturers of	
	equipment designed and	equipment designed and	
	intended to download data	intended to download data	
	files shall take all	files shall take all	
	reasonable steps to ensure	reasonable steps to ensure	
	that the downloading of	that the downloading of	
	such data can be	such data can be	
	performed with the	performed with the	
	minimum delay by	minimum delay by	
	transport undertakings or	transport undertakings or	
	drivers.	drivers.	
	The downloading of the	The downloading of the	
	detailed speed file may not	detailed speed file may not	
	be necessary to establish	be necessary to establish	
	compliance with Regulation	compliance with this	
	(EC) N°. 561/2006, but may	Agreement but may be used	
	be used for other purposes	for other purposes such as	
	such as accident	accident investigation.	
	investigation.		
1, t)	t) "driver card" means:	t) "driver card" means:	
	a tachograph card, issued by	a tachograph card, issued by	
	the authorities of a Member	the authorities of a Contracting	
	State to a particular driver,	Party to a particular driver,	
	which identifies the driver and	which identifies the driver and	
	allows for the storage of driver	allows for the storage of driver	
	activity data;	activity data;	
1, u)	u) "effective circumference of	u) "effective circumference of	
	the wheels" means:	the wheels" means:	
	the average of the distances	the average of the distances	
	travelled by each of the wheels	travelled by each of the wheels	
	moving the vehicle (driving	moving the vehicle (driving	
	wheels) in the course of one complete rotation. The	wheels) in the course of one complete rotation. The	
	measurement of these	measurement of these	
	distances shall be made under	distances shall be made under	
	standard test conditions as	standard test conditions as	
	defined under requirement	defined under requirement	
	414 and is expressed in the	414 and is expressed in the	
	form "I = mm". Vehicle	form "I = mm". Vehicle	
	manufacturers may replace	manufacturers may replace	
	the measurement of these	the measurement of these	
	distances by a theoretical	distances by a theoretical	
	,	,	

	calculation which takes into account the distribution of the weight on the axles, vehicle unladen in normal running order ³ . The methods for such theoretical calculation are subject to approval by a competent Member State authority and can take place only before tachograph activation;	calculation which takes into account the distribution of the weight on the axles, vehicle unladen in normal running order, namely with coolant fluid, lubricants, fuel, tools, spare-wheel and driver. The methods for such theoretical calculation are subject to approval by a competent Contracting Party authority and can take place only before tachograph activation;	
1, u)	Regulation (EU) N°. 1230/2012 relating to the masses and dimensions of certain categories of motor vehicles and their trailers and amending Directive 2007/46/EC, as last amended.	Regulation (EU) N°. 1230/2012 relating to the masses and dimensions of certain categories of motor vehicles and their trailers and amending Directive 2007/46/EC, as last amended. uu) 'Mass of the unladen vehicle in running order' means (a) in the case of a motor vehicle: the mass of the vehicle, with its fuel tank(s) filled to at least 90 % of its or their capacity/ies, including the mass of the driver, of the fuel and liquids, fitted with the standard equipment in accordance with the manufacturer's specifications and, when they are fitted, the mass of the bodywork, the cabin, the coupling and the spare wheel(s) as well as the tools; (b) in the case of a trailer: the mass of the vehicle including the fuel and liquids, fitted with the standard equipment in accordance with the manufacturer's specifications, and, when they are fitted, the mass of the bodywork, additional	Replace the reference to the Regulation with the definition of mass in running order

		coupling(s), the spare wheel(s) and the tools;	
1, gg)	gg) "out of scope" means: when the use of the recording equipment is not required, according to the provisions of Regulation (EC) N°. 561/2006.	gg) "out of scope" means: when the use of the recording equipment is not required, according to the provisions of this Agreement.	The AETR defines what rules must be complied with, instead of Regulation (EC) N°. 561/2006).
1, uu)	uu) "tyre size" means: the designation of the dimensions of the tyres (external driving wheels) in accordance with Directive 92/23/EEC of 31 march 1992 as last amended;	uu) "tyre size" means: the designation of the dimensions of the tyres (external driving wheels) in accordance with ECE Regulation 54;	Same replacement as for Appendix 1B, as stipulated in Article 2, 2.1.2.
1, vv)	vv) "vehicle identification" means: numbers identifying the vehicle: Vehicle Registration Number (VRN) with indication of the registering Member State and Vehicle Identification Number (VIN) ⁶ ;	vv) "vehicle identification" means: numbers identifying the vehicle: Vehicle Registration Number (VRN) with indication of the registering Contracting Party and Vehicle Identification Number (VIN); vvv) 'Vehicle Identification Number' means a fixed combination of characters assigned to each vehicle by the manufacturer, which consists of two sections: the first, composed of not more than six characters (letters or figures), identifying the general characteristics of the vehicle, in particular the type and model; the second, composed of eight characters of which the first four may be letters or figures and the other four figures only, providing, in conjunction with the first section, clear identification of a particular vehicle.	Add VIN definition
1, vv)	Footnote 6 Directive 76/114/EEC, 18/12/1975; OJ No L 024,	Footnote 6 Directive 76/114/EEC, 18/12/1975; OJ No L 024,	Replaced with VIN definition in vv)
1, xx)	30/01/1976, p. 0001 - 0005. xx) "workshop card" means: a tachograph card issued by the authorities of a Member State to designated staff of a tachograph manufacturer, a	30/01/1976, p. 0001 0005. xx) "workshop card" means: a tachograph card issued by the authorities of a Contracting Party to designated staff of a tachograph manufacturer, a	

	fitter, a vehicle manufacturer or a workshop, approved by that Member State, which identifies the cardholder and allows for the testing, calibration and activation of tachographs, and/or downloading from them;	fitter, a vehicle manufacturer or a workshop, approved by that Contracting Party, which identifies the cardholder and allows for the testing, calibration and activation of tachographs, and/or downloading from them;	
1, yy)	yy) "adaptor" means: a device, providing a signal permanently representative of vehicle speed and/or distance travelled, other than the one used for the independent movement detection, and which is: - installed and used only in M1 and N1 type vehicles (as defined in Annex II to Directive 2007/46/EC of the European Parliament and of the Council (*), as last amended), - installed where it is not mechanically possible to install any other type of existing motion sensor which is otherwise compliant with the provisions of this Annex and its Appendixes 1 to 15, - installed between the vehicle unit and where the speed/distance impulses are generated by integrated sensors or alternative interfaces, - seen from a vehicle unit, the adaptor behaviour is the same as if a motion sensor, compliant with the provisions of this Annex and its Appendixes 1 to 16,	yy) "adaptor" means: a device, providing a signal permanently representative of vehicle speed and/or distance travelled, other than the one used for the independent movement detection, and which is: - installed and used only in M1 and N1 type vehicles (as defined in Consolidated Resolution on the Construction of Vehicles (R.E.3), Revision 6, ECE/TRANS/WP.29/ 78/Rev.6 of 11 July 2017), - installed where it is not mechanically possible to install any other type of existing motion sensor which is otherwise compliant with the provisions of this Appendix and its Sub- appendixes 1 to 15, - installed between the vehicle unit and where the speed/distance impulses are generated by integrated sensors or alternative interfaces, - seen from a vehicle unit, the adaptor behaviour is the same as if a motion sensor, compliant with the	

	T		
	was connected to the vehicle unit; use of such an adaptor in those vehicles described above shall allow for the installation and correct use of a vehicle unit compliant with all the requirements of this Annex, for those vehicles, the smart tachograph includes cables, an adaptor, and a vehicle unit;	provisions of this Appendix and its Sub- appendixes 1 to 16, was connected to the vehicle unit; use of such an adaptor in those vehicles described above shall allow for the installation and correct use of a vehicle unit compliant with all the requirements of this Appendix, for those vehicles, the smart tachograph includes cables, an adaptor, and a vehicle unit;	
1, aaa)	aaa) data privacy means: the overall technical measures taken to ensure the proper implementation of the principles laid down in Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as well as of those laid down in Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector;	aaa) reserved	Definition suppressed (not needed).
1, ccc)	ccc) introduction date: 36 months after the entry into force of the detailed provisions referred to in Article 11 of Regulation (EU) N°. 165/2014. This is the date after which vehicles registered for the first time: - shall be fitted with a tachograph connected to a positioning service based on a satellite navigation system,	ccc) introduction date: 36 months after the entry into force of the detailed provisions referred to in Article 11 of Regulation (EU) N°. 165/2014. This is the date after which vehicles registered for the first time: - shall be fitted with a tachograph connected to a positioning service based on a satellite navigation system,	

	- shall be able to	- shall be able to	
	communicate data	communicate data	
	for targeted roadside	for targeted roadside	
	checks to competent	checks to competent	
	control authorities	control authorities	
	while the vehicle is in	while the vehicle is in	
	motion,	motion,	
	 and may be equipped 	 and may be equipped 	
	with standardised	with standardised	
	interfaces allowing	interfaces allowing	
	the data recorded or	the data recorded or	
	produced by	produced by	
	tachographs to be	tachographs to be	
	used in operational	used in operational	
	mode, by an external	mode, by an external	
	device.	device.	
2.1	Any vehicle fitted with the	Any vehicle fitted with the	
	recording equipment	recording equipment	
	complying with the provisions	complying with the provisions	
	of this Annex, must include a	of this Appendix, must include	
	speed display and an	a speed display and an	
	odometer. These functions	odometer. These functions	
	may be included within the	may be included within the	
	recording equipment.	recording equipment.	
2.1, 2)	02) The interface between	02) The interface between	
	motion sensors and vehicle	motion sensors and vehicle	
	units shall comply with the	units shall comply with the	
	requirements specified in	requirements specified in Sub-	
	Appendix 11.	appendix 11.	
2.1, 3)	03) The vehicle unit shall be	03) The vehicle unit shall be	
	connected to global navigation	connected to global navigation	
	satellite system(s), as specified	satellite system(s), as specified	
	in Appendix 12.	in Sub-appendix 12.	
2.1, 4)	04) The vehicle unit shall	04) The vehicle unit shall	
	communicate with remote	communicate with remote	
	early detection	early detection	
	communication readers, as	communication readers, as	
0.4.5)	specified in Appendix 14.	specified in Sub-appendix 14.	
2.1, 5)	05) The vehicle unit may	05) The vehicle unit may	
	include an ITS interface, which	include an ITS interface, which	
	is specified in Appendix 13	is specified in Sub-appendix 13.	
	The recording equipment may	The recording equipment may	
	be connected to other	be connected to other	
	facilities through additional	facilities through additional	
	interfaces and/or through the	interfaces and/or through the	
2.1.6\	optional ITS interface.	optional ITS interface.	
2.1, 6)	06) Any inclusion in or	06) Any inclusion in or	
	connection to the recording	connection to the recording	
	equipment of any function,	equipment of any function,	
	device, or devices, approved or otherwise, shall not	device, or devices, approved or otherwise, shall not	
	interfere with, or be capable	interfere with, or be capable	
	interiere with, or be capable	interiere with, or be capable	

	6: 1 6 : 21 11	6: 1 6 : 201 11	
	of interfering with, the proper	of interfering with, the proper	
	and secure operation of the	and secure operation of the	
	recording equipment and the	recording equipment and the	
	provisions of this Regulation.	provisions of this Agreement.	
2.1, 7)	07) The recording	07) The recording	
	equipment provides selective	equipment provides selective	
	access rights to data and	access rights to data and	
	functions according to user's	functions according to user's	
	type and/or identity.	type and/or identity.	
	The recording equipment	The recording equipment	
	records and stores data in its	records and stores data in its	
	data memory, in the remote	data memory, in the remote	
	communication facility and in	communication facility and in	
	tachograph cards.	tachograph cards.	
	This is done in accordance	This is done in accordance	
	with Directive 95/46/EC of 24	with Directive 95/46/EC of 24	
	October 1995 on the	October 1995 on the	
	protection of individuals with	protection of individuals with	
		regard to the processing of	
	regard to the processing of personal data and on the free	personal data and on the free	
		·	
	movement of such data, with	movement of such data, with	
	Directive 2002/58/EC of 12	Directive 2002/58/EC of 12	
	July 2002 concerning the	July 2002 concerning the processing of personal data	
	processing of personal data		
	and the protection of privacy	and the protection of privacy in the electronic	
	in the electronic		
	communications sector and in	communications sector and in	
	compliance with Article 7 of	compliance with Article 7 of	
0.4.44)	Regulation (EU) N°. 165/2014.	Regulation (EU) N°. 165/2014.	
2.4, 14)	14) In order to achieve the	14) In order to achieve the	
	system security, the following	system security, the following	
	components shall meet the	components shall meet the	
	security requirements	security requirements	
	specified in their Protection	specified in their Protection	
	Profiles, as required in	Profiles, as required in Sub-	
	Appendix 10:	appendix 10:	
	- vehicle unit,	- vehicle unit,	
	- tachograph card,	- tachograph card,	
	- motion sensor,	- motion sensor,	
	- external GNSS facility (this	- external GNSS facility (this	
	Profile is only needed and	Profile is only needed and	
	applicable for the external	applicable for the external	
	GNSS variant).	GNSS variant).	
3.1, 17)	17) First generation	17) First generation	
	tachograph cards shall be	tachograph cards shall be	
	considered as non-valid by the	considered as non-valid by the	
	recording equipment, after	recording equipment, after	
	the possibility of using first	the possibility of using first	
	generation tachograph cards	generation tachograph cards	
	has been suppressed by a	has been suppressed by a	

	and the later of the second because of the		
	workshop, in compliance with	workshop, in compliance with	
	Appendix 15 (req. MIG003).	Sub-appendix 15 (req.	
		MIG003).	
3.2, 25)	25) Devices displaying speed	25) Devices displaying speed	
	(speedometer) and total	(speedometer) and total	
	distance travelled (odometer)	distance travelled (odometer)	
	installed in any vehicle fitted	installed in any vehicle fitted	
	with a recording equipment	with a recording equipment	
	complying with the provisions	complying with the provisions	
	of this Regulation, shall	of this Agreement, shall	
	comply with the requirements	comply with the requirements	
	relating to maximum	relating to maximum	
	tolerances (see 3.2.1 and	tolerances (see 3.2.1 and	
	3.2.2) laid down in this Annex.	3.2.2) laid down in this	
		Appendix.	
3.3, 39)	39) UTC date and time shall be	39) UTC date and time shall be	
	used for dating data inside the	used for dating data inside the	
	recording equipment	recording equipment	
	(recordings, data exchange)	(recordings, data exchange)	
	and for all printouts specified	and for all printouts specified	
	in Appendix 4 "Printouts".	in Sub-appendix 4 "Printouts".	
3.6.3, 62	62) (last paragraph)	62) (last paragraph)	The AETR defines what rules
	An opened FERRY/TRAIN	An opened FERRY/TRAIN	must be complied with, instead
	CROSSING shall end when it is	CROSSING shall end when it is	of Regulation (EC) N°.
	no longer valid based on the	no longer valid based on the	561/2006).
	rules stated in Regulation (EC)	rules stated in this Agreement.	
	N°. 561/2006.	561/2006.	
3.9.13, 84)	3.9.13 "Vehicle motion	3.9.13 "Vehicle motion	
	conflict" event	conflict" event	
	84) This event shall be	84) This event shall be	
	triggered, while not in	triggered, while not in	
	calibration mode, in case	calibration mode, in case	
	motion information calculated	motion information calculated	
	from the motion sensor is	from the motion sensor is	
	contradicted by motion	contradicted by motion	
	information calculated from	information calculated from	
	the internal GNSS receiver or	the internal GNSS receiver or	
	from the external GNSS facility	from the external GNSS facility	
	and optionally by other	and optionally by other	
	independent sources, as specified in Appendix 12. This	independent sources, as specified in Sub-appendix 12.	
	event shall not be triggered	This event shall not be	
	during a ferry/train crossing,	triggered during a ferry/train	
	an OUT OF SCOPE condition,	crossing, an OUT OF SCOPE	
	or when the position	condition, or when the	
	information from the GNSS	position information from the	
	receiver is not available.	GNSS receiver is not available.	
3.9.14, 85)	3.9.14 "Security breach	3.9.14 "Security breach	
= 1, 30,	attempt" event	attempt" event	
	85) This event shall be	85) This event shall be	
	triggered for any other event	triggered for any other event	
	affecting the security of the	affecting the security of the	
L			

	motion sensor and/or of the	motion sensor and/or of the	
	vehicle unit and/or the	vehicle unit and/or the	
	external GNSS facility as	external GNSS facility as	
	required in Appendix 10, while	required in Sub-appendix 10,	
	not in calibration mode.	while not in calibration mode.	
3.12.3 102)	102) For each insertion and	102) For each insertion and	
	withdrawal cycle of a driver or	withdrawal cycle of a driver or	
	workshop card in the	workshop card in the	
	equipment, the recording	equipment, the recording	
	equipment shall record and	equipment shall record and	
	store in its data memory:	store in its data memory:	
	- the card holder's surname	- the card holder's surname	
	and first name(s) as stored in	and first name(s) as stored in	
	the card,	the card,	
	- the card's number, issuing	- the card's number, issuing	
	Member State and expiry date	Contracting Party and expiry	
	as stored in the card,	date as stored in the card,	
	- the card generation,	- the card generation,	
	- the insertion date and time,	- the insertion date and time,	
	- the vehicle odometer value	- the vehicle odometer value	
	at card insertion,	at card insertion,	
	- the slot in which the card is	- the slot in which the card is	
	inserted,	inserted,	
	- the withdrawal date and	- the withdrawal date and	
	time,	time,	
	- the vehicle odometer value	- the vehicle odometer value	
	at card withdrawal,	at card withdrawal,	
	- the following information	- the following information	
	about the previous vehicle	about the previous vehicle	
	used by the driver, as stored in	used by the driver, as stored in	
	the card:	the card:	
	- VRN and registering	 VRN and registering 	
	Member State,	Contracting Party,	
	- VU generation (when	 VU generation (when 	
	available),	available),	
	- card withdrawal date and	- card withdrawal date and	
	time,	time,	
	- a flag indicating whether,	- a flag indicating whether,	
	at card insertion, the card	at card insertion, the card	
	holder has manually entered	holder has manually entered	
	activities or not.	activities or not.	
3.12, 91)	91) Data stored into the	91) Data stored into the	
,,	data memory shall not be	data memory shall not be	
	affected by an external power	affected by an external power	
	supply cut-off of less than	supply cut-off of less than	
	twelve months in type	twelve months in type	
	approval conditions. In	approval conditions. In	
	addition, data stored in the	addition, data stored in the	
	external remote	external remote	
	communication facility, as	communication facility, as	
		_	
	defined in Appendix 14, shall	defined in Sub-appendix 14,	
	not be affected by power-	shall not be affected by	

	supply cut-off of less than 28	power-supply cut-off of less	
	days.	than 28 days.	
3.12.2, 101)	101) The recording equipment shall be able to store a number of cryptographic keys and	101) The recording equipment shall be able to store a number of cryptographic keys and	
	certificates, as specified in	certificates, as specified in	
	Appendix 11 part A and part B.	Sub-appendix 11 part A and	
	pp - pp	part B.	
3.12.5 110)	110) Together with each place or position, the recording equipment shall record and store in its data memory: - the (co-)driver card number and card issuing Member State, - the card generation, - the date and time of the entry, - the type of entry (begin, end or 3 hours accumulated	110) Together with each place or position, the recording equipment shall record and store in its data memory: - the (co-)driver card number and card issuing Contracting Party, - the card generation, - the date and time of the entry, - the type of entry (begin, end or 3 hours accumulated	
	driving time),	driving time),	
	 the related GNSS 	 the related GNSS 	
	accuracy, date and	accuracy, date and	
	time if applicable;	time if applicable;	
	- the vehicle odometer	- the vehicle odometer	
3.12.8 117)	value. See Annex 1	value. See Annex 1	
3.12.9 118)	See Annex 2	See Annex 2	
3.12.10 120)	120) The following data shall	120) The following data shall	
3.12.10 120)	be recorded for each of these calibrations:	be recorded for each of these calibrations:	
	 purpose of calibration (activation, first installation, periodic inspection), workshop name and address, workshop card number, card issuing Member State and card expiry date, vehicle identification, parameters updated or confirmed: w, k, l, tyre size, speed limiting device setting, odometer 	 purpose of calibration (activation, first installation, installation, periodic inspection), workshop name and address, workshop card number, card issuing Contracting Party and card expiry date, vehicle identification, parameters updated or confirmed: w, k, l, tyre size, speed limiting device setting, odometer 	

3.12.11 125)	(old and new values), date and time (old and new values), the types and identifiers of all the seals in place. 125) The following data shall	(old and new values), date and time (old and new values), the types and identifiers of all the seals in place. 125) The following data shall	
	be recorded for each of these time adjustments: - date and time, old value, - date and time, new value, - workshop name and address, - workshop card number, card issuing Member State, card generation and card	be recorded for each of these time adjustments: - date and time, old value, - date and time, new value, - workshop name and address, workshop card number, card issuing Contracting Party, card generation and card expiry date.	
3.12.12 126)	expiry date. 126) The recording equipment shall record and store in its data memory the following data relevant to the 20 most recent control activities: - date and time of the control, - control card number, card issuing Member State and card generation, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading and/or roadside calibration checking).	126) The recording equipment shall record and store in its data memory the following data relevant to the 20 most recent control activities: - date and time of the control, - control card number, card issuing Contracting Party and card generation, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading and/or roadside calibration checking).	
3.12.13 128)	128) The recording equipment shall record and store in its data memory the following data relevant to the 255 most recent company locks: - lock-in date and time, - lock-out date and time, - company card number, card issuing Member State and card generation,	128) The recording equipment shall record and store in its data memory the following data relevant to the 255 most recent company locks: - lock-in date and time, - lock-out date and time, - company card number, card issuing Contracting Party and card generation,	

	 company name and 	 company name and 	
	address.	address.	
	Data previously locked by a	Data previously locked by a	
	lock removed from memory	lock removed from memory	
	due to the limit above, shall	due to the limit above, shall	
	be treated as not locked.	be treated as not locked.	
3.12.14 129)	129) The recording equipment	129) The recording equipment	
	shall record and store in its	shall record and store in its	
	data memory the following	data memory the following	
	data relevant to the last data	data relevant to the last data	
	memory downloading to	memory downloading to	
	external media while in	external media while in	
	company or in calibration	company or in calibration	
	mode:	mode:	
	 date and time of 	 date and time of 	
	downloading,	downloading,	
	– company or	companyor	
	workshop card	workshop card	
	number, card issuing	number, card issuing	
	Member State and	Contracting Party and	
	card generation,	card generation,	
	companyor	- company or	
	workshop name.	workshop name.	
3.14.2, 144)	Second generation tachograph	Second generation tachograph	
	cards shall contain 2 different	cards shall contain 2 different	
	card applications, the first of	card applications, the first of	
	which shall be exactly the	which shall be exactly the	
	same as the TACHO	same as the TACHO	
	application of first generation	application of first generation	
	tachograph cards, and the	tachograph cards, and the	
	second the "TACHO_G2"	second the "TACHO_G2"	
	application, as specified in	application, as specified in	
	Chapter 4 and Appendix 2.	Chapter 4 and Sub-appendix 2.	
3.15, 153)	153) The display shall	153) The display shall	
	support the characters	support the characters	
	specified in Appendix 1	specified in Sub-appendix 1	
	Chapter 4 'Character sets'. The	Chapter 4 'Character sets'. The	
	display may use simplified	display may use simplified	
	glyphs (e.g. accented	glyphs (e.g. accented	
	characters may be displayed	characters may be displayed	
	without accent, or lower case	without accent, or lower case	
	letters may be shown as upper	letters may be shown as upper	
2.45.457\	case letters).	case letters).	
3.15, 157)	157) The display of the recording equipment shall use	157) The display of the	
		recording equipment shall use the pictograms or pictograms	
	the pictograms or pictograms combinations listed in		
		combinations listed in Sub-	
	Appendix 3. Additional	appendix 3. Additional	
	pictograms or pictograms combinations may also be	pictograms or pictograms combinations may also be	
	provided by the display, if	provided by the display, if	
	clearly distinguishable from	clearly distinguishable from	

	the aforementioned	the aforementioned	
	pictograms or pictograms	pictograms or pictograms	
	combinations.	combinations.	
3.15, 159)	159 (last line)	159 (last line)	
3.13, 139)	Displaying format is specified	Displaying format is specified	
	in Appendix 5.	in Sub-appendix 5.	
3.15.2, 165)	165) The recording	165) The recording	
3.13.2, 103)	equipment shall display	equipment shall display	
	warning information using	warning information using	
	primarily the pictograms of	primarily the pictograms of	
	Appendix 3, completed where	Sub-appendix 3, completed	
	needed by additional	where needed by additional	
	numerically coded	numerically coded	
	information. A literal	information. A literal	
	description of the warning	description of the warning	
	may also be added in the	may also be added in the	
	driver's preferred language	driver's preferred language	
3.16, 169)	169) (2 nd paragraph)	169) (2 nd paragraph)	
3.23, 233,	The detailed format and	The detailed format and	
	content of these printouts are	content of these printouts are	
	specified in Appendix 4.	specified in Sub-appendix 4.	
3.16, 174)	174) The printer shall	174) The printer shall	
3123, 27 .,	support the characters	support the characters	
	specified in Appendix 1	specified in Sub-appendix 1	
	Chapter 4 'Character sets'.	Chapter 4 'Character sets'.	
3.16, 179)	179) Printouts shall conform	179) Printouts shall conform	
,	at least to the test	at least to the test	
	specifications defined in	specifications defined in Sub-	
	Appendix 9.	appendix 9.	
3.18, 195)	195) The	195) The	
	calibration/downloading	calibration/downloading	
	connector electrical interface	connector electrical interface	
	is specified in Appendix 6.	is specified in Sub-appendix 6.	
3.18, 196)	196) Downloading protocols	196) Downloading protocols	
	are specified in Appendix 7.	are specified in Sub-appendix	
		7.	
3.19, 197)	197) When the ignition is on,	197) When the ignition is on,	
	the Vehicle Unit shall store	the Vehicle Unit shall store	
	every 60 seconds in the	every 60 seconds in the	
	remote communication facility	remote communication facility	
	the most recent data	the most recent data	
	necessary for the purpose of	necessary for the purpose of	
	targeted roadside checks.	targeted roadside checks.	
	Such data shall be encrypted	Such data shall be encrypted	
	and signed as specified in	and signed as specified in Sub-	
	Appendix 11 and Appendix 14.	appendix 11 and Sub-appendix	
2.40.400	100)	14.	
3.19, 198)	198) Data to be checked	198) Data to be checked	
	remotely shall be available to	remotely shall be available to	
	remote communication	remote communication	
	readers through wireless	readers through wireless	

	communication, as specified in	communication, as specified in	
	Appendix 14.	Sub-appendix 14.	
3.20, 200)	200) The recording equipment may also be equipped with standardised interfaces allowing the data recorded or produced by tachograph to be used in operational or calibration mode, by an external facility.	200) The recording equipment may also be equipped with standardised interfaces allowing the data recorded or produced by tachograph to be used in operational or calibration mode, by an external facility.	Change reference to Regulation (EU) 2016/679 ("General Data Protection Regulation") as appropriate.
	In Appendix 13, an optional ITS interface is specified and standardized. Other vehicle unit interfaces may co-exist, provided they fully comply with the requirements of Appendix 13 in term of minimum list of data, security and driver consent. The driver consent doesn't	In Sub-appendix 13, an optional ITS interface is specified and standardized. Other vehicle unit interfaces may co-exist, provided they fully comply with the requirements of Sub-appendix 13 in term of minimum list of data, security and driver consent.	
	apply to data transmitted by the recording equipment to the vehicle network. In case the personal data injected in the vehicle network are further processed outside the vehicle network, it is the responsibility of the vehicle manufacturer to have that personal data process compliant with Regulation (EU) 2016/679 ("General Data Protection Regulation").	The driver consent doesn't apply to data transmitted by the recording equipment to the vehicle network. In case the personal data injected in the vehicle network are further processed outside the vehicle network, it is the responsibility of the vehicle manufacturer to have that personal data process complying with the legislation on personal data protection applicable in the territory of the Contracting Parties and	
	The driver consent doesn't apply either to tachograph data downloaded to a remote company (requirement 193), as this scenario is monitored by the company card access right. The following requirements apply to ITS data made available through that interface:	with the Convention for the protection of individuals with regard to automatic processing of personal data. The driver consent doesn't apply either to tachograph data downloaded to a remote company (requirement 193), as this scenario is monitored by the company card access right. The following requirements apply to ITS data made	

- these data are a set of selected existing data from the tachograph data dictionary (Appendix 1),
- a subset of these selected data are marked 'personal data',
- the subset of 'personal data' is only available if the verifiable consent of the driver, accepting his personal data can leave the vehicle network, is enabled,
- At any moment, the driver consent can be enabled or disabled through commands in the menu, provided the driver card is inserted,
- the set and subset of data will be broadcasted via Bluetooth wireless protocol in the radius of the vehicle cab, with a refresh rate of 1 minute,
- the pairing of the external device with the ITS interface will be protected by a dedicated and random PIN of at least 4 digits, recorded in and available through the display of each vehicle unit,
- in any circumstances, the presence of the ITS interface cannot disturb or affect the correct functioning and the security of the vehicle unit.

available through that interface:

- these data are a set of selected existing data from the tachograph data dictionary (Subappendix 1),
- a subset of these selected data are marked 'personal data',
- the subset of 'personal data' is only available if the verifiable consent of the driver, accepting his personal data can leave the vehicle network, is enabled,
- At any moment, the driver consent can be enabled or disabled through commands in the menu, provided the driver card is inserted,
- the set and subset of data will be broadcasted via Bluetooth wireless protocol in the radius of the vehicle cab, with a refresh rate of 1 minute,
- the pairing of the external device with the ITS interface will be protected by a dedicated and random PIN of at least 4 digits, recorded in and available through the display of each vehicle unit,
- in any circumstances, the presence of the ITS interface cannot disturb or affect the correct functioning and the security of the vehicle unit.

	Other data many data to the control		
	Other data may also be output in addition to the set of		
	selected existing data,	Other data may also be subject	
	considered as the minimum	Other data may also be output in addition to the set of	
	list, provided they cannot be	selected existing data,	
	considered as personal data.	considered as the minimum	
	considered as personal data.	list, provided they cannot be	
	The recording equipment shall	considered as personal data.	
	have the capacity to	considered as personal data.	
	communicate the driver	The recording equipment shall	
	consent status to other	have the capacity to	
	platforms in the vehicle	communicate the driver	
	network.	consent status to other	
		platforms in the vehicle	
	When the ignition of the	network.	
	vehicle is ON, these data shall		
	be permanently broadcasted.	When the ignition of the	
	, , , , , , , , , , , , , , , , , , , ,	vehicle is ON, these data shall	
		be permanently broadcasted.	
3.20, 201)	The serial link interface as	The serial link interface as	
	specified in Annex 1B to	specified in Appendix 1B of	
	Regulation (EEC) N°. 3821/85,	this Agreement can continue	
	as last amended, can continue	to equip tachographs for back	
	to equip tachographs for back	compatibility. Anyhow, the	
	compatibility. Anyhow, the	driver consent is still required	
	driver consent is still required	in case personal data are	
	in case personal data are	transmitted.	
	transmitted.		
3.21, 203)	203) In addition, the	203) In addition, the	
	calibration function shall allow	calibration function shall allow	
	to supress the use of first	to supress the use of first	
	generation tachograph cards	generation tachograph cards	
	in the recording equipment, provided the conditions	in the recording equipment, provided the conditions	
	specified in Appendix 15 are	specified in Sub-appendix 15	
	met.	are met.	
3.21, 206)	206) The calibration function	206) The calibration function	
0.21, 200)	shall be able to input	shall be able to input	
	necessary data through the	necessary data through the	
	calibration/downloading	calibration/downloading	
	connector in accordance with	connector in accordance with	
the state of the s	the calibration protocol	the calibration protocol	
	the calibration protocol	the calibration protocol	
	the calibration protocol defined in Appendix 8. The	the calibration protocol defined in Sub-appendix 8.	
	the calibration protocol defined in Appendix 8. The calibration function may also	the calibration protocol defined in Sub-appendix 8. The calibration function may	
3.22, 209)	the calibration protocol defined in Appendix 8. The calibration function may also input necessary data through other means. 209) The roadside	the calibration protocol defined in Sub-appendix 8. The calibration function may also input necessary data through other means. 209) The roadside	
3.22, 209)	the calibration protocol defined in Appendix 8. The calibration function may also input necessary data through other means. 209) The roadside calibration checking function	the calibration protocol defined in Sub-appendix 8. The calibration function may also input necessary data through other means. 209) The roadside calibration checking function	
3.22, 209)	the calibration protocol defined in Appendix 8. The calibration function may also input necessary data through other means. 209) The roadside calibration checking function shall also allow controlling the	the calibration protocol defined in Sub-appendix 8. The calibration function may also input necessary data through other means. 209) The roadside calibration checking function shall also allow controlling the	
3.22, 209)	the calibration protocol defined in Appendix 8. The calibration function may also input necessary data through other means. 209) The roadside calibration checking function shall also allow controlling the selection of the I/O mode of	the calibration protocol defined in Sub-appendix 8. The calibration function may also input necessary data through other means. 209) The roadside calibration checking function shall also allow controlling the selection of the I/O mode of	
3.22, 209)	the calibration protocol defined in Appendix 8. The calibration function may also input necessary data through other means. 209) The roadside calibration checking function shall also allow controlling the	the calibration protocol defined in Sub-appendix 8. The calibration function may also input necessary data through other means. 209) The roadside calibration checking function shall also allow controlling the	

4.1, 227)	the K-line interface. This shall be done through the ECUAdjustmentSession, as specified in Appendix 8, section 7 Control of Test Pulses – Input output control functional unit. 227) the words "Driver card" or "Control card" or "Control card" or "Company card" printed in capital letters in the official language or languages of the Member State issuing the card, according to the type of	via the K-line interface. This shall be done through the ECUAdjustmentSession, as specified in Sub-appendix 8, section 7 Control of Test Pulses – Input output control functional unit. 227) the words "Driver card" or "Control card" or "Control card" or "Company card" printed in capital letters in the official language or languages of the Contracting Party issuing the card, according to the type of	
4.1, 228)	the card. 228) the name of the Member State issuing the card	the card. 228) the name of the Contracting Party issuing the	
4.1, 229)	(optional); 229) the distinguishing sign of the Member State issuing the card, printed in negative in a blue rectangle and encircled by 12 yellow stars. The distinguishing signs shall be as follows:	card (optional); 229) For EU Member States, the distinguishing sign of the Member State issuing the card, printed in negative in a blue rectangle and encircled by 12 yellow stars. The distinguishing signs shall be as follows: (see table in Annex 3) For non-EU Contracting Parties, the distinguishing sign of the Contracting Party issuing the card. The distinguishing signs of non EU Contracting Parties are those drawn in accordance with the 1968 Vienna Convention on Road Traffic or the 1949 Geneva Convention on Road Traffic.	
4.1, 235)	Community Model Tachograph Cards	NON-EU CONTRACTING PARTIES MODEL TACHOGRAPH CARDS -	Specific models for non-EU contracting Parties should be displayed
4.1, 236)	236) After consulting the Commission, Member States may add colours or markings, such as national symbols and security features, without prejudice to the other provisions of this Annex.	After consulting the UN/ECE secretariat, non-EU Contracting Parties may add colours or markings, such as national symbols and security features, without prejudice to the other provisions of this Appendix.	

4.1, 237)	237) Temporary cards referred to in Article 26.4 of Regulation (EU) N°. 165/2014 shall comply with the provisions of this Annex.	237) Reserved	This disposition doesn't apply fir the AETR.
4.2, 238)	238) In order to achieve the system security, the tachograph cards shall meet the security requirements defined in Appendixes 10 and 11.	238) In order to achieve the system security, the tachograph cards shall meet the security requirements defined in Sub-appendixes 10 and 11.	
4.4, 241)	241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in Community territory and at least in the temperature range -25°C to +70°C with occasional peaks of up to +85°C, "occasional" meaning not more than 4 hours each time and not over 100 times during the life time of the card.	241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in the territory of the Contracting Parties and at least in the temperature range – 25 °C to + 70 °C with occasional peaks of up to + 85 °C, 'occasional' meaning not more than 4 hours each time and not over 100 times during the life time of the card.'	
4.5	4.5 (2 nd paragraph) The tachograph cards functions, commands and logical structures, fulfilling data storage requirements are specified in Appendix 2.	4.5 (2 nd paragraph) The tachograph cards functions, commands and logical structures, fulfilling data storage requirements are specified in Sub-appendix 2.	
4.5, 246)	246) Any additional data that may be stored on tachograph cards, related to other applications possibly borne by the card, shall be stored in accordance with Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and with Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and in compliance with Article 7 of Regulation (EU) N°. 165/2014.	246) Any additional data that may be stored on tachograph cards, related to other applications possibly borne by the card, shall be stored in accordance with the legislation on personal data protection applicable in the territory of Contracting Parties and with the Convention for the protection of individuals with regard to automatic processing of personal data.	
4.5, 247)	247) (last line)	247) (last line)	

The full details of the tachograph cards structure are specified in Appendix 2. The full details of the tachograph cards structure are specified in Sub-appendix 2.
specified in Appendix 2. specified in Sub-appendix 2.
4.5.0.0.050) 7.1. 1.1.1.050) 7.1. 1.1.1.1.
4.5.2.2, 250) Zefol Tachograph cards shall 250) Tachograph cards shall
be able to store the be able to store the
application identification data application identification data
objects specified in Appendix objects specified in Sub-
2. appendix 2.
4.5.2.3, 251) 251) Tachograph cards shall 251) Tachograph cards shall
be able to store the following be able to store the following
extended length information extended length information
data object: data object:
- in the case the tachograph - in the case the tachograph
card supports extended length card supports extended length
fields, the extended length fields, the extended length
information data object information data object
specified in Appendix 2. specified in Sub-appendix 2.
4.5.2.4, 252) 252) Tachograph cards shall 252) Tachograph cards shall
be able to store the following be able to store the following
extended length information extended length information
data objects: data objects:
- in the case the tachograph - in the case the tachograph
card supports extended length card supports extended length
fields, the extended length fields, the extended length
information data objects information data objects
specified in Appendix 2. specified in Sub-appendix 2.
4.5.3.1.2, 254) The driver card shall be 254) The driver card shall be
able to store a number of able to store a number of
cryptographic keys and cryptographic keys and
certificates, as specified in certificates, as specified in
Appendix 11 part A. Sub-appendix 11 part A.
4.5.3.1.3, 255) The driver card shall be 255) The driver card shall be
able to store the following card able to store the following card
identification data: identification data:
card number,card number,
issuingMemberissuingContracting
State, issuing Party, issuing
authority name, issue authority name, issue
date, date,
card beginning of validity date, card beginning of validity date,
card expiry date. card expiry date.
4.5.3.1.6, 259) The driver card shall be 259) The driver card shall be
able to store the following able to store the following
driving licence data: driving licence data:
issuingMemberissuingContracting
State, issuing Party, issuing
authority name, authority name,
driving licence number (at the driving licence number (at the
date of the issue of the card). date of the issue of the card).
date of the issue of the card). date of the issue of the card). 4.5.3.1.7 261) The driver card shall be 261) The driver card shall be
date of the issue of the card). date of the issue of the card).

Г			<u> </u>
	 Event code, 	Event code,	
	 Date and time of 	 Date and time of 	
	beginning of the	beginning of the	
	event (or of card	event (or of card	
	insertion if the event	insertion if the event	
	was on-going at that	was on-going at that	
	time),	time),	
	 Date and time of end 	 Date and time of end 	
	of the event (or of	of the event (or of	
	card withdrawal if the	card withdrawal if the	
	event was on-going at	event was on-going at	
	that time),	that time),	
	VRN and registering Member	VRN and registering	
	State of vehicle in which the	Contracting Party of vehicle in	
	event happened.	which the event happened.	
4.5.3.1.8,	264) The driver card shall be	264) The driver card shall be	
264)	able to store the following data	able to store the following data	
	for these faults:	for these faults:	
	Fault code,	Fault code,	
	 Date and time of 	 Date and time of 	
	beginning of the fault	beginning of the fault	
	(or of card insertion if	(or of card insertion if	
	the fault was on-going	the fault was on-going	
	at that time),	at that time),	
	 Date and time of end 	 Date and time of end 	
	of the fault (or of card	of the fault (or of card	
	withdrawal if the fault	withdrawal if the fault	
	was on-going at that	was on-going at that	
	time),	time),	
	VRN and registering Member	VRN and registering	
	State of vehicle in which the	Contracting Party of vehicle in	
	fault happened.	which the fault happened.	
4.5.3.1.10,	269) The driver card shall be	269) The driver card shall be	
269)	able to store, for each calendar	able to store, for each calendar	
	day where the card has been	day where the card has been	
	used, and for each period of	I *	
	use of a given vehicle that day	use of a given vehicle that day	
	(a period of use includes all	(a period of use includes all	
	consecutive insertion /	consecutive insertion /	
	withdrawal cycle of the card in	withdrawal cycle of the card in	
	the vehicle, as seen from the	the vehicle, as seen from the	
	card point of view), the	card point of view), the	
	following data:	following data:	
	 date and time of first 	 date and time of first 	
	use of the vehicle (i.e.	use of the vehicle (i.e.	
	first card insertion for	first card insertion for	
	this period of use of	this period of use of	
	the vehicle, or 00h00	the vehicle, or 00h00	
	if the period of use is	if the period of use is	
	on-going at that	on-going at that	
1	time),	time),	i

- vehicle odometer value at that time, - date and time of last use of the vehicle, le. last card withdrawal for this period of use of the vehicle, or 23h59 if the period of use of the vehicle, or 23h59 if the period of use is on-going at that time), - vehicle odometer value at that time, - VRN and registering Member State of the vehicle. 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State 1 ype of the control card number and card issuing Member State, - 1 ype of the control (displaying and/or printing and/or VI downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, — VRN and registering Member State, - 1 ype of the control (displaying and/or printing and/or VI downloading and/or card downloading, see note)), - Period downloaded, in case of downloading, — VRN and registering Member State, - Type of the control card momber and card issuing Member State, - Type of the control card downloading, (see note)), - Period downloaded, in case of downloading, — VRN and registering Member State, - Type of the control card downloading will only be recorded if performed through a recording equipment.				
- date and time of last use of the vehicle, (i.e. last card withdrawal for this period of use of the vehicle, or 23h59 if the period of use is on-going at that time), — vehicle odometer value at that time, VRN and registering Member State of the vehicle. 273) The driver card shall be able to store data related to the vehicle which opened its current session: — date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store data related to the vehicle which opened its current session: — date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: — date and time of the control, clisplaying and/or printing and/or vU downloading and/or card downloading (see note), — Period downloaded, in case of downloading, will only be recorded if performed through a recording equipment. 4.5.3.1.14, 274) The driver card shall be able to store the following data related to control activities: — date and time of the control (displaying and/or printing and/or vU downloading and/or card downloading (see note)). — Period downloaded, in case of downloading will only be recorded if performed through a recording equipment.		– vehicle odometer	 vehicle odometer 	
use of the vehicle, (i.e. last card withdrawal for this period of use of the vehicle, or 23h59 if the period of use is on-going at that time), - vehicle odometer value at that time, - value at that time, - vehicle odometer value at that time, - value at that time, - vehicle odometer value at that time, - value a			value at that time,	
last card withdrawal for this period of use of the vehicle, or 23h59 if the period of use is on-going at that time), - vehicle odometer value at that time, VRN and registering Member State of the vehicle. 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control (displaying and/or printing and/or vul downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, will only be recorded if performed through a recording party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording party of the vehicle in which the control happened.		 date and time of last 		
for this period of use of the vehicle, or 23h59 if the period of use is on-going at that time), - vehicle odometer value at that time, VRN and registering Member State of the vehicle. 273) 4.5.3.1.12, 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control (displaying and/or printing and/or v U downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, (see note), - Period downloaded, in case of downloading, will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed through a recording will only be recorded if performed thr		use of the vehicle, (i.e.	use of the vehicle, (i.e.	
of the vehicle, or 23h59 if the period of use is on-going at that time), - vehicle odometer value at that time, VRN and registering Member State of the vehicle. 273) 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vul downloading (see note)), - Period downloaded, in case of downloading, (see note), - Period downloading (see note), - Period downloading will only be recorded if performed through a recording party of the vehicle or value at that time, vehicle odometer value at that time, vehicle of the		last card withdrawal	last card withdrawal	
23h59 if the period of use is on-going at that time), - vehicle odometer value at that time, VRN and registering Member State of the vehicle. 4.5.3.1.12, 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control (displaying and/or printing and/or VU downloading and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, Member State of the vehicle in which the control hopened through a recording equipment. Note: card downloading will only be recorded if performed through a recording equipment.		for this period of use	for this period of use	
use is on-going at that time), - vehicle odometer value at that time, VRN and registering Member State of the vehicle. 273) 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or Vu downloading and/or card downloading, (see note)), - Period downloaded, in case of downloading, (see note), Note: card downloading will only be recorded if performed through a recording gequipment. use is on-going at that time, - vehicle odometer value at that time, VRN and registering Contracting Party of the vehicle. 273) The driver card shall be able to store the following data related to control activities: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Contracting Party of the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Contracting Party of the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment.		of the vehicle, or	of the vehicle, or	
time), vehicle odometer value at that time, VRN and registering Member State of the vehicle. 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. Contracting Party. - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Contracting Party. - vehicle odometer value at that time, VRN and registering Contracting Party of the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Contracting Party. - vehicle. - value at that time, VRN and registering Contracting Party of the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Contracting Party. - vehicle. - value at that time, VRN and registering Contracting Party of the vehicle on the vehicle on which the control (i.e. card insertion) with a resolution of one second, VRN and registering Contracting party of the vehicle in which the control hadron provided in performed through a recording equipment.		23h59 if the period of	23h59 if the period of	
time), vehicle odometer value at that time, VRN and registering Member State of the vehicle. 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. Contracting Party. - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Contracting Party. - vehicle odometer value at that time, VRN and registering Contracting Party of the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Contracting Party. - vehicle. - value at that time, VRN and registering Contracting Party of the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Contracting Party. - vehicle. - value at that time, VRN and registering Contracting Party of the vehicle on the vehicle on which the control (i.e. card insertion) with a resolution of one second, VRN and registering Contracting party of the vehicle in which the control hadron provided in performed through a recording equipment.		use is on-going at that	use is on-going at that	
value at that time, VRN and registering Member State of the vehicle. 273) The driver card shall be able to store data related to the vehicle which opened its current session: — date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store data related to the vehicle which opened its current session: — date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: — date and time of the control, — control card number and card issuing Member State, — type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), — Period downloaded, in case of downloading, — VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. value at that time, and registering Party of the vehicle. 773) The driver card shall be able to store data related to the vehicle which opened its current session: — date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. 274) The driver card shall be able to store data related to the vehicle and time the session: — date and time		time),	time),	
VRN and registering Member State of the vehicle. 4.5.3.1.12, 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vul downloading (see note)), - Period downloading (see note)), - Period downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment.		vehicle odometer	vehicle odometer	
VRN and registering Member State of the vehicle. 4.5.3.1.12, 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vul downloading (see note)), - Period downloading (see note)), - Period downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment.		value at that time,	value at that time,	
State of the vehicle. 4.5.3.1.12, 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vud downloading (see notel)), - Period downloading (see note)), - Period downloading, (see note)), - Period downloading, on thick the control happened. Note: card downloading will only be recorded if performed through a recording equipment.		-		
4.5.3.1.12, 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be assion was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. 4.5.3.1.13, 274) The driver card shall be session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. 4.5.3.1.13, 274) The driver card shall be session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. 4.5.3.1.13, 274) The driver card shall be session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. 4.5.3.1.13, 274) The driver card shall be session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, (see note)), - Period downloaded, in case of downloading, (see note)), - Period downloaded, in case of downloading, (see note)), - Period downloaded, in case of downloading, (see note)), - Period downloading will only be recorded if performed through a recording equipment.			0 0	
4.5.3.1.12, 273) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) 274) The driver card shall be able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or card downloading (see note)), - Period downloaded, in case of downloading, (see note), - Period downloaded, in case of downloading, (see note), - Period downloaded, in case of downloading, (see note), - Period downloaded, in case of downloading, (see note), - Period downloaded, in case of downloading, (see note), - Period downloaded, in case of downloading, (see note), - Period downloaded, in case of downloading, (see note), - Period downloaded, in case of downloading, (see note), - Period downloaded, in case of downloading, (see note), - Period downloaded, in case of downloading, (see note), - Period downloaded, in case of downloading, (see note), - Period downloading (s				
able to store data related to the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, control card number and card issuing Member State, type of the control (displaying and/or printing and/or vU downloading (see note)), - Period downloading, (see note)), - Period downloading, - VRN and registering Member State of the vehicle in which the control lappened. Note: card downloading will only be recorded if performed through a recording value of the vehicle in which the control appened. Note: card downloading will only be recorded if performed through a recording value and time of the vehicle in which the control downloading will only be recorded if performed through a recording value are related to store data related to the wehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Contracting Party. 274) The driver card shall be able to store the following data related to control activities: - date and time the session: 274) The driver card shall be able to store the following data related to control activities: - date and time the session was opened (i.e. card shall be able to store the following data related to control activities: - date and time the session was opened (i.e. card shall be able to store the following data related to control activities: - date and time the session was opened (i.e. card shall be able to store the following data related to control activities: - date and time the session was opened (i.e. card shall be able to store the following data related to control activities: - date and time the session was opened (i.e. card shall be able to store the following data related to control activities: - date and time the session was opened	453112	273) The driver card shall be		
the vehicle which opened its current session: — date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 274) The driver card shall be able to store the following data related to control activities: — date and time of the control (displaying and/or printing and/or card downloading (see note)), — Period downloaded, in case of downloading, — VRN and registering Member State of twelchicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. the vehicle which opened its current session: — date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. — date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. — date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. — date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. — date and time of the control (activities: — date and time of the control, Control card number and card issuing Member State, — type of the control (displaying and/or card downloading and/or card downloading, (see note)), — Period downloaded, in case of downloading, — VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording		*	' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' '	
current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vprinting and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Party. 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, control card number and card issuing Member State, - type of the control (displaying and/or printing and/or card downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording	_, _,			
- date and time the session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment.		· ·	· ·	
session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: — date and time of the control, — control card number and card issuing Member State, — type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), — Period downloaded, in case of downloading, — VRN and registering Member State of the vehicle in which the control happened. Note: card downloading in equipment. Session was opened (i.e. card insertion) with a resolution of one second, VRN and registering Contracting Party. 274) The driver card shall be able to store the following data related to control activities: — date and time of the control, — control card number and card issuing Member State, — type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), — Period downloaded, in case of downloading, — VRN and registering Contracting Party Other Control insertion) with a resolution of one second, VRN and registering Control (displaying addor printing and/or VU downloading and/or card downloading (see note)), — Period downloaded, in case of downloading, — VRN and registering Contracting Party Of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording				
(i.e. card insertion) with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or printing and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the wehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. (i.e. card insertion) with a resolution of one second, VRN and registering (i.e. card insertion) with a resolution of one second, Wall and registering Contracting Party. 244) The driver card shall be able to store the following data related to control activities: — date and time of the control (activities: — date and time of the control (displaying and/or printing and/or printing and/or card downloading (see note)). — Period downloading (see note)). — Period downloaded, in case of downloading, — VRN and registering Contracting Party of the control happened. Note: card downloading will only be recorded if performed through a recording				
with a resolution of one second, VRN and registering Member State. 4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment.		The state of the s	-	
one second, VRN and registering Member State. 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vud downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State, - type of the control (displaying and/or printing and/or vud downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. Note: card downloading will only be recorded if performed through a recording equipment.		The state of the s		
VRN and registering Member State. 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording value of the store the following data related to control activities: - date and time of the control, - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording				
4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment.		The state of the s		
4.5.3.1.13, 274) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording and precorded if performed through a recording disable to store the following data related to control activities: - date and time of the control control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vu downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording				
able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording	A E 2 1 12			
related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which toontrol happened. Note: card downloading will only be recorded if performed through a recording equipment. related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording	-	The state of the s		
- date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or vU downloading and/or card downloading and/or card downloading (see note)), - Period downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording	274)	_	_	
control, control card number and card issuing Member State, type of the control (displaying and/or printing and/or vU downloading and/or card downloading (see note)), Period downloaded, in case of downloading, VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. control, control, control, type of the control (displaying and/or printing and/or vU downloading and/or card downloading (see note)), Period downloaded, in case of downloading, VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording				
- control card number and card issuing Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording				
and card issuing Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. and card issuing Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment.		· ·	· ·	
Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading and/or card downloading (see note)), - Period downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording				
- type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment type of the control (displaying and/or printing and/or VU downloading and/or card downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording				
(displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which tecontrol happened. Note: card downloading will only be recorded if performed through a recording (displaying and/or printing and/or downloading and/or card downloading and/or card downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording		-	•	
printing and/or VU downloading and/or card downloading (see note)), Period downloaded, in case of downloading, VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. printing and/or VU downloading and/or card downloading (see note)), Period downloaded, in case of downloading, VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment.		_		
downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. downloading and/or card downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording		(1 / 0 /	, , , , ,	
card downloading (see note)), Period downloaded, in case of downloading, VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. card downloading (see note)), Period downloaded, in case of downloading, VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording		_		
(see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording		_	_	
 Period downloaded, in case of downloading, VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. Period downloaded, in case of downloading, VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording 				
in case of downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording				
downloading, - VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. downloading, - VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording		•	·	
 VRN and registering Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. VRN and registering Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording 				
Member State of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. Contracting Party of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording		G.		
vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment. the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording				
control happened. Note: card downloading will only be recorded if performed through a recording equipment. the control happened. happened. Note: card downloading will only be recorded if performed through a recording			<u> </u>	
Note: card downloading will only be recorded if performed through a recording equipment. happened. Note: card downloading will only be recorded if performed through a recording				
only be recorded if performed through a recording equipment. Note: card downloading will only be recorded if performed through a recording				
through a recording only be recorded if performed equipment. only be recorded if performed through a recording		_		
equipment. through a recording				
		_		
equipment.		equipment.	_	
			equipment.	

45222	270) The driver could shall be	270) The driver could shall be	
4.5.3.2.2,	279) The driver card shall be	279) The driver card shall be	
279)	able to store a number of	able to store a number of	
	cryptographic keys and	cryptographic keys and	
	certificates, as specified in	certificates, as specified in	
45222	Appendix 11 part B. 280) The driver card shall be	Sub-appendix 11 part B. 280) The driver card shall be	
4.5.3.2.3, 280)	able to store the following card	able to store the following card	
280)	identification data:	identification data:	
	- card number,	- card number,	
	card number,issuing Member	card flumber,issuing Contracting	
	State, issuing	Party, issuing	
	authority name, issue	authority name, issue	
	date,	date,	
	card beginning of	card beginning of validity date,	
	validity date, card	card expiry date.	
	expiry date.	cara exp., y date.	
4.5.3.2.6,	284) The driver card shall be	284) The driver card shall be	
284)	able to store the following	able to store the following	
	driving licence data:	driving licence data:	
	issuingMember	issuing Contracting	
	State, issuing	Party, issuing	
	authority name,	authority name,	
	drivinglicence	driving licence number (at the	
	number (at the date	date of the issue of the card).	
	of the issue of the		
	card).		
	cara).		
4.5.3.2.7,	286) The driver card shall be	286) The driver card shall be	
4.5.3.2.7, 286)	286) The driver card shall be able to store the following data	able to store the following data	
	286) The driver card shall be able to store the following data for these events:	able to store the following data for these events:	
	286) The driver card shall be able to store the following data for these events: — Event code,	able to store the following data for these events: — Event code,	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of	able to store the following data for these events: - Event code, - Date and time of	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the	able to store the following data for these events: - Event code, - Date and time of beginning of the	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time),	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time),	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time),	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time),	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering	
	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Member State of	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Contracting Party of vehicle in which the event happened.	
4.5.3.2.8,	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Member State of vehicle in which the event happened. 289) The driver card shall be	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Contracting Party of vehicle in which the event happened. 289) The driver card shall be	
286)	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Member State of vehicle in which the event happened. 289) The driver card shall be able to store the following data	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Contracting Party of vehicle in which the event happened. 289) The driver card shall be able to store the following data	
4.5.3.2.8,	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Member State of vehicle in which the event happened. 289) The driver card shall be able to store the following data for these faults:	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Contracting Party of vehicle in which the event happened. 289) The driver card shall be able to store the following data for these faults:	
4.5.3.2.8,	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Member State of vehicle in which the event happened. 289) The driver card shall be able to store the following data for these faults: - Fault code,	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Contracting Party of vehicle in which the event happened. 289) The driver card shall be able to store the following data for these faults: - Fault code,	
4.5.3.2.8,	286) The driver card shall be able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Member State of vehicle in which the event happened. 289) The driver card shall be able to store the following data for these faults:	able to store the following data for these events: - Event code, - Date and time of beginning of the event (or of card insertion if the event was on-going at that time), - Date and time of end of the event (or of card withdrawal if the event was on-going at that time), - VRN and registering Contracting Party of vehicle in which the event happened. 289) The driver card shall be able to store the following data for these faults:	

	1	/ 6 1:	
	(or of card insertion if	(or of card insertion if	
	the fault was on-going	the fault was on-going	
	at that time),	at that time),	
	 Date and time of end 	 Date and time of end 	
	of the fault (or of card	of the fault (or of card	
	withdrawal if the fault	withdrawal if the fault	
	was on-going at that	was on-going at that	
	time),	time),	
	 VRN and registering 	 VRN and registering 	
	Member State of	Contracting Party of	
	vehicle in which the	vehicle in which the	
	fault happened.	fault happened.	
4.5.3.2.10,	294) The driver card shall be	294) The driver card shall be	
294	able to store, for each calendar	able to store, for each calendar	
	day where the card has been	day where the card has been	
	used, and for each period of	used, and for each period of	
	use of a given vehicle that day	use of a given vehicle that day	
	(a period of use includes all	(a period of use includes all	
	consecutive insertion /	consecutive insertion /	
	withdrawal cycle of the card in	withdrawal cycle of the card in	
	the vehicle, as seen from the	the vehicle, as seen from the	
	card point of view), the	card point of view), the	
	following data:	following data:	
	 date and time of first 	 date and time of first 	
	use of the vehicle (i.e.	use of the vehicle (i.e.	
	first card insertion for	first card insertion for	
	this period of use of	this period of use of	
	the vehicle, or 00h00	the vehicle, or 00h00	
	if the period of use is	if the period of use is	
	on-going at that	on-going at that	
	time),	time),	
	vehicle odometer	vehicle odometer	
	value at that first use	value at that first use	
	time,	time,	
	 date and time of last 	 date and time of last 	
	use of the vehicle, (i.e.	use of the vehicle, (i.e.	
	last card withdrawal	last card withdrawal	
	for this period of use	for this period of use	
	of the vehicle, or	of the vehicle, or	
	23h59 if the period of	23h59 if the period of	
	use is on-going at that	use is on-going at that	
	time),	time),	
	vehicle odometer	vehicle odometer	
	value at that last use	value at that last use	
	time,	time,	
	 VRN and registering 	 VRN and registering 	
	Member State of the	Contracting Party of	
	vehicle,	the vehicle,	
	 VIN of the vehicle. 	- VIN of the vehicle.	
4.5.3.2.12,	298) The driver card shall be	298) The driver card shall be	
298)	able to store data related to	able to store data related to	

	the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, - VRN and registering Member State.	the vehicle which opened its current session: - date and time the session was opened (i.e. card insertion) with a resolution of one second, - VRN and registering Contracting Party.	
4.5.3.2.13, 299)	299) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Member State of the vehicle in which the control happened.	299) The driver card shall be able to store the following data related to control activities: - date and time of the control, - control card number and card issuing Member State, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)), - Period downloaded, in case of downloading, - VRN and registering Contracting Party of the vehicle in which the control happened.	
4.5.4.1.2, 308)	308) The workshop card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A	308) The workshop card shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part A.	
4.5.4.1.3, 310)	310) The workshop card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date.	310) The workshop card shall be able to store the following card identification data: - card number, - issuing Contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date.	
4.5.4.2.2, 331)	331) The workshop card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part B.	331) The workshop card shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part B.	

1	222) The workshop card shall	222) The workshop card shall	
4.5.4.2.3,	333) The workshop card shall	333) The workshop card shall	
333)	be able to store the following	be able to store the following card identification data:	
	card identification data:		
	card number,	card number,	
	– issuing Member	 issuing Contracting 	
	State, issuing	Party, issuing	
	authority name, issue	authority name, issue	
	date,	date,	
	card beginning of validity date,	card beginning of validity date,	
	card expiry date.	card expiry date.	
4.5.5.1.2,	358) The control card shall	358) The control card shall	
358)	be able to store a number of	be able to store a number of	
	cryptographic keys and	cryptographic keys and	
	certificates, as specified in	certificates, as specified in	
	Appendix 11 part A.	Sub-appendix 11 part A.	
4.5.5.1.3,	359) The control card shall be	359) The control card shall be	
359)	able to store the following card	able to store the following card	
	identification data:	identification data:	
	- card number,	- card number,	
	- issuing Member State,	 issuing Contracting Party, 	
	issuing authority name,	issuing authority name,	
	issue date,	issue date,	
	card beginning of validity date,	card beginning of validity date,	
	card expiry date (if any).	card expiry date (if any).	
4.5.5.1.5,	361) The control card shall be	361) The control card shall be	
361)	able to store the following	able to store the following	
	control activity data:	control activity data:	
	- date and time of the	- date and time of the	
	control,	control,	
	- type of the control	- type of the control	
	(displaying and/or printing	(displaying and/or printing	
	and/or VU downloading	and/or VU downloading	
	and/or card downloading	and/or card downloading	
	and/or roadside	and/or roadside	
	calibration checking),	calibration checking),	
	- period downloaded (if	- period downloaded (if	
	any),	any),	
	- VRN and Member State	- VRN and Contracting Party	
	registering authority of	registering authority of	
	the controlled vehicle,	the controlled vehicle,	
	card number and card issuing	card number and card issuing	
	Member State of the driver	Contracting Party of the driver	
	card controlled.	card controlled.	
4.5.5.2.2,	364) The control card shall	364) The control card shall	
364)	be able to store a number of	be able to store a number of	
	cryptographic keys and	cryptographic keys and	
	certificates, as specified in	certificates, as specified in	
	Appendix 11 part B.	Sub-appendix 11 part B.	
4.5.5.2.3,	365) The control card shall be	365) The control card shall be	
365)	able to store the following card	able to store the following card	
	identification data:	identification data:	
	- card number,	- card number,	

- issuing Member State, issuing authority name, issue date, card beginning of validity date, card dexpiny date (if any). 4.5.5.2.5, 367) The control card shall be able to store the following control activity data: - date and time of the control, displaying and/or printing and/or VU downloading and/or card downloading and/or roadside calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing member State, issuing authority of the controlled vehicle, card despiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority of the controlled vehicle, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card unmber, - issuing authority of the controlled vehicle, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card authority of the development of cryptographic keys and certificates, as specified in sub-papendix 11 part A. 371) The company card shall be able to store the following card identification data:		1		
issue date, card beginning of validity date, card expiry date (if any). 367) The control card shall be able to store the following control activity data: date and time of the control (displaying and/or printing and/or VU downloading and/or card downloaded (if any), Period downloaded (if any), VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State ender the activity, - VRN and Member State ender the activity of the controlled of the activity, - VRN and Member State ender the activity of the controlled of the activity of the controlled controlled ender the activity of the controlled controlled ender the activity of the controlled controlled ender the controlled ende				
acard beginning of validity date, card expiry date (if any). 4.5.5.2.5, 367) The control card shall be able to store the following control activity data: - date and time of the control (displaying and/or printing and/or VU downloading and/or card downloading and/or card downloading and/or with controlled. - type of the control (displaying and/or printing and/or vul downloading and/or card downloading and/or with controlled. - VRN and Member State registering authority of the controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Contracting Party, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (U locking in and/or out,				
Card expiry date (if any). Card expiry date (if any).		issue date,	issue date,	
a.5.5.2.5, able to store the following control activity data: - date and time of the control, - type of the control (displaying and/or printing and/or vul downloading and/or crad downloading and/or roadside calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled. 4.5.6.1.2, 370) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing Member State, issuing authority name, issue date, card beginning of validity, and/or under and card issuing card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity, and/or vul downloading and/or card downloaded (if any), - VRN and Contracting Party registering authority of the controlled. 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (Vulocking in and/or vul downloading) - period downloaded (if any), - VRN and Member State registering authority of registering authority o		card beginning of validity date,	card beginning of validity date,	
able to store the following control activity data: - date and time of the control, - type of the control (displaying and/or VU downloading and/or card downloading and/or roadside calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading) and/or card downloading) and/or card downloading and/or card downloading and/or UV downloading and/or Card downloading) - period downloaded (if any).		card expiry date (if any).	card expiry date (if any).	
control activity data: - date and time of the control, - type of the control (displaying and/or printing and/or VU downloading and/or card downloading and/or card downloading and/or roadside calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing member State, issuing Contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading) and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of registering authority of	4.5.5.2.5,	367) The control card shall be	367) The control card shall be	
- date and time of the control, - type of the control (displaying and/or printing and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of crybtographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the control (displaying and/or card downloading and/or card downloading and/or card downloading) and/or card downloading and/or card downloading) and/or card downloading) and/or card downloading and/or card downloading) and/or card downloaded (if any), VRN and Member State card expiry date (if any). - VRN and Member State card expiry date (if any). - VRN and Member State card expiry date (if any). - VRN and Member State card expiry date (if any). - VRN and Member State registering authority of several party registering authority of sex pecified in solve and time of the activity, visual party registering authority of sex pecified in solve and time of the control (displaying and/or protadising and/or card downloading and/or card downloading and/or card downloading and/or card downloading and/or card d	367)	able to store the following	able to store the following	
control, - type of the control (displaying and/or printing and/or VU downloading and/or roadside calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the drive card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, issuing Contracting Party, issuing company activity data: - date and time of the activity, VU locking in and/or out, and/or VU downloading, and/or card downloaded (if any), - VRN and Member State registering authority of egistering authority of		control activity data:	control activity data:	
- type of the control (displaying and/or printing and/or VU downloading and/or roadside calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of downloaded (if any), - VRN and Member State registering authority of testing au		- date and time of the	- date and time of the	
(displaying and/or printing and/or card downloading and/or card downloading and/or roadside calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store a the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority of the driver card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of the activity (VU locking in and/or out, and/or vU downloading) - period downloaded (if any), - VRN and Member State registering authority of the activity (VU locking in and/or out, and/or VU downloading) - period downloaded (if any), - VRN and Member State registering authority of				
(displaying and/or printing and/or card downloading and/or card downloading and/or roadside calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store a the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority of the driver card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of the activity (VU locking in and/or out, and/or vU downloading) - period downloaded (if any), - VRN and Member State registering authority of the activity (VU locking in and/or out, and/or VU downloading) - period downloaded (if any), - VRN and Member State registering authority of		- type of the control	- type of the control	
and/or VU downloading and/or card downloading and/or roadside calibration checking) period downloaded (if any), VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing Member State, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority neme, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority neme, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority of the driver card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any). VRN and Member State registering authority of the activity of the		* *	1	
and/or card downloading and/or roadside calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or card downloading) and/or card downloading and/or card downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of selection calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled. and/or card downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card downloaded (if any), - VRN and Member State registering authority of registering author				
and/or roadside calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing Member State, issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or vut downloading and/or card downloaded (if any), - VRN and Member State registering authority of			_	
calibration checking) - period downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or vut, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of vegistering authority of vegistering authority of registering authority of		_	_	
- period downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store an umber of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or VU downloading and/or card downloading) and/or card downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of the controlled vehicle, card unsuber and card issuing Contracting Party of the driver card controlled. 370) The company card shall be able to store the following card identification data: - card number, - issuing Contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or VU downloading) and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of registering authority of			I	
any), - VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Contracting Party registering authority of the controlled chicke, card card insubic, card card insubic, card card insubic part of the controlled. 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part A. 371) The company card shall be able to store the following contracting Party, issuing authority of the driver card controlled. 373) The company card shall be able to store the following card identification data: - card number, - issuing Contracting Party, issuing authority of the driver card controlled. 373) The company card shall be able to store the following card identification data: - card number, - issuing Contracting Party, - issuing Contracting Party - issuing authority of the driver card indentification data: - card number issuing Contracting Party - issuing authority of the driver card indentificati		o.		
- VRN and Member State registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card demtification data: 4.5.6.1.5, 373) The company card shall be able to store the following card demtification data: 4.5.6.1.5, 373				
registering authority of the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.3, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State, registering authority of the controlled vehicle, card number activity of the driver card controlled. 370) The company card shall be able to store the following contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of			7.7	
the controlled vehicle, card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of				
card number and card issuing Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, issuing Member State, issuing authority name, issue date, card expiny date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, issuing Member State, issuing authority name, issue date, card expiny date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card deginning of validity date, card expiny date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of				
Member State of the driver card controlled. 4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or vut, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of				
a.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part A. 371) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part A. 371) The company card shall be able to store a following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of		3		
4.5.6.1.2, 370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store an umber of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Tontracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of			I	
be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part A. Sub-appendix 12 part A. S	15612			
cryptographic keys and certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of - VRN and Contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of				
certificates, as specified in Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of	370)			
Appendix 11 part A. 4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following card identification data: - card number, - issuing Contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of				
4.5.6.1.3, 371) The company card shall be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of 731) The company card shall be able to store the following card identification data: - card number, - issuing Contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of			-	
be able to store the following card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of	45643			
card identification data: - card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded any), - VRN and Member State registering authority of card identification data: - card number, - issuing Contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Contracting Party registering authority of	-			
- card number, - issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of - issuing Contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of	3/1)			
- issuing Member State, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of - issuing Contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of				
issuing authority name, issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of issue date, card beginning of validity date, card expiry date (if any). 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloaded (if any), - VRN and Member State registering authority of		-	I -	
issue date, card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading - period downloaded (if any), - VRN and Member State registering authority of issue date, card beginning of validity date, card expiry date (if any). 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of		_		
card beginning of validity date, card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of		_		
card expiry date (if any). 4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Contracting Party registering authority of				
4.5.6.1.5, 373) The company card shall be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of				
be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of be able to store the following company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of				
company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of company activity data: - date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Contracting Party registering authority of				
- date and time of the activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of	373)	_	_	
activity, - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of - type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Contracting Party registering authority of				
 type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) period downloaded (if any), VRN and Member State registering authority of type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) period downloaded (if any), VRN and Contracting Party registering authority of 				
locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of locking in and/or out, and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Contracting Party registering authority of		**	**	
and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of and/or VU downloading and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of				
and/or card downloading) - period downloaded (if any), - VRN and Member State registering authority of and/or card downloading) - period downloaded (if any), - VRN and Contracting Party registering authority of		_	_	
 period downloaded (if any), VRN and Member State registering authority of period downloaded (if any), VRN and Contracting Party registering authority of 		_	_	
any), - VRN and Member State registering authority of registering authority of				
 VRN and Member State registering authority of VRN and Contracting Party registering authority of 		The state of the s	· · · · · · · · · · · · · · · · · · ·	
registering authority of registering authority of				
vehicle, vehicle,		registering authority of	registering authority of	
, , , , , , , , , , , , , , , , , , , ,		vehicle,	vehicle,	
vernicie,		registering authority of	registering authority of	

	card number and card issuing	card number and card issuing	
	Member State (in case of card	Contracting Party (in case of	
4.5.6.0.0	downloading).	card downloading).	
4.5.6.2.2,	376) The company card shall	376) The company card shall	
376)	be able to store a number of	be able to store a number of	
	cryptographic keys and	cryptographic keys and	
	certificates, as specified in	certificates, as specified in	
45600	Appendix 11 part B.	Sub-appendix 11 part B.	
4.5.6.2.3,	377) The company card shall	377) The company card shall	
377)	be able to store the following	be able to store the following	
	card identification data:	card identification data:	
	- card number,	- card number,	
	- issuing Member State,	- issuing Contracting Party,	
	issuing authority name,	issuing authority name,	
	issue date,	issue date,	
	- card beginning of validity	- card beginning of validity	
	date, card expiry date (if	date, card expiry date (if	
45635	any).	any).	
4.5.6.2.5,	379) The company card shall	379) The company card shall	
379)	be able to store the following	be able to store the following	
	company activity data:	company activity data:	
	- date and time of the	- date and time of the	
	activity,	activity,	
	- type of the activity (VU	- type of the activity (VU	
	locking in and/or out,	locking in and/or out,	
	and/or VU downloading	and/or VU downloading	
	and/or card downloading)	and/or card downloading)	
	- period downloaded (if	- period downloaded (if	
	any),	any),	
	- VRN and Member State	- VRN and Contracting Party	
	registering authority of	registering authority of	
	vehicle,	vehicle,	
	- card number and card	- card number and card	
	issuing Member State (in	issuing Contracting Party	
	case of card downloading).	(in case of card	
E 1 205\	205) Vohiola manufacturare	downloading).	The AETP defines what miles
5.1, 385)	385) Vehicle manufacturers or	385) Vehicle manufacturers or	The AETR defines what rules
	fitters shall activate the	fitters shall activate the	must be complied with, instead
	installed recording equipment at the latest before the vehicle	installed recording equipment at the latest before the vehicle	of Regulation (EC) N°.
		is used in scope of this	561/2006).
	is used in scope of Regulation	·	
	(EC) N°. 561/2006.	Agreement.	
5.1.202\	392) Installation shall be	392) Installation shall be	The AETR defines what rules
5.1, 392)	392) Installation shall be followed by a calibration. The	followed by a calibration. The	must be complied with, instead
	first calibration may not	first calibration may not	
	necessarily include entry of	necessarily include entry of	of Regulation (EC) N°.
	the vehicle registration	the vehicle registration	561/2006).
	number (VRN), when it is not	number (VRN), when it is not	
	known by the approved	known by the approved	
	workshop having to undertake	workshop having to undertake	
	this calibration. In these	this calibration. In these	
	uns campiation. Ill these	uns candiation. III these	

	T		
	circumstances, it shall be	circumstances, it shall be	
	possible, for the vehicle	possible, for the vehicle	
	owner, and at this time only,	owner, and at this time only,	
	to enter the VRN using his	to enter the VRN using his	
	Company Card prior to using	Company Card prior to using	
	the vehicle in scope of	the vehicle in scope of this	
	Regulation (EC) N°. 561/2006	Agreement (e.g by using	
	(e.g by using commands	commands through an	
	through an appropriate menu	appropriate menu structure of	
	structure of the vehicle unit's	the vehicle unit's man-	
	man-machine interface.) . Any	machine interface.) . Any	
	update or confirmation of this	update or confirmation of this	
	entry shall only be possible	entry shall only be possible	
	using a Workshop Card.	using a Workshop Card.	
5.2, 397)	397) 1 st paragraph	397) 1 st paragraph	
312, 331,	For M1 and N1 vehicles only,	For M1 and N1 vehicles only,	
	and which are fitted with an	and which are fitted with an	
	adaptor in conformity with	adaptor in conformity with	
	Regulation (EC) N°. 68/2009	Sub-appendix 16 and where it	
	as last amended and where it	is not possible to include all	
	is not possible to include all	the information necessary, as	
	the information necessary, as	described in Requirement 396,	
	described in Requirement 396,	a second, additional, plaque	
	a second, additional, plaque	may be used. In such cases,	
	may be used. In such cases,	this additional plaque shall contain at least the last four	
	this additional plaque shall		
	contain at least the last four	indents described in	
	indents described in	Requirement 396.	
F 2, 402\	Requirement 396.	402) The seeds shall be seed	
5.3, 402)	402) The seals shall have a	402) The seals shall have a	
	free space where approved	free space where approved	
	fitters, workshops or vehicle	fitters, workshops or vehicle	
	manufacturers can add a	manufacturers can add a	
	special mark according the	special mark according to EN	
	Article 22.3 of Regulation (EU)	16882:2016.	
	N° 165/2014.	This mark shall not cover the	
	This mark shall not cover the	seal identification number.	
5.0.453	seal identification number.	101)	
5.3, 404)	404) Approved workshops	404) Approved workshops	
	and vehicle manufacturers	and vehicle manufacturers	
	shall, in the frame of	shall, in the frame of this	
	Regulation (EU) N° 165/2014,	Agreement, only use seals	
	only use seals certified	certified according EN	
	according EN 16882:2016	16882:2016 from those of the	
	from those of the seals	seals manufacturers listed in	
	manufacturers listed in the	the data base mentioned	
	data base mentioned above.	above.	
5.3, 405)	405) Seal manufacturers and	405) Seal manufacturers and	
	their distributors shall	their distributors shall	
	maintain full traceability	maintain full traceability	
	records of the seeds sold to be	records of the seals sold to be	
	records of the seals sold to be used in the frame of	used in the frame of this	

6	Regulation (EU) N° 165/2014 and shall be prepared to produce them to competent national authorities whenever need be. Requirements on the circumstances in which seals may be removed, as referred to in Article 22.5 of Regulation (EU) N° 165/2014, are defined	Agreement and shall be prepared to produce them to competent national authorities whenever need be. Requirements on the circumstances in which seals may be removed, as referred to in Article 22.5 of Regulation (EU) N° 165/2014, are defined	Reference to Regulation (EU) N°165/2014 can be removed (not needed)
	in Chapter 5.3 of this annex.	in Chapter 5.3 of this Appendix.	
6.1	The Member States approve, regularly control and certify the bodies to carry out: - installations, - checks, - inspections, - repairs.	The Contracting Parties approve, regularly control and certify the bodies to carry out: - installations, - checks, - inspections, - repairs.	
	Workshop cards shall be issued only to fitters and/or workshops approved for the activation and/or the calibration of recording equipment in conformity with this annex and, unless duly justified:	Workshop cards shall be issued only to fitters and/or workshops approved for the activation and/or the calibration of recording equipment in conformity with this Appendix and, unless duly justified:	
	 who are not eligible for a company card; and whose other professional activities do not present a potential compromise of the overall security of the system as required in Appendix 10. 	 who are not eligible for a company card; and whose other professional activities do not present a potential compromise of the overall security of the system as required in Subappendix 10. 	
7	The card issuing processes set- up by the Member States shall conform to the following:	The card issuing processes set- up by the Contracting Parties shall conform to the following:	
7, 422)	The exchange of an existing tachograph card, in order to modify administrative data, shall follow the rules of the renewal if within the same Member State, or the rules of a first issue if performed by another Member State.	The exchange of an existing tachograph card, in order to modify administrative data, shall follow the rules of the renewal if within the same Contracting Party, or the rules of a first issue if performed by another Member State.	
7, 423)	The "card holder surname" for non-personal workshop or control cards shall be filled	The "card holder surname" for non-personal workshop or control cards shall be filled	

7, 424)	with workshop or control body name or with the fitter or control officer's name would Member States so decide. 424) Member States shall exchange data electronically in order to ensure the uniqueness of driver cards that they issue in accordance with Article 31 of Regulation (EU) N° 165/2014.	with workshop or control body name or with the fitter or control officer's name would Contracting Parties so decide. 424) Reserved	This requirement is removed (not applicable within the frame of the AETR)
8.1	(2nd and 3rd paragraphs) Any manufacturer may ask for type approval of recording equipment component(s) with any other recording equipment component (s), provided each component complies with the requirements of this annex. Alternately, manufacturers may also ask for type approval of recording equipment. As described in definition (10) in Article 2 of this Regulation, vehicle units have variants in components assembly. Whatever the vehicle unit components assembly, the external antenna and (if applicable) the antenna splitter connected to the GNSS receiver or to the remote communication facility are not part of the vehicle unit type approval.	(2nd and 3rd paragraphs) Any manufacturer may ask for type approval of recording equipment component(s) with any other recording equipment component(s), provided each component complies with the requirements of this Appendix. Alternately, manufacturers may also ask for type approval of recording equipment. As described in definition (10) in Article 2 of this Agreement, vehicle units have variants in components assembly. Whatever the vehicle unit components assembly, the external antenna and (if applicable) the antenna splitter connected to the GNSS receiver or to the remote communication facility are not part of the vehicle unit type approval.	
8.1, 427)	Member States type approval authorities will not grant a type approval certificate as long as they do not hold: - a security certificate (if requested by this Annex), - a functional certificate, - and an interoperability certificate (if requested by this Annex)	Contracting Parties type approval authorities will not grant a type approval certificate as long as they do not hold: - a security certificate (if requested by this	

			1
	for the recording equipment	requested by this	
	or the tachograph card,	Appendix)	
	subject of the request for type	for the recording equipment	
	approval.	or the tachograph card,	
		subject of the request for type	
		approval.	
8.1, 430)	Type approval of software	Type approval of software	
	modifications aimed to	modifications aimed to	
	upgrade a previously type	upgrade a previously type	
	approved recording	approved recording	
	equipment may not be	equipment may not be	
	refused if such modifications	refused if such modifications	
	only apply to functions not	only apply to functions not	
	specified in this Annex.	specified in this Appendix.	
	Software upgrade of a	Software upgrade of a	
	recording equipment may	recording equipment may	
	exclude the introduction of	exclude the introduction of	
	new character sets, if not	new character sets, if not	
	technically feasible.	technically feasible.	
0.2.424\			
8.2, 431)	431) The security certificate is	431) The security certificate is	
	delivered in accordance with	delivered in accordance with	
	the provisions of Appendix 10	the provisions of Sub-	
	of this Annex. Recording	appendix 10 of this Appendix.	
	equipment components to be	Recording equipment	
	certified are vehicle unit,	components to be certified	
	motion sensor, external GNSS	are vehicle unit, motion	
	facility and tachograph cards.	sensor, external GNSS facility	
		and tachograph cards.	
8.2, 432)	432) In the exceptional	432) In the exceptional	
	circumstance that the security	circumstance that the security	
	certification authorities refuse	certification authorities refuse	
	to certify new equipment on	to certify new equipment on	
	the ground of obsolescence of	the ground of obsolescence of	
	the security mechanisms, type	the security mechanisms, type	
	approval shall continue to be	approval shall continue to be	
	granted only in these specific	granted only in these specific	
	and exceptional	and exceptional	
	circumstances, and when no	circumstances, and when no	
	alternative solution, compliant	alternative solution, compliant	
	with the Regulation, exists.	with this Agreement, exists.	
8.2, 433)	Each candidate for type	Each candidate for type	
	approval shall provide the	approval shall provide the	
	Member State's type approval	Contracting Party's type	
	authority with all the material	approval authority with all the	
	and documentation that the	material and documentation	
	authority deems necessary.	that the authority deems	
	, , , , , , , , , , , , , , , , , , , ,	necessary.	
8.3, 436)	436) A functional certificate	436) A functional certificate	
3.0, .00,	shall be delivered to the	shall be delivered to the	
	manufacturer only after all	manufacturer only after all	
	functional tests specified in	functional tests specified in	
	Tarrectorial tests specifica in	ranctional tests specifica in	

	Annondiy 0 at loast have	Sub appendix 0 at least have	
	Appendix 9, at least, have been successfully passed.	Sub-appendix 9, at least, have been successfully passed.	
9.4.440\	1		
8.4, 440)	440) Interoperability tests are carried out by a single	Interoperability tests are carried out by a single	
	laboratory under the authority	competent body.	
	and responsibility of the	competent body.	
	European Commission.		
8.4, 445)	445) The interoperability tests	The interoperability tests shall	
0.4, 443)	shall be carried out, in	be carried out, in accordance	
	accordance with the	with the provisions of Sub-	
	provisions of Appendix 9 of	appendix 9 of this Appendix,	
	this Annex, with respectively	with respectively all the types	
	all the types of recording	of recording equipment or	
	equipment or tachograph	tachograph cards:	
	cards:	- for which type	
	- for which type	approval is still valid	
	approval is still valid	or,	
	or,	- or which type	
	- or which type	approval is pending	
	approval is pending	and that have a valid	
	and that have a valid	interoperability	
	interoperability	certificate.	
	certificate.	cer image.	
8.4, 449)	449) The interoperability	449) The interoperability	
0,,	certificate is valid for six	certificate is valid for six	
	months. It is revoked at the	months. It is revoked at the	
	end of this period if the	end of this period if the	
	manufacturer has not received	manufacturer has not received	
	a corresponding type approval	a corresponding type approval	
	certificate. It is forwarded by	certificate. It is forwarded by	
	the manufacturer to the type	the manufacturer to the type	
	approval authority of the	approval authority of the	
	Member State who has	Contracting Party who has	
	delivered the functional	delivered the functional	
	certificate.	certificate.	
8.5, 451)	451) The type approval	451) The type approval	
	authority of the Member State	authority of the Contracting	
	may deliver the type approval	Party may deliver the type	
	certificate as soon as it holds	approval certificate as soon as	
	the three required certificates.	it holds the three required	
		certificates.	
8.6, 455) to	Provisions for Exceptional	Each requirement to be	
459)	procedure: first	deleted and replaced by:	
	interoperability certificates	455) Reserved	
	for 2nd generation recording	456) Reserved	
	equipment and tachograph	457) Reserved	
	cards	458) Reserved	
		459) Reserved	

ANNEX 1 Current annex 1C text

117) The recording equipment shall record and store in its data memory the following data for each event detected according to the following storage rules:

Event	Storage rules	Data to be recorded per event
Insertion of a non-valid card	- the 10 most recent events.	 date and time of event, card(s) type, number, issuing Member State and generation of the card creating the event. number of similar events that day
Card conflict	- the 10 most recent events.	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of the two cards creating the conflict.
Driving without an appropriate card	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Card insertion while driving	- the last event for each of the 10 last days of occurrence,	 date and time of the event, card(s) type, number, issuing Member State and generation, number of similar events that day
Last card session not correctly closed	- the 10 most recent events.	 date and time of card insertion, card(s) type, number, issuing Member State and generation, last session data as read from the card: date and time of card insertion, VRN, Member State of registration and VU generation.
Over speeding (1)	 the most serious event for each of the 10 last days of occurrence (i.e. the one with the highest average speed), the 5 most serious events over the last 365 days. the first event having occurred after the last calibration 	 date and time of beginning of event, date and time of end of event, maximum speed measured during the event, arithmetic average speed measured during the event, card type, number, issuing Member State and generation of the driver card (if applicable), number of similar events that day.
Power supply interruption (2)	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.

Communication error with the remote communication facility Absence of position information from GNSS receiver	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day. date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event,
Communication error with the external GNSS facility	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 number of similar events that day. date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Motion data error	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Vehicle motion conflict	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Security breach attempt	- the 10 most recent events per type of event.	 date and time of beginning of event, date and time of end of event (if relevant), card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, type of event.
Time conflict	 the most serious event for each of the 10 last days of occurrence (i.e. the ones with the greatest difference between recording equipment date and time, and GNSS date and time), the 5 most serious events over the last 365 days. 	 recording equipment date and time GNSS date and time, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.

- (1) The recording equipment shall also record and store in its data memory:
 - the date and time of the last OVER SPEEDING CONTROL,

- the date and time of the first over speeding following this OVER SPEEDING CONTROL,
- the number of over speeding events since the last OVER SPEEDING CONTROL.
- (2) These data may be recorded at power supply reconnection only, times may be known with an accuracy to the minute.

To be replaced with:

117) The recording equipment shall record and store in its data memory the following data for each event detected according to the following storage rules:

Event	Storage rules	Data to be recorded per event
Insertion of a non-valid card	- the 10 most recent events.	 date and time of event, card(s) type, number, issuing Contracting Party and generation of the card creating the event. number of similar events that day
Card conflict	- the 10 most recent events.	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party and generation of the two cards creating the conflict.
Driving without an appropriate card	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Card insertion while driving	- the last event for each of the 10 last days of occurrence,	 date and time of the event, card(s) type, number, issuing Contracting Party and generation, number of similar events that day
Last card session not correctly closed	- the 10 most recent events.	 date and time of card insertion, card(s) type, number, issuing Contracting Party and generation, last session data as read from the card: date and time of card insertion, VRN, Contracting Party of registration and VU generation.
Over speeding (1)	 the most serious event for each of the 10 last days of occurrence (i.e. the one with the highest average speed), the 5 most serious events over the last 365 days. the first event having occurred after the last calibration 	 date and time of beginning of event, date and time of end of event, maximum speed measured during the event, arithmetic average speed measured during the event, card type, number, issuing Contracting Party and generation of the driver card (if applicable), number of similar events that day.

Power supply	- the longest event for each of the 10	- date and time of beginning of event,
interruption (2)	last days of occurrence, - the 5 longest events over the last 365 days.	 date and time of end of event, card(s) type, number, issuing Contracting Party and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Communication error with the remote communication facility	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Absence of position information from GNSS receiver	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Communication error with the external GNSS facility	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Motion data error	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Vehicle motion conflict	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Security breach attempt	- the 10 most recent events per type of event.	 date and time of beginning of event, date and time of end of event (if relevant), card(s) type, number, issuing Contracting Party and generation of any card inserted at beginning and/or end of the event, type of event.

Time conflict	- the most serious event for each of	- recording equipment date and time
	the 10 last days of occurrence (i.e.	- GNSS date and time,
	the ones with the greatest difference	- card(s) type, number, issuing
	between recording equipment date	Contracting Party and generation of
	and time, and GNSS date and time),	any card inserted at beginning and/or
	- the 5 most serious events over the	end of the event,
	last 365 days.	- number of similar events that day.

- (1) The recording equipment shall also record and store in its data memory:
 - the date and time of the last OVER SPEEDING CONTROL,
 - the date and time of the first over speeding following this OVER SPEEDING CONTROL,
 - the number of over speeding events since the last OVER SPEEDING CONTROL.
- (2) These data may be recorded at power supply reconnection only, times may be known with an accuracy to the minute.

ANNEX 2

Current text

118) The recording equipment shall attempt to record and store in its data memory the following data for each fault detected according to the following storage rules:

Fault	Storage rules	Data to be recorded per fault
Card fault	- the 10 most recent driver card faults.	- date and time of beginning of fault,
		- date and time of end of fault,
		- card(s) type, number, issuing
		Member State and generation.
Recording equipment	- the 10 most recent faults for each	- date and time of beginning of fault,
faults	type of fault,	- date and time of end of fault,
	- the first fault after the last	- type of fault,
	calibration.	- card(s) type, number and issuing
		Member State and generation of any
		card inserted at beginning and/or end
		of the fault.

To be replaced with:

118) The recording equipment shall attempt to record and store in its data memory the following data for each fault detected according to the following storage rules:

Fault	Storage rules	Data to be recorded per fault
Card fault	- the 10 most recent driver card faults.	 date and time of beginning of fault, date and time of end of fault, card(s) type, number, issuing Contracting Party and generation.
Recording equipment faults	 the 10 most recent faults for each type of fault, the first fault after the last calibration. 	 date and time of beginning of fault, date and time of end of fault, type of fault, card(s) type, number and issuing Contracting Party and generation of any card inserted at beginning and/or end of the fault.

ANNEX 3 Distinguishing signs of the Member States

В	Belgium	LV	Latvia
BG	Bulgaria	L	Luxembourg
CZ	Czech Republic	LT	Lithuania
CY	Cyprus	M	Malta
DK	Denmark	NL	The Netherlands
D	Germany	A	Austria
EST	Estonia	PL	Poland
GR	Greece	P	Portugal
		RO	Romania
		SK	Slovakia
		SLO	Slovenia
Е	Spain	FIN	Finland

F	France	S	Sweden
HR	Croatia		
Н	Hungary		
IRL	Ireland	UK	The United Kingdom
I	Italy		

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 1 FOR AETR V0.1 20190120

Point or	Text Appendix 1	Proposed text for	Comments
article	/T:+1-\	AETR	
TITLE	(Title) APPENDIX 1. DATA	SUB-APPENDIX 1. DATA	
	DICTIONARY	DICTIONARY	
TABLE OF		Update Table of contents	
CONTENTS		according to the changes in	
0011121110		the document as necessary	
1	This appendix specifies data	This Sub-appendix specifies	
	formats, data elements, and	data formats, data elements,	
	data structures for use within	and data structures for use	
	the recording equipment and	within the control device and	
	tachograph cards.	tachograph cards.	
1.1	This appendix uses Abstract	This Sub-appendix uses	
	Syntax Notation One (ASN.1)	Abstract Syntax Notation One	
	to define data types. This	(ASN.1) to define data types.	
	enables simple and structured	This enables simple and	
	data to be defined without	structured data to be defined	
	implying any specific transfer	without implying any specific	
	syntax (encoding rules) which	transfer syntax (encoding	
	will be application and	rules) which will be	
	environment dependent.	application and environment	
	ASN.1 type naming	dependent.	
	conventions are done in	ASN.1 type naming	
	accordance with ISO/IEC 8824-	conventions are done in	
	1. This implies that:	accordance with ISO/IEC 8824-	
	- where possible, the	1. This implies that:	
	meaning of the data type is	- where possible, the	
	implied through the names	meaning of the data type is	
	being selected,	implied through the names	
	 where a data type is a composition of other data 	being selected, - where a data type is a	
	types, the data type name is	composition of other data	
	still a single sequence of	types, the data type name is	
	alphabetical characters	still a single sequence of	
	commencing with a capital	alphabetical characters	
	letter, however capitals are	commencing with a capital	
	used within the name to	letter, however capitals are	
	impart the corresponding	used within the name to	
	meaning,	impart the corresponding	
	- in general, the data	meaning,	
	types names are related to the	- in general, the data	
	name of the data types from	types names are related to the	
	which they are constructed,	name of the data types from	
	the equipment in which data	which they are constructed,	
	is stored and the function	the equipment in which data	
	related to the data.	is stored and the function	
		related to the data.	

	If an ACN 1 type is already	If an ACN 1 tune is already	
	If an ASN.1 type is already defined as part of another	If an ASN.1 type is already defined as part of another	
	standard and if it is relevant	standard and if it is relevant	
		for usage in the control	
	for usage in the recording		
	equipment, then this ASN.1 type will be defined in this	device, then this ASN.1 type will be defined in this Sub-	
	1 2 2		
	appendix.	appendix.	
	To enable several types of encoding rules, some ASN.1	To enable several types of encoding rules, some ASN.1	
		_	
	types in this appendix are constrained by value range	types in this appendix are constrained by value range	
	identifiers. The value range	identifiers. The value range	
	identifiers are defined in	identifiers are defined in	
	paragraph 3 and Appendix 2.	paragraph 3 and Sub-appendix	
	paragraph 5 and Appendix 2.	2.	
1.2	The following references are	The following references are	
1.2	used in this Appendix:	used in this Sub-appendix:	
2			
2	For any of the following data	For any of the following data	
	types, the default value for an "unknown" or a "not	types, the default value for an "unknown" or a "not	
	applicable" content will consist in filling the data	applicable" content will consist in filling the data	
	element with 'FF' bytes.	element with 'FF' bytes.	
	All data types are used for	All data types are used for	
	Generation 1 and Generation	Generation 1 and Generation	
	2 applications unless	2 applications unless	
	otherwise specified.	otherwise specified.	
	For card data types used for	For card data types used for	
	Generation 1 and Generation	Generation 1 and Generation	
	2 applications, the size	2 applications, the size	
	specified in this Appendix is	specified in this Sub-appendix	
	the one for Generation 2	is the one for Generation 2	
	application. The size for	application. The size for	
	Generation 1 application is	Generation 1 application is	
	supposed to be already known	supposed to be already known	
	by the reader. The Annex 1C	by the reader. The Appendix	
	requirement numbers related	1C requirement numbers	
	to such data types cover both	related to such data types	
	Generation 1 and Generation	cover both Generation 1 and	
	2 applications.	Generation 2 applications.	
2.1	This data type enables to	This data type enables to	
	code, within a two bytes word,	code, within a two bytes word,	
	a slot status at 00:00 and/or a	a slot status at 00:00 and/or a	
	driver status at 00:00 and/or	driver status at 00:00 and/or	
	changes of activity and/or	changes of activity and/or	
	changes of driving status	changes of driving status	
	and/or changes of card status	and/or changes of card status	
	for a driver or a co-driver. This	for a driver or a co-driver. This	
	data type is related to Annex	data type is related to	
	1C requirements 105, 266,	Appendix 1C requirements	
	291, 320, 321, 343, and 344.	105, 266, 291, 320, 321, 343,	
	, , , , , , , , , , , , , , , , , , , ,	and 344.	

2.8	Code explaining why a set of calibration parameters was recorded. This data type is related to Annex 1B requirements 097 and 098 and Annex 1C requirements 119.	Code explaining why a set of calibration parameters was recorded. This data type is related to Appendix 1B requirements 097 and 098 and Appendix 1C requirements 119.	
2.9	(1st paragraph) Information, stored in a card, related to the driver activities for a particular calendar day. This data type is related to Annex 1C requirements 266, 291, 320 and 343.	Information, stored in a card, related to the driver activities for a particular calendar day. This data type is related to Appendix 1C requirements 266, 291, 320 and 343.	
2.9	(activityPreviousRecordLength definition) activityPreviousRecordLength is the total length in bytes of the previous daily record. The maximum value is given by the length of the OCTET STRING containing these records (see CardActivityLengthRange Appendix 2 paragraph 4). When this record is the oldest daily record, the value of activityPreviousRecordLength must be set to 0.	activityPreviousRecordLength is the total length in bytes of the previous daily record. The maximum value is given by the length of the OCTET STRING containing these records (see CardActivityLengthRange Subappendix 2 paragraph 4). When this record is the oldest daily record, the value of activityPreviousRecordLength must be set to 0.	
2.10	(value assignment) Value assignment: see Appendix 2.	(value assignment) Value assignment: see Subappendix 2.	
2.11	(value assignment) The approval number shall be provided as published on the corresponding European Commission web site, i.e. for example including hyphens if any. The approval number shall be left-aligned.	The approval number shall be provided as published on the corresponding web site run by the laboratory competent for interoperability tests, i.e. for example including hyphens if any. The approval number shall be left-aligned.	
2.13	Information, stored in a card, related to the identification of the card's Integrated Circuit (IC) (Annex 1C requirement 249). The icSerialNumber together with the icManufacturingReferences identifies the card chip uniquely. The icSerialNumber alone does not uniquely identify the card chip. (value assignment)	Information, stored in a card, related to the identification of the card's Integrated Circuit (IC) (Appendix 1C requirement 249). The icSerialNumber together with the icManufacturingReferences identifies the card chip uniquely. The icSerialNumber alone does not uniquely identify the card chip.	

	\(\lambda \)	M-1	
	Value assignment: (see Annex	Value assignment: (see	
2.15	1C chapter 7) (1st paragraph)	Appendix 1C chapter 7)	
2.15	Information, stored in a driver	Information, stored in a driver	
	or workshop card, related to	or workshop card, related to	
	the last control the driver has	the last control the driver has	
	been subject to (Annex 1C	been subject to (Appendix 1C	
	requirements 274, 299, 327,	requirements 274, 299, 327,	
	and 350).	and 350).	
2.15	(controlVehicleRegistration	(controlVehicleRegistration	
2.13	definition)	definition)	
	controlVehicleRegistration is	controlVehicleRegistration is	
	the VRN and registering	the VRN and registering	
	Member State of the vehicle	Contracting Party of the	
	in which the control	vehicle in which the control	
	happened.	happened.	
2.16	Information about the actual	Information about the actual	
	usage of the card (Annex 1C	usage of the card (Appendix	
	requirement 273, 298, 326,	1C requirement 273, 298, 326,	
	and 349).	and 349).	
2.17	Information, stored in a driver	Information, stored in a driver	
	or a workshop card, related to	or a workshop card, related to	
	the activities of the driver	the activities of the driver	
	(Annex 1C requirements 267,	(Appendix 1C requirements	
	268, 292, 293, 321 and 344).	267, 268, 292, 293, 321 and	
		344).	
2.18	Information, stored in a driver	Information, stored in a driver	
	card, related to the card	card, related to the card	
	holder driver licence data	holder driver licence data	
	(Annex 1C requirement 259	(Appendix 1C requirement 259	
2.10	and 284).	and 284).	
2.19	(Generation 1, 1 st paragraph) Information, stored in a driver	Information stored in a driver	
	or workshop card, related to	Information, stored in a driver or workshop card, related to	
	the events associated with the	the events associated with the	
	card holder (Annex 1C	card holder (Appendix 1C	
	requirements 260 and 318).	requirements 260 and 318).	
2.19	(Generation 2, 1st paragraph)	. equitements 200 and 510).	
	Information, stored in a driver	Information, stored in a driver	
	or workshop card, related to	or workshop card, related to	
	the events associated with the	the events associated with the	
	card holder (Annex 1C	card holder (Appendix 1C	
	requirements 285 and 341).	requirements 285 and 341).	
2.20	(1 st paragraph)		
2.20	Information, stored in a driver	Information, stored in a driver	
	or a workshop card, related to	or a workshop card, related to	
	an event associated to the	an event associated to the	
	card holder (Annex 1C	card holder (Appendix 1C	
	requirements 261, 286, 318	requirements 261, 286, 318	
	and 341).	and 341).	
L	,	· · · · · · · · · · · · · · · · · · ·	

2.20	(eventVehicleRegistration definition) eventVehicleRegistration is the VRN and registering Member State of vehicle in which the event happened.	eventVehicleRegistration is the VRN and registering Contracting Party of vehicle in which the event happened.	
2.21	(1st paragraph) Information, stored in a driver or a workshop card, related to the faults associated to the card holder (Annex 1C requirements 263, 288, 318, and 341).	Information, stored in a driver or a workshop card, related to the faults associated to the card holder (Appendix 1C requirements 263, 288, 318, and 341).	
2.21	(definitions) CardFaultData is a sequence of Recording Equipment faults set of records followed by card faults set of records. cardFaultRecords is a set of fault records of a given fault category (Recording Equipment or card).	CardFaultData is a sequence of Control Device faults set of records followed by card faults set of records. cardFaultRecords is a set of fault records of a given fault category (Control Device or card).	
2.22	Information, stored in a driver or a workshop card, related to a fault associated to the card holder (Annex 1C requirement 264, 289, 318, and 341).	Information, stored in a driver or a workshop card, related to a fault associated to the card holder (Appendix 1C requirement 264, 289, 318, and 341).	
2.22	(faultVehicleRegistration definition) faultVehicleRegistration is the VRN and registering Member State of vehicle in which the fault happened.	(faultVehicleRegistration definition) faultVehicleRegistration is the VRN and registering Contracting Party of vehicle in which the fault happened.	
2.23	Information, stored in a card, related to the identification of the integrated circuit (IC) card (Annex 1C requirement 248).	Information, stored in a card, related to the identification of the integrated circuit (IC) card (Appendix 1C requirement 248).	
2.24	Information, stored in a card, related to the identification of the card (Annex 1C requirements 255, 280, 310, 333, 359, 365, 371, and 377).	Information, stored in a card, related to the identification of the card (Appendix 1C requirements 255, 280, 310, 333, 359, 365, 371, and 377).	
2.24	(cardIssuingMemberState definition) cardIssuingMemberState is the code of the Member State issuing the card.	(cardIssuingMemberState definition) cardIssuingMemberState is the code of the Contracting Party issuing the card.	
2.25	Generation 2: Certificate of the card public key for mutual authentication	Generation 2: Certificate of the card public key for mutual authentication	

	with a VIII The atmost one of	with a MI The atmost	
	with a VU. The structure of	with a VU. The structure of	
	this certificate is specified in	this certificate is specified in Sub-appendix 11.	
2.26	Appendix 11. (definitions)	Sub-appelluix 11.	
2.20	driverIdentification is the	driverIdentification is the	
	unique identification of a	unique identification of a	
	driver in a Member State.	driver in a Contracting Party.	
	ownerldentification is the	ownerldentification is the	
	unique identification of a	unique identification of a	
	company or a workshop or a	company or a workshop or a	
	control body within a member	control body within a	
	state.	Contracting Party.	
2.27	Information, stored in a driver	Information, stored in a driver	
2.27	or a workshop card, related to	or a workshop card, related to	
	the places where daily work	the places where daily work	
	periods begin and/or end	periods begin and/or end	
	(Annex 1C requirements 272,	(Appendix 1C requirements	
	297, 325, and 348).	272, 297, 325, and 348).	
2.32	Generation 2:	212, 231, 323, and 340).	
2.32	Certificate of the card public	Certificate of the card public	
	key for signature. The	key for signature. The	
	structure of this certificate is	structure of this certificate is	
	specified in Appendix 11.	specified in Sub-appendix 11.	
2.37	Information, stored in a driver	Information, stored in a driver	
2.37	or workshop card, related to a	or workshop card, related to a	
	period of use of a vehicle	period of use of a vehicle	
	during a calendar day (Annex	during a calendar day	
	1C requirements 269, 294,	(Appendix 1C requirements	
	322, and 345).	269, 294, 322, and 345).	
2.37	(Generation 1		
	vehicleRegistration		
	definition)	vehicleRegistration is the	
	vehicleRegistration is the		
		VRN and the registering	
	VRN and the registering	Contracting Party of the	
	Member State of the	vehicle.	
	vehicle.		
2.38	Information, stored in a driver	Information, stored in a driver	
	or workshop card, related to	or workshop card, related to	
	the vehicles used by the card	the vehicles used by the card	
	holder (Annex 1C	holder (Appendix 1C	
	requirements 270, 295, 323,	requirements 270, 295, 323,	
2.20	and 346).	and 346).	
2.39	Information, stored in a driver	Information, stored in a driver	
	or workshop card, related to a	or workshop card, related to a	
	vehicle unit that was used	vehicle unit that was used	
	(Annex 1C requirement 303	(Appendix 1C requirement 303	
2.40	and 351).	and 351).	
2.40	Information, stored in a driver	Information, stored in a driver	
	or workshop card, related to	or workshop card, related to	
	the vehicle units used by the	the vehicle units used by the	

	card holder (Annex 1C	card holder (Appendix 1C	
	requirement 306 and 352).	requirement 306 and 352).	
2.41	Generation 1:	Generation 1:	
	Certificate ::= OCTET STRING (SIZE(194))	Certificate ::= OCTET STRING (SIZE(194))	
	Value assignment: digital signature with partial recovery of a CertificateContent according to Appendix 11 common security mechanisms: Signature (128 bytes) Public Key remainder (58 bytes) Certification Authority Reference (8 bytes).	Value assignment: digital signature with partial recovery of a CertificateContent according to Sub-appendix 11 common security mechanisms: Signature (128 bytes) Public Key remainder (58 bytes) Certification Authority Reference (8 bytes).	
	Generation 2: Certificate ::= OCTET STRING (SIZE(204341))	Generation 2: Certificate ::= OCTET STRING (SIZE(204341))	
	Value assignment: See Appendix 11	Value assignment: See Sub- appendix 11	
2.42	The (clear) content of the certificate of a public key according to Appendix 11 common security mechanisms.	The (clear) content of the certificate of a public key according to Sub-appendix 11 common security mechanisms.	
2.43	Value assignment: in accordance with EquipmentType data type. 0 if certificate is the one of a Member State.	Value assignment: in accordance with EquipmentType data type. 0 if certificate is the one of a Contracting Party.	
2.45	Identifier of the Public Key of a Certification Authority (a Member State or the European Certification Authority).	Identifier of the Public Key of a Certification Authority (a Contracting Party or the Root Certification Authority).	
2.46	Information, stored in a company card, related to activities performed with the card (Annex 1C requirement 373 and 379).	Information, stored in a company card, related to activities performed with the card (Appendix 1C requirement 373 and 379).	
2.46	(definitions) cardNumberInformation is the card number and the card issuing Member State of the card downloaded, if any. vehicleRegistrationInformatio n is the VRN and registering	cardNumberInformation is the card number and the card issuing Contracting Party of the card downloaded, if any. vehicleRegistrationInformation is the VRN and registering	

	Member State of the vehicle downloaded or locked in or out.	Contracting Party of the vehicle downloaded or locked in or out.	
2.48	Information, stored in a company card related to the identification of the application of the card (Annex 1C requirement 369 and 375).	Information, stored in a company card related to the identification of the application of the card (Appendix 1C requirement 369 and 375).	
2.49	Information, stored in a company card, related to the cardholder identification (Annex 1C requirement 372 and 378).	Information, stored in a company card, related to the cardholder identification (Appendix 1C requirement 372 and 378).	
2.50	Information, stored in a control card related to the identification of the application of the card (Annex 1C requirement 357 and 363).	Information, stored in a control card related to the identification of the application of the card (Appendix 1C requirement 357 and 363).	
2.51	Information, stored in a control card, related to control activity performed with the card (Annex 1C requirement 361 and 367).	Information, stored in a control card, related to control activity performed with the card (Appendix 1C requirement 361 and 367).	
2.51	(definitions) controlledCardNumber is the card number and the card issuing Member State of the card controlled. controlledVehicleRegistration is the VRN and registering Member State of the vehicle in which the control happened.	controlledCardNumber is the card number and the card issuing Contracting Party of the card controlled. controlledVehicleRegistration is the VRN and registering Contracting Party of the vehicle in which the control happened.	
2.52	Information, stored in a control card, related to the identification of the cardholder (Annex 1C requirement 360 and 366).	Information, stored in a control card, related to the identification of the cardholder (Appendix 1C requirement 360 and 366).	
2.53	Code indicating the activities carried out during a control. This data type is related to Annex 1C requirements 126, 274, 299, 327, and 350.	Code indicating the activities carried out during a control. This data type is related to Appendix 1C requirements 126, 274, 299, 327, and 350.	
2.54	The current date and time of the recording equipment.	The current date and time of the control device.	
2.56	Counter, stored in a driver or workshop card, increased by one for each calendar day the card has been inserted in a VU. This data type is related to	Counter, stored in a driver or workshop card, increased by one for each calendar day the card has been inserted in a VU. This data type is related to	

	T		
	Annex 1C requirements 266,	Appendix 1C requirements	
2.54	299, 320, and 343.	266, 299, 320, and 343.	
2.61	Information, stored in a driver	Information, stored in a driver	
	card related to the	card related to the	
	identification of the	identification of the	
	application of the card (Annex	application of the card	
	1C requirement 253 and 278).	(Appendix 1C requirement 253	
2.62		and 278).	
2.62	Information, stored in a driver	Information, stored in a driver	
	card, related to the	card, related to the	
	identification of the	identification of the	
	cardholder (Annex 1C	cardholder (Appendix 1C	
2.62	requirement 256 and 281).	requirement 256 and 281).	
2.63	The plain text information and the MAC to be transmitted via	The plain text information and the MAC to be transmitted via	
	DSRC from the tachograph to	DSRC from the tachograph to the Remote Interrogator (RI),	
	the Remote Interrogator (RI), see Appendix 11 Part B	see Sub-appendix 11 Part B	
	chapter 13 for details.	chapter 13 for details.	
2.63	(definitions)	chapter 13 for details.	
2.03	tagLength is part of the DER-	tagLength is part of the DER-	
	TLV encoding and shall be set	TLV encoding and shall be set	
	to '81 10' (see Appendix 11	to '81 10' (see Sub-appendix	
	Part B chapter 13).	11 Part B chapter 13).	
	rare b enapter 15).	11 rate b chapter 13).	
	currentDateTime is the	currentDateTime is the	
	current date and time of the	current date and time of the	
	vehicle unit.	vehicle unit.	
	counter enumerates the RTM	counter enumerates the RTM	
	messages.	messages.	
	vuSerialNumber is the serial	vuSerialNumber is the serial	
	number of the vehicle unit.	number of the vehicle unit.	
	dSRCMKVersionNumber is the	dSRCMKVersionNumber is the	
	version number of the DSRC	version number of the DSRC	
	Master Key from which the VU	Master Key from which the VU	
	specific DSRC keys were	specific DSRC keys were	
	derived.	derived.	
	tagLengthMac is the tag and	tagLengthMac is the tag and	
	length of the MAC data object	length of the MAC data object	
	as part of the DER-TLV	as part of the DER-TLV	
	encoding. The tag shall be set	encoding. The tag shall be set	
	to '8E', the length shall encode	to '8E', the length shall encode	
	the length of the MAC in	the length of the MAC in	
	octets (see Appendix 11 Part B	octets (see Sub-appendix 11	
	chapter 13).	Part B chapter 13).	
	mac is the MAC calculated	mac is the MAC calculated	
	over the RTM message (see	over the RTM message (see	

	Apparative 11 Doub D. aboutou	Cub apparative 11 Dant D	
	Appendix 11 Part B chapter	Sub-appendix 11 Part B	
2.64	13).	chapter 13).	
2.64	Consider the caternal	Consider the caternal	
	GNSS facility public key for	GNSS facility public key for	
	mutual authentication with a	mutual authentication with a	
	VU. The structure of this	VU. The structure of this	
	certificate is specified in	certificate is specified in Sub-	
2.67	Appendix 11.	appendix 11.	
2.67	(Generation 1 value		
	assignment)	Value assignment: According	
	Value assignment: According	to ISO/IEC8824-1.	
	to ISO/IEC8824-1.	Value 0 is reserved for the	
	Value 0 is reserved for the	purpose of designating a	
	purpose of designating a	Contracting Party or Root	
	Member State or Europe in	Authority in the CHA field of	
0.67	the CHA field of certificates.	certificates.	
2.67	(Generation 2 values list)	D 104/5531	
	European Root CA (ERCA)	Root CA (ERCA)	
	(13),	(13),	
	Member State CA (MSCA)	Contracting Party CA (MSCA)	
	(14),	(14),	
2.68	Generation 1:	Generation 1:	
	The European public key.	The Root public key.	
2.70	(Generation 2 values list)		
	'3x'H Recording equipment	'3x'H Control device faults,	
	faults,		
2.71	The extended seal identifier	The extended seal identifier	
	uniquely identifies a seal	uniquely identifies a seal	
	(Annex 1C requirement 401).	(Appendix 1C requirement	
		401).	
2.73	(cardIssuingMemberState		
	definition)	cardIssuingMemberState is	
	cardlssuingMemberState is	the code of the Contracting	
	the code of the Member State	Party having issued the card.	
	having issued the card.		
2.78	Information, stored in a driver	Information, stored in a driver	
	or workshop card, related to	or workshop card, related to	
	the GNSS position of the	the GNSS position of the	
	vehicle if the accumulated	vehicle if the accumulated	
	driving time reaches a	driving time reaches a	
	multiple of three hours (Annex	multiple of three hours	
	IC requirement 306 and 354).	(Appendix IC requirement 306	
	_	and 354).	
2.79	Information, stored in a driver	Information, stored in a driver	
	or workshop card, related to	or workshop card, related to	
	the GNSS position of the	the GNSS position of the	
	vehicle if the accumulated	vehicle if the accumulated	
	driving time of the driver	driving time of the driver	
	reaches a multiple of three	reaches a multiple of three	
	hours (Annex 1C requirement	hours (Appendix 1C	
	305 and 353).	requirement 305 and 353).	

2.00	Information related to the	Information related to the	
2.80	Information related to the	Information related to the	
	GNSS position of the vehicle	GNSS position of the vehicle	
	(Annex 1C requirements 108,	(Appendix 1C requirements	
	109, 110, 296, 305, 347, and	108, 109, 110, 296, 305, 347,	
2.05	353).	and 353).	
2.85	Constant of the recording equipment (definition m)).	Constant of the control device (definition m)).	
2.86	(last paragraph)	(definition iii)).	
2.00	The third choice is suitable to	The third choice is suitable to	
	reference the public key of a	reference the public key of a	
	Member State.	Contracting Party.	
2.87	AES key and its associated key	AES key and its associated key	
2.07	version used for VU – Motion	version used for VU – Motion	
	Sensor pairing. For details see	Sensor pairing. For details see	
	Appendix 11.	Sub-appendix 11.	
2.89	Date and time, stored on a	Date and time, stored on a	
2.03	driver card, of last card	driver card, of last card	
	download (for other purposes	download (for other purposes	
	than control) Annex 1C	than control) Appendix 1C	
	requirement 257 and 282. This	requirement 257 and 282. This	
	date is updateable by a VU or	date is updateable by a VU or	
	any card reader.	any card reader.	
2.90	The link certificate between	The link certificate between	
	European Root CA key pairs.	European Root CA key pairs.	
2.92	A cryptographic checksum of	A cryptographic checksum of	
	8, 12 or 16 bytes length	8, 12 or 16 bytes length	
	corresponding to the cipher	corresponding to the cipher	
	suites specified in Appendix	suites specified in Sub-	
	11.	appendix 11.	
2.93	Code identifying whether a	Code identifying whether a	
	cardholder has manually	cardholder has manually	
	entered driver activities at	entered driver activities at	
	card insertion or not (Annex	card insertion or not	
	1B requirement 081 and	(Appendix 1B requirement 081	
	Annex 1C requirement 102).	and Appendix 1C requirement	
		102).	
2.94	Code identifying a	Code identifying a	
	manufacturer of type	manufacturer of type	
	approved equipment.	approved equipment.	
	ManufacturerCode ::=	ManufacturerCode ::=	
	INTEGER(0255)	INTEGER(0255)	
	The laboratory competent for	The laboratory competent for	
	interoperability tests	interoperability tests	
	maintains and publishes the	maintains and publishes the	
	list of manufacturer codes on	list of manufacturer codes on	
	its web site (Annex 1C	its web site (Appendix 1C	
	requirement 454).	requirement 454).	
	ManufacturerCodes are	ManufacturerCodes are	
	provisionally assigned to	provisionally assigned to	
	developers of tachograph	developers of tachograph	
	equipment on application to	equipment on application to	

		-	
	the laboratory competent for	the laboratory competent for	
	interoperability tests.	interoperability tests.	
2.96	The certificate of the public	The certificate of the public	
	key of a member state issued	key of a Contracting Party	
	by the European certification	issued by the Root	
	authority.	certification authority.	
2.97	The member state certificate	The Contracting Party	
	plus metadata as used in the	certificate plus metadata as	
	download protocol.	used in the download	
2.00	The could be been after the could be	protocol.	
2.98	The public key of a Member	The public key of a Contracting	
2.400	State.	Party.	
2.100	(Last paragraph)	The Nietiem Almber and Niversia	
	The Nation Alpha and Numeric	The Nation Alpha and Numeric	
	codes shall be held on a list	codes shall be held on a list maintained on the website of	
	maintained on the website of	the laboratory appointed to	
	the laboratory appointed to carry out interoperability	carry out interoperability	
	testing, as set out in Annex 1C	testing, as set out in Appendix	
	requirement 440.	1C requirement 440.	
2.102	(Generation 1 value	10 requirement 440.	
2.102	assignment)	Value assignment: see Sub-	
	Value assignment: see	appendix 2.	
	Appendix 2.	appendix 2.	
2.102	(Generation 2 value		
	assignment)	Value assignment: see Sub-	
	Value assignment: see	appendix 2.	
	Appendix 2.		
2.103	Counter indicating the number	Counter indicating the number	
	of calibrations performed with	of calibrations performed with	
	a workshop card since its last	a workshop card since its last	
	download (Annex 1C	download (Appendix 1C	
	requirement 317 and 340).	requirement 317 and 340).	
2.104	(Generation 1 value		
	assignment)	Value assignment: see Sub-	
	Value assignment: see	appendix 2.	
	Appendix 2.		
2.104	(Generation 2 value		
	assignment)	Value assignment: see Sub-	
	Value assignment: see	appendix 2.	
	Appendix 2.		
2.105	Value assignment: see	Value assignment: see Sub-	
	Appendix 2.	appendix 2.	
2.106	Value assignment: see	Value assignment: see Sub-	
2.407	Appendix 2.	appendix 2.	
2.107	Value assignment: see	Value assignment: see Sub-	
2.400	Appendix 2.	appendix 2.	
2.108	Value assignment: see	Value assignment: see Sub-	
2.400	Appendix 2.	appendix 2.	
2.109	Value assignment: see	Value assignment: see Sub-	
	Appendix 2.	appendix 2.	

2.110	Value assignment: see	Value assignment: see Sub-	
2.110	Appendix 2.	appendix 2.	
2.111	Value assignment: see	Value assignment: see Sub-	
2.111	Appendix 2.	appendix 2.	
2.112	Value assignment: see	Value assignment: see Sub-	
	Appendix 2.	appendix 2.	
2.114	The vehicle's odometer value	The vehicle's odometer value	
	at midnight on a given day	at midnight on a given day	
	(Annex 1B requirement 090	(Appendix 1B requirement 090	
	and Annex 1C requirement	and Appendix 1C requirement	
	113).	113).	
2.117	Information related to a place	Information related to a place	
	where a daily work period	where a daily work period	
	begins or ends (Annex 1C	begins or ends (Appendix 1C	
	requirements 108, 271, 296,	requirements 108, 271, 296,	
2.118	324, and 347). Information related to the	324, and 347). Information related to the	
2.110	vehicle previously used by a	vehicle previously used by a	
	driver when inserting his card	driver when inserting his card	
	in a vehicle unit (Annex 1B	in a vehicle unit (Appendix 1B	
	requirement 081 and Annex	requirement 081 and	
	1C requirement 102).	Appendix 1C requirement	
		102).	
2.118	(Generation 1,		
	vehicleRegistrationIdentificati		
	on definition)		
	vehicleRegistrationIdentificati	vehicleRegistrationIdentificati	
	on is the VRN and the	on is the VRN and the	
	registering Member State of	registering Contracting Party	
2.127	the vehicle. For the definition of this data	of the vehicle. For the definition of this data	
2.12/	type see Appendix 14.	type see Sub-appendix 14.	
2.130	This data type stores	This data type stores	
2.130	information about a seal that	information about a seal that	
	is attached to a component.	is attached to a component.	
	This data type is related to	This data type is related to	
	Annex 1C requirement 337.	Appendix 1C requirement 337.	
2.131	(Generation 2 value	-	
	assignment)	The approval number shall be	
	The approval number shall be	provided as published on the	
	provided as published on the	corresponding web site run by	
	corresponding European	the laboratory competent for	
	Commission web site, i.e. for	interoperability tests, i.e. for	
	example including hyphens if	example including hyphens if	
	any. The approval number shall be left-aligned.	any. The approval number shall be left-aligned.	
2.132	(Value assignment)	shall be left-aligned.	
2.132	The approval number shall be	The approval number shall be	
	provided as published on the	provided as published on the	
	corresponding European	corresponding web site run by	
	Commission web site, i.e. for	the laboratory competent for	
	example including hyphens if	interoperability tests, i.e. for	

	T		
	any. The approval number	example including hyphens if	
	shall be left-aligned.	any. The approval number	
		shall be left-aligned.	
2.133	Information, stored in a	Information, stored in a	
	vehicle unit, related to the	vehicle unit, related to the	
	identification of the external	identification of the external	
	GNSS facility coupled with the	GNSS facility coupled with the	
	vehicle unit (Annex 1C	vehicle unit (Appendix 1C	
	requirement 100).	requirement 100).	
2.134	Information related to the	Information related to the	
	identification of the external	identification of the external	
	GNSS facility (Annex 1C	GNSS facility (Appendix 1C	
	requirement 98).	requirement 98).	
2.135	Information, stored in an	Information, stored in an	
	external GNSS facility, related	external GNSS facility, related	
	to the installation of the	to the installation of the	
	external GNSS sensor (Annex	external GNSS sensor	
	1C requirement 123).		
	10 requirement 123).	(Appendix 1C requirement	
2.112		123).	
2.140	Information, stored in a	Information, stored in a	
	motion sensor, related to the	motion sensor, related to the	
	identification of the motion	identification of the motion	
	sensor (Annex 1B requirement	sensor (Appendix 1B	
	077 and Annex 1C	requirement 077 and	
	requirement 95).	Appendix 1C requirement 95).	
2.141	Information, stored in a	Information, stored in a	
	motion sensor, related to the	motion sensor, related to the	
	installation of the motion	installation of the motion	
	sensor (Annex 1B requirement	sensor (Appendix 1B	
	099 and Annex 1C		
		requirement 099 and	
	requirement 122).	Appendix 1C requirement	
		122).	
2.142	Information, stored in a	Information, stored in a	
	workshop card, related to the	workshop card, related to the	
	security data needed for	security data needed for	
	pairing motion sensors to	pairing motion sensors to	
	vehicle units (Annex 1C	vehicle units (Appendix 1C	
	requirement 308 and 331).	requirement 308 and 331).	
2.142	(Generation 2)	,	
	As described in Appendix 11 a	As described in Sub-appendix	
	workshop card shall store up	11 a workshop card shall store	
	to three keys for VU Motion	up to three keys for VU	
	*	The state of the s	
	Sensor pairing. These keys	Motion Sensor pairing. These	
	have different key versions.	keys have different key	
		versions.	
2.145	Information, stored in a	Information, stored in a	
	vehicle unit, related to the	vehicle unit, related to the	
	identification of a motion	identification of a motion	
	sensor paired with the vehicle	sensor paired with the vehicle	
	unit (Annex 1C requirement	unit (Appendix 1C	
	97).	requirement 97).	
	371.	requirement 37).	

2.149	(Congration 1 value		
2.149	(Generation 1 value assignment)	Value assignment: in	
	Value assignment: in	accordance with Sub-appendix	
	accordance with Appendix 11	11 Common security	
	Common security	mechanisms.	
	mechanisms.	····csiidiiisiisi	
2.149	(Generation 2 value		
	assignment)	Value assignment: in	
	Value assignment: in	accordance with Sub-appendix	
	accordance with Appendix 11	11 Common security	
	Common security	mechanisms.	
2.151	mechanisms. The number of similar events	The number of similar events	
2.131	for one given day (Annex 1B	for one given day (Appendix	
	requirement 094 and Annex	1B requirement 094 and	
	1C requirement 117).	Appendix 1C requirement	
		117).	
2.152	Information, stored in a driver	Information, stored in a driver	
	card, a workshop card or a	card, a workshop card or a	
	vehicle unit, related to a	vehicle unit, related to a	
	specific condition	specific condition	
	(requirements Annex 1C 130,	(requirements Appendix 1C	
2.452	276, 301, 328, and 355).	130, 276, 301, 328, and 355).	
2.153	Information, stored in a driver	Information, stored in a driver	
	card, a workshop card or a	card, a workshop card or a	
	vehicle unit, related to a	vehicle unit, related to a	
	specific condition (Annex 1C requirement 131, 277, 302,	specific condition (Appendix 1C requirement 131, 277, 302,	
	329, and 356).	329, and 356).	
2.154	Code identifying a specific	Code identifying a specific	
	condition (Annex 1B	condition (Appendix 1B	
	requirements 050b, 105a,	requirements 050b, 105a,	
	212a and 230a and Annex 1C	212a and 230a and Appendix	
	requirements 62).	1C requirements 62).	
2.159	For the definition of this data	For the definition of this data	
	type see Appendix 14.	type see Sub-appendix 14.	
2.163	(Value assignment)		
2.103	(Value assignment) Value assignment: in	Value assignment: in	
	accordance with Directive	accordance with ECE	
	92/23 (EEC) 31/03/92 O.J.	Regulation 54.	
	L129 p.95.	negalation 54.	
2.166	Identification of a vehicle,	Unique identification of a	
	unique for Europe (VRN and	vehicle (VRN and Contracting	
	Member State).	Party).	
2.169	Information stored in a VU on	Information stored in a VU on	
	the ability of the VU to use	the ability of the VU to use	
	generation 1 tachograph cards	generation 1 tachograph cards	
	or not (Annex 1C requirement	or not (Appendix 1C	
2.470	121).	requirement 121).	
2.170	Information, stored in a VU,	Information, stored in a VU,	
	related to changes of activity	related to changes of activity	

	T		1
	and/or changes of driving	and/or changes of driving	
	status and/or changes of card	status and/or changes of card	
	status for a given calendar day	status for a given calendar day	
	(Annex 1B requirement 084	(Appendix 1B requirement 084	
	and Annex 1C requirement	and Appendix 1C requirement	
	105, 106, 107) and to slots	105, 106, 107) and to slots	
	status at 00:00 that day.	status at 00:00 that day.	
2.171	Information, stored in a VU,	Information, stored in a VU,	
	related to changes of activity	related to changes of activity	
	and/or changes of driving	and/or changes of driving	
	status and/or changes of card	status and/or changes of card	
	status for a given calendar day	status for a given calendar day	
	(Annex 1C requirement 105,	(Appendix 1C requirement	
	106, 107) and to slots status at	105, 106, 107) and to slots	
	00:00 that day.	status at 00:00 that day.	
2.172	(Value assignment)		
	The approval number shall be	The approval number shall be	
	provided as published on the	provided as published on the	
	corresponding European	corresponding web site run by	
	Commission web site, i.e. for	the laboratory competent for	
	example including hyphens if	interoperability tests, i.e. for	
	any. The approval number	example including hyphens if	
	shall be left-aligned.	any. The approval number	
		shall be left-aligned.	
2.173	Information, stored in a	Information, stored in a	
	vehicle unit, related to the	vehicle unit, related to the	
	calibrations of the recording	calibrations of the recording	
	equipment (Annex 1B	equipment (Appendix 1B	
	requirement 098).	requirement 098).	
2.174	Information, stored in a	Information, stored in a	
	vehicle unit, related a	vehicle unit, related a	
	calibration of the recording	calibration of the recording	
	equipment (Annex 1B	equipment (Appendix 1B	
	requirement 098 and Annex	requirement 098 and	
	1C requirement 119 and 120).	Appendix 1C requirement 119	
		and 120).	
2.174	(vehicleRegistrationIdentificati		
	on definition)		
	vehicleRegistrationIdentificati	vehicleRegistrationIdentificati	
	on contains the VRN and	on contains the VRN and	
	registering Member State.	registering Contracting Party.	
2.175	Information, stored in a	Information, stored in a	
	vehicle unit, related to the	vehicle unit, related to the	
	calibrations of the recording	calibrations of the recording	
	equipment (Annex 1C	equipment (Appendix 1C	
	requirement 119 and 120).	requirement 119 and 120).	
2.176	Information, stored in a	Information, stored in a	
	vehicle unit, related to	vehicle unit, related to	
	insertion and withdrawal	insertion and withdrawal	
	cycles of driver cards or of	cycles of driver cards or of	
	workshop cards in the vehicle	workshop cards in the vehicle	

	081 and Annex 1C	requirement 081 and	
	requirement 103).	Appendix 1C requirement 103).	
2.177	Information stored in a	Information, stored in a	
2.1//	Information, stored in a vehicle unit, related to an	vehicle unit, related to an	
		insertion and withdrawal cycle	
	insertion and withdrawal cycle of a driver card or of a	of a driver card or of a	
	workshop card in the vehicle	workshop card in the vehicle	
	unit (Annex 1B requirement	unit (Appendix 1B	
	081 and Annex 1C	requirement 081 and	
	requirement 102).	Appendix 1C requirement	
2.177	(fullCardNumber definition)	102).	
2.1//	(fullCardNumber definition)	full Cond Number is the tune of	
	fullCardNumber is the type of	fullCardNumber is the type of	
	card, its issuing Member State	card, its issuing Contracting	
	and its card number as stored	Party and its card number as	
2 177	in the card.	stored in the card.	
2.177	(fullCardNumberAndGeneratio		
	n definition) fullCardNumberAndGeneratio	full Count Name to an American and a	
		fullCardNumberAndGeneratio	
	n is the type of card, its issuing	n is the type of card, its issuing	
	Member State, its card	Contracting Party, its card	
	number and generation as	number and generation as	
	stored in the card.	stored in the card.	
2.178	Information, stored in a	Information, stored in a	
	vehicle unit, related to	vehicle unit, related to	
	insertion and withdrawal	insertion and withdrawal	
	cycles of driver cards or of	cycles of driver cards or of	
	workshop cards in the vehicle	workshop cards in the vehicle	
	unit (Annex 1C requirement	unit (Appendix 1C	
0.470	103).	requirement 103).	
2.179	Information, stored in a	Information, stored in a	
	vehicle unit, about a	vehicle unit, about a	
	tachograph card used (Annex	tachograph card used	
	1C requirement 132).	(Appendix 1C requirement	
2.400		132).	
2.180	Information stored in a vehicle	Information stored in a vehicle	
	unit about the tachograph	unit about the tachograph	
	cards used with this VU. This	cards used with this VU. This	
	information is intended for	information is intended for	
	the analysis of VU – card	the analysis of VU – card	
	problems (Annex 1C	problems (Appendix 1C	
2.400	requirement 132).	requirement 132).	
2.183	Information, stored in a	Information, stored in a	
	vehicle unit, related to	vehicle unit, related to	
	company locks (Annex 1B	company locks (Appendix 1B	
0.46	requirement 104).	requirement 104).	
2.184	Information, stored in a	Information, stored in a	
	vehicle unit, related to one	vehicle unit, related to one	
	company lock (Annex 1B	company lock (Appendix 1B	
	requirement 104 and Annex	requirement 104 and	
	1C requirement 128).		

		Appendix 1C requirement 128).	
2.185	Information, stored in a	Information, stored in a	
	vehicle unit, related to	vehicle unit, related to	
	company locks (Annex 1C	company locks (Appendix 1C	
	requirement 128).	requirement 128).	
2.186	Information, stored in a	Information, stored in a	
2.100	vehicle unit, related to	vehicle unit, related to	
	controls performed using this	controls performed using this	
	VU (Annex 1B requirement	VU (Appendix 1B requirement	
	102).	102).	
2.187	Information, stored in a	Information, stored in a	
	vehicle unit, related to a	vehicle unit, related to a	
	control performed using this	control performed using this	
	VU (Annex 1B requirement	VU (Appendix 1B requirement	
	102 and Annex 1C	102 and Appendix 1C	
	requirement 126).	requirement 126).	
2.188	Information, stored in a	Information, stored in a	
	vehicle unit, related to	vehicle unit, related to	
	controls performed using this	controls performed using this	
	VU (Annex 1C requirement	VU (Appendix 1C requirement	
	126).	126).	
2.190	Information, stored in a	Information, stored in a	
	vehicle unit, related to the	vehicle unit, related to the	
	vehicle's detailed speed for a	vehicle's detailed speed for a	
	minute during which the	minute during which the	
	vehicle has been moving	vehicle has been moving	
	(Annnex 1B requirement 093	(Appendix 1B requirement 093	
	and Annex 1C requirement	and Appendix 1C requirement	
	116).	116).	
2.193	Oldest and latest dates for	Oldest and latest dates for	
	which a vehicle unit holds data	which a vehicle unit holds data	
	related to drivers activities	related to drivers activities	
	(Annex 1B requirements 081,	(Appendix 1B requirements	
	084 or 087 and Annex 1C	081, 084 or 087 and Appendix	
	requirements 102, 105, 108).	1C requirements 102, 105,	
		108).	
2.195	Information, stored in a	Information, stored in a	
	vehicle unit, related to its last	vehicle unit, related to its last	
	download (Annex 1B	download (Appendix 1B	
	requirement 105 and Annex	requirement 105 and	
	1C requirement 129).	Appendix 1C requirement	
		129).	
2.196	Information related to the last	Information related to the last	
	VU download (Annex 1C	VU download (Appendix 1C	
	requirement 129).	requirement 129).	
2.197	Information, stored in a	Information, stored in a	
	vehicle unit, related to events	vehicle unit, related to events	
	(Annex 1B requirement 094	(Appendix 1B requirement 094	
	except over speeding event).	except over speeding event).	
2.198	Information, stored in a	Information, stored in a	
	vehicle unit, related to an	vehicle unit, related to an	

	1		
	event (Annex 1B requirement	event (Appendix 1B	
	094 and Annex 1C	requirement 094 and	
	requirement 117 except over	Appendix 1C requirement 117	
	speeding event).	except over speeding event).	
2.199	Information, stored in a	Information, stored in a	
	vehicle unit, related to events	vehicle unit, related to events	
	(Annex 1C requirement 117	(Appendix 1C requirement 117	
	except over speeding event).	except over speeding event).	
2.200	Information, stored in a	Information, stored in a	
	vehicle unit, related to faults	vehicle unit, related to faults	
	(Annex 1B requirement 096).	(Appendix 1B requirement	
	(/ iiiiex 15 requirement 650).	096).	
2.201	Information, stored in a	Information, stored in a	
2.201	vehicle unit, related to a fault	vehicle unit, related to a fault	
	(Annex 1B requirement 096	(Appendix 1B requirement 096	
	and Annex 1C requirement	and Appendix 1C requirement	
2 202	118).	118).	
2.202	Information, stored in a	Information, stored in a	
	vehicle unit, related to faults	vehicle unit, related to faults	
	(Annex 1C requirement 118).	(Appendix 1C requirement	
		118).	
2.203	Information, stored in a	Information, stored in a	
	vehicle unit, related to the	vehicle unit, related to the	
	GNSS position of the vehicle if	GNSS position of the vehicle if	
	the accumulated driving time	the accumulated driving time	
	of the driver reaches a	of the driver reaches a	
	multiple of three hours (Annex	multiple of three hours	
	1C requirement 108, 110).	(Appendix 1C requirement	
		108, 110).	
2.204	Information, stored in a	Information, stored in a	
	vehicle unit, related to the	vehicle unit, related to the	
	GNSS position of the vehicle if	GNSS position of the vehicle if	
	the accumulated driving time	the accumulated driving time	
	reaches a multiple of three	reaches a multiple of three	
	hours (Annex 1C requirement	hours (Appendix 1C	
	108 and 110).	requirement 108 and 110).	
2.205	Information, stored in a	Information, stored in a	
	vehicle unit, related to the	vehicle unit, related to the	
	identification of the vehicle	identification of the vehicle	
	unit (Annex 1B requirement	unit (Appendix 1B	
	075 and Annex 1C	requirement 075 and	
	requirement 93 and 121).	T	
	requirement 95 and 121).	Appendix 1C requirement 93	
2 200	Information started in	and 121). Information, stored in a	
2.208	Information, stored in a	•	
	vehicle unit, related to drivers'	vehicle unit, related to drivers'	
	consent on the usage of	consent on the usage of	
	Intelligent Transport Systems	Intelligent Transport Systems	
	(Annex 1C requirement 200).	(Appendix 1C requirement	
		200).	
2.212	Information, stored in a	Information, stored in a	
	vehicle unit, related to over	vehicle unit, related to over	
	speeding events since the last	speeding events since the last	

	over speeding control (Annex 1B requirement 095 and Annex 1C requirement 117).	over speeding control (Appendix 1B requirement 095 and Appendix 1C requirement 117).	
2.214	Information, stored in a vehicle unit, related to over speeding events (Annex 1B requirement 094).	Information, stored in a vehicle unit, related to over speeding events (Appendix 1B requirement 094).	
2.215	(Generation 1) Information, stored in a vehicle unit, related to over speeding events (Annex 1B requirement 094 and Annex 1C requirement 117).	Information, stored in a vehicle unit, related to over speeding events (Appendix 1B requirement 094 and Appendix 1C requirement 117).	
2.215	(Generation 2) Information, stored in a vehicle unit, related to over speeding events (Annex 1B requirement 094 and Annex 1C requirement 117).	Information, stored in a vehicle unit, related to over speeding events (Appendix 1B requirement 094 and Appendix 1C requirement 117).	
2.216	Information, stored in a vehicle unit, related to over speeding events (Annex 1C requirement 117).	Information, stored in a vehicle unit, related to over speeding events (Appendix 1C requirement 117).	
2.218	Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1B requirement 087 and Annex 1C requirement 108 and 110).	Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Appendix 1B requirement 087 and Appendix 1C requirement 108 and 110).	
2.219	(Generation 1) Information, stored in a vehicle unit, related to a place where a driver begins or ends a daily work period (Annex 1B requirement 087 and Annex 1C requirement 108 and 110).	Information, stored in a vehicle unit, related to a place where a driver begins or ends a daily work period (Appendix 1B requirement 087 and Appendix 1C requirement 108 and 110).	
2.219	(Generation 1, fullCardNumber definition) fullCardNumber is the driver's card type, card issuing Member State and card number.	fullCardNumber is the driver's card type, card issuing Contracting Party and card number.	
2.219	(Generation 2) Information, stored in a vehicle unit, related to a place where a driver begins or ends a daily work period (Annex 1B	Information, stored in a vehicle unit, related to a place where a driver begins or ends a daily work period (Appendix	

1. Tequirement 108 and 110). 2.219 (Generation 2, fullCardNumberAndGeneration of fullCardNumberAndGeneration is the type of card, its issuing Member State, its card number and generation as stored in the card. 2.220 Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1C requirement 108 and 110). 2.223 Serial number of the webicle unit (Anpex 1B requirement 108 and 110). 2.224 Serial number of the webicle unit (Anpex 1B requirement 105 and 110). 2.225 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 103). Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 124 and 125). 3. Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 3. Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 1		requirement 007 and Anner	1D requirement 007 and	
2.219 (Generation 2, fullCardNumberAndGeneration of fullCardNumberAndGeneration on is the type of card, its issuing Member State, its card number and generation as stored in the card. 2.220 Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1 C requirement 108 and 110). 2.223 Serial number of the vehicle unit (Annex 1B requirement 1075 and Annex 1C requirement 108 and 110). 2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.231 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.233 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.234 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.235 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.235 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.235 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.236 Information, stored in a vehicle unit, related to time adjustment		requirement 087 and Annex	1B requirement 087 and	
Contracting Party, its card number and generation is the type of card, its issuing Member State, its card number and generation as stored in the card.		1C requirement 108 and 110).	1	
fullCardNumberAndGeneration n definition) n is the type of card, its issuing Member State, its card number and generation as stored in the card. 2.220 Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1C requirement 108 and 110). 2.223 Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1C requirement 193). 2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 193). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.233 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.234 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 102 and Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1B requirement 102 and Appendix 1C requirement 124 and 125). 2.235 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and			and 110).	
n definition) fullCardNumberAndGeneratio n is the type of card, its issuing Member State, its card number and generation as stored in the card. 2.220 Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1 C requirement 108 and 110). 2.223 Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1C requirement 193). 1nformation, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related at time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 1101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 1101 and Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 1nformation, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 1nformation, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 1nformation, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 1nformation, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Appendix 1C requirement 101 and Appendix 1C requirement 124 and 125). 1nformation, stored in a	2.219			
fullCardNumberAndGeneration is the type of card, its issuing Member State, its card number and generation as stored in the card. 2.220 Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1C requirement 108 and 110). 2.223 Serial number of the vehicle unit (Annex 1B requirement 1075 and Annex 1C requirement 193). 2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to to specific conditions (Annex 1B requirement 101). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related at time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the card (Annex 1C requirement 124 and 125). 3.234 Information, stored in a workshop card related to the identification of the card (Annex 1C requirement 307 and 330). 3.225 Information, stored in a workshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). 3.228 Information, stored in a workshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). 3.228 Information, stored in a workshop		fullCardNumberAndGeneratio		
n is the type of card, its issuing Member State, its card number and generation as stored in the card. 2.220 Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1 Crequirement 108 and 110). 2.223 Serial number of the vehicle unit (Annex 18 requirement 1075 and Annex 1 Crequirement 130). 2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1 Crequirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1 Brequirement 130). 2.232 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1 Brequirement 101). 2.233 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Appendix 1 Brequirement 101 and Annex 1 Crequirement 124 and 125). 2.233 Information, stored in a vehicle unit, related a time adjustments performed outside the frame of a regular calibration (Annex 1 Brequirement 101 and Annex 1 Crequirement 101 and Annex 1 Crequirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1 Brequirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1 Crequirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the card (Annex 1 Brequirement 124 and 125). Information, stored in a workshop card related to the identification of the card (Appendix 1 Crequirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification of the card (Appendix 1 Crequirement 307 and 330).		n definition)	fullCardNumberAndGeneratio	
Member State, its card number and generation as stored in the card. 2.220 Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1C requirement 108 and 110). 2.223 Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1C requirement 193). 2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.231 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to the identification of the application of the card (Annex 1C requirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the application of the card (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the card (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the card (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the card (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the card (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the card (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit,		fullCardNumberAndGeneratio	n is the type of card, its issuing	
2.220 Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1 C requirement 108 and 110). 2.223 Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1C requirement 93). 2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.231 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 1101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 1101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the agalication (Appendix 1C requirement 124 and 125). Information, stored in a workshop card related to the identification of the agaplication of the card (Appendix 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification of the card (Appendix 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification of the card (Appendix 1C requirement 307 and 330).		n is the type of card, its issuing	Contracting Party, its card	
2.220 Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1 C requirement 108 and 110). 2.223 Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1C requirement 93). 2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.231 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 1101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 1101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the agalication (Appendix 1C requirement 124 and 125). Information, stored in a workshop card related to the identification of the agaplication of the card (Appendix 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification of the card (Appendix 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification of the card (Appendix 1C requirement 307 and 330).		Member State, its card	number and generation as	
Stored in the card. Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1 C requirement 108 and 110). Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1 C requirement 93). Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1 C requirement 93). Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1 C requirement 130). Information, stored in a vehicle unit, related to specific conditions (Annex 1 C requirement 130). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1 C requirement 101 and Annex 1 C requirement 101 and Annex 1 C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1 C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1 C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1 C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1 C requirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the application of the card (Annex 1 C requirement 307 and 330). Information, stored in a vehicle unit, related to the identification of the card (Appendix 1 C requirement 307 and 330). Information, stored in a vehicle unit, related to the identification of the card (Appendix 1 C requirement 307 and 330). Information, stored in a vehicle unit, related to the identification of the car			stored in the card.	
Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Annex 1C requirement 108 and 110). Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1C requirement 93). Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 124 and 125). Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the application of the card (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the application of the card (Appendix 1C requirement 307 and 330). Information, stored in a vehicle unit, related to the identification of the application of the card (Appendix 1C requirement 307 and 330). Information, stored in a vehicle u		_		
vehicle unit, related to places where drivers begin or end a daily work period (Annex 1C requirement 108 and 110). 2.223 Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1C requirement 93). 2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.233 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to the identification of the card (Appendix 1C requirement 124 and 125). 2.235 Information, stored in a vehicle unit, related to the identification of the card (Appendix 1C requirement 124 and 125). 2.235 Information, stored in a vehicle unit, appendix 1D requirement 125 and application of the card (Appendix 1C requirement 124 and 125).	2.220		Information, stored in a	
where drivers begin or end a daily work period (Annex 1 C requirement 108 and 110). 2.223				
daily work period (Annex 1 Crequirement 108 and 110). Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1 Crequirement 93). Information, stored in a vehicle unit, related to specific conditions (Annex 1 Crequirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1 Brequirement 101). 2.232 Information, stored in a vehicle unit, related at time adjustment performed outside the frame of a regular calibration (Annex 1 Brequirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1 Brequirement 101). 2.233 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1 Brequirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1 Brequirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1 Crequirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1 Crequirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1 Crequirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the application of the card (Annex 1 Crequirement 124 and 125). Information, stored in a vehicle unit, related to the identification of the application of the card (Anpendix 1 Crequirement 307 and 330). Information, stored in a vehicle unit, related to the identification of the application of the card (Anpendix 1 Crequirement 307 and 330).				
2.223 Serial number of the vehicle unit (Annex 18 requirement 108 and 110). Serial number of the vehicle unit (Annex 18 requirement 2075 and Annex 1C requirement 30). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 18 requirement 101). Information, stored in a vehicle unit, related at time adjustment performed outside the frame of a regular calibration (Annex 18 requirement 101). Information, stored in a vehicle unit, related at time adjustment performed outside the frame of a regular calibration (Annex 18 requirement 101 and Annex 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 18 requirement 101 and Annex 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration of the application of the card (Annex 1C requirement 307 and 330). Information, stored in a vehicle unit, related to the identification of the application of the card (Anpendix 1C requirement 307 and 330). Information, stored in a vehicle unit, related to the identification of the application of the card (Anpendix 1C requirement 307 and 330). Information, stored in a vehicle unit, related to the identification of the application of the card (Anpendix 1C requirement 307 and 330).		_	_	
2.223 Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1C requirement 93). 2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.233 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101 and Appendix 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). 3.300 Information, stored in a Information, stored in a workshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). 3.301 Information, stored in a Information, stored in a Workshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). 3.303 Information, stored in a Information, stored in a Workshop card related to the identification of the application of the card (Appendix 1C requirement 307				
unit (Annex 1B requirement 075 and Annex 1C requirement 93). 2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101 and Appendix 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification of the card (Appendix 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). 3.330.	2 223			
2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 3.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 3.35 Information, stored in a vehicle unit, related to the identification of the application of the card (Annex 1C requirement 307 and 330). 3.36 Information, stored in a vehicle unit, related to the identification of the card (Appendix 1C requirement 307 and 330). 3.355 Information, stored in a vehicle unit, related to the identification of the card (Appendix 1C requirement 307 and 330).	2.223			
2.228 Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Anpendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit,				
Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130).			·	
vehicle unit, related to specific conditions (Annex 1C requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Appendix 1B requirement 101 and Appendix 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 2.235 Information, stored in a Information, stored in a vorkshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a Information, stored in a vorkshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330).	2.222		i ·	
conditions (Annex 1C requirement 130). 2.229	2.228		I -	
requirement 130). 2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1B requirement 101 and Appendix 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the card (Annex 1C requirement 124 and 125). Information, stored in a workshop card related to the identification of the card (Annex 1C requirement 307 and 330). Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustment performed outside the frame of a regular calibr		· · · · · · · · · · · · · · · · · · ·	-	
2.229 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.233 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related a time adjustments performed outside the frame of a regular calibration (Appendix 1B requirement 101 and Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related a time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 101 and Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1E requirement 101 and Appendix 1C requirement 101 a			1	
vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.233 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Information Information Information Inf				
adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1B requirement 101 and Anpendix 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Information of the application of the card (Appendix 1C requirement 307 and 330). 3 adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 4 and 125). 5 and 3 and	2.229			
outside the frame of a regular calibration (Annex 1B requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Informa			-	
calibration (Annex 1B requirement 101). 2.232		adjustments performed	adjustments performed	
requirement 101). 2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). Information, stored in a vorkshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). Information, stored in a Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vorkshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). Information, stored in a Information, stored i		outside the frame of a regular	outside the frame of a regular	
2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a linformation, stored in a linformation linformation a linformation		calibration (Annex 1B	calibration (Appendix 1B	
2.232 Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). 2.234 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a linformation, stored in a linformation linformation a linformation		requirement 101).	requirement 101).	
vehicle unit, related a time adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). Information, stored in a linformation, stored in a workshop card related to the identification of the card (Appendix 1C requirement 307 and 330). Information, stored in a linformation, stored in a linformation linformation linformation linformation linformation linformation	2.232		Information, stored in a	
adjustment performed outside the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification, stored in a Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). Information, stored in a Information, stored in a Information, stored in a Information, stored in a Information, stored in a Information, stored in a Information, stored in a Information, stored in a Information, stored in a Information, stored in a Information, stored in a Information, stored in a Information, stored in a Information, stored in a				
the frame of a regular calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1B requirement 124 and 125). Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). Information, stored in a Information, stored in a workshop card related to the identification of the card (Appendix 1C requirement 307 and 330). Information, stored in a				
calibration (Annex 1B requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Information Informa				
requirement 101 and Annex 1C requirement 124 and 125). 2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a				
2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a		•	1	
2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Information of the card (Appendix 1C requirement 307 and 330).		T	•	
2.233 Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card (Appendix 1C requirement 307 and 330). Information, stored in a Information, stored in a workshop card related to the identification of the card (Appendix 1C requirement 307 and 330). Information, stored in a Information, stored in a		25 (Squit Smelle 12-7 and 125).	I	
vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a Vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a Vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a Information, stored in a	2 233	Information stored in a		
adjustments performed outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification of the card (Appendix 1C requirement 307 and 330). Information, stored in a Information, stored in a Information, stored in a	2.233			
outside the frame of a regular calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a workside the frame of a regular calibration (Appendix 1C requirement 124 and 125). Information, stored in a workshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). Information, stored in a Information, stored in a				
calibration (Annex 1C requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a calibration (Appendix 1C requirement 124 and 125). Information, stored in a linformation (Appendix 1C requirement 124 and 125). Information, stored in a linformation (Appendix 1C requirement 307 and 330).				
requirement 124 and 125). 2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a requirement 124 and 125). Information, stored in a linformation, stored in a requirement 124 and 125). Information, stored in a linformation, stored in a			_	
2.234 Information, stored in a workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a workshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). Information, stored in a Information, stored in a				
workshop card related to the identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a workshop card related to the identification of the application of the card (Appendix 1C requirement 307 and 330). Information, stored in a	2.224			
identification of the application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a identification of the application of the card (Appendix 1C requirement 307 and 330).	2.234		I	
application of the card (Annex 1C requirement 307 and 330). 2.235 Information, stored in a application of the card (Appendix 1C requirement 307 and 330). Information, stored in a		•	I	
1C requirement 307 and 330). (Appendix 1C requirement 307 and 330). 2.235 Information, stored in a Information, stored in a				
and 330). 2.235 Information, stored in a Information, stored in a				
2.235 Information, stored in a Information, stored in a		1C requirement 307 and 330).		
workshop card, related to workshop card, related to	2.235	Information, stored in a	Information, stored in a	
		workshop card, related to	workshop card, related to	

		-	-
	workshop activity performed	workshop activity performed	
	with the card (Annex 1C	with the card (Appendix 1C	
	requirements 314, 316, 337,	requirements 314, 316, 337,	
	and 339).	and 339).	
2.236	Information, stored in a	Information, stored in a	
	workshop card, related to a	workshop card, related to a	
	calibration performed with the	calibration performed with the	
	card (Annex 1C requirement	card (Appendix 1C	
	314 and 337).	requirement 314 and 337).	
2.236	(Generation 1,		
	vehicleRegistration definition)		
	vehicleRegistration contains	vehicleRegistration contains	
	the VRN and registering	the VRN and registering	
	Member State.	Contracting Party.	
2.236	(Generation 1,		
	kConstantOfRecordingEquipm		
	ent definition)		
	kConstantOfRecordingEquipm	kConstantOfRecordingEquipm	
	ent is the constant of the	ent is the constant of the	
	recording equipment.	control device.	
2.236	(Generation 1, vuPartNumber,	CONTROL GEVICE.	
2.230	vuSerialNumber and		
	sensorSerialNumber		
	definitions)	vuPartNumber,	
	vuPartNumber,	vuSerialNumber and	
	vuSerialNumber and	sensorSerialNumber are the	
	sensorSerialNumber are the	data elements for control	
	data elements for recording	device identification.	
	equipment identification.	device identification.	
2.237	Information, stored in a	Information, stored in a	
2.237	workshop card, related to the	workshop card, related to the	
	identification of the	identification of the	
	cardholder (Annex 1C	cardholder (Appendix 1C	
2.238	requirement 311 and 334). Personal identification	requirement 311 and 334). Personal identification	
2.238			
	number of the Workshop Card	number of the Workshop Card	
	(Annex 1C requirement 309	(Appendix 1C requirement 309	
2.240	and 332).	and 332).	
2.240	Information, stored in a	Information, stored in a	
	vehicle unit, related to Power	vehicle unit, related to Power	
	Supply Interruption events	Supply Interruption events	
	(Annex 1C requirement 117).	(Appendix 1C requirement	
		117).	
2.241	Information, stored in a	Information, stored in a	
	vehicle unit, related to Power	vehicle unit, related to Power	
	Supply Interruption events	Supply Interruption events	
		4.	
	(Annex 1C requirement 117).	(Appendix 1C requirement	
		(Appendix 1C requirement 117).	

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 2 FOR AETR V0.2 20190112

Point or	Text Appendix 2	Proposed text for	Comments
article	Text Tippellulx 2	AETR	Comments
TITLE/TABLE			To be updated as needed,
OF			according to the validated
CONTENTS			changes
3.5.7.1, TCS	TCS_83 In any case, the	TCS_83 In any case, the	
83	VERIFY CERTIFICATE command	VERIFY CERTIFICATE command	
	uses the public key previously	uses the public key previously	
	selected by the MSE command	selected by the MSE command	
	to open the certificate. This	to open the certificate. This	
	public key must be the one of	public key must be the one of	
	a Member State or of Europe.	a Contracting Party or the root	
2 F 7 1 TCC	(Eth in do not)	public key.	
3.5.7.1, TCS 85	(5 th indent) Generation 1 only: If the	(5 th indent) Generation 1 only: If the	
65	selected public key (used to	selected public key (used to	
	unwrap the certificate) has a	unwrap the certificate) has a	
	CHA.LSB	CHA.LSB	
	(CertificateHolderAut	(CertificateHolderAut	
	horisation.equipment	horisation.equipment	
	Type) different from '00' (i.e.	Type) different from '00' (i.e.	
	is not the one of a Member	is neither the one of a	
	State or of Europe), the	Contracting Party nor the root	
	processing state returned is	certificate), the processing	
	'6985'	state returned is '6985'	
1.1	For the purpose of this	For the purpose of this sub-	
	appendix, the following	appendix, the following	
	abbreviations apply.	abbreviations apply.	
1.2	The following references are	The following references are	
	used in this Appendix:	used in this Sub-appendix:	
3.3 TCS_23	(in the table)	(in the table)	
	EXT-AUT-G1, SM-MAC-G1,	EXT-AUT-G1, SM-MAC-G1,	
	SM-C-MAC-G1, SM-R-ENC-G1,	SM-C-MAC-G1, SM-R-ENC-G1,	
	SM-R-ENC-MAC-G1	SM-R-ENC-MAC-G1	
	(see Appendix 11 Part A)	(see Sub-appendix 11 Part A)	
3.3 TCS_23	(in the table)	(in the table)	
	SM-MAC-G2, SM-C-MAC-G2,	SM-MAC-G2, SM-C-MAC-G2,	
	SM-R-ENC-MAC-G2	SM-R-ENC-MAC-G2	
2.4. TCC 20	(see Appendix 11 Part B)	(see Sub-appendix Part B)	
3.4, TCS_29	(after the table) Additional status words as	(after the table)	
	defined in ISO/IEC 7816-4 can	Additional status words as defined in ISO/IEC 7816-4 can	
	be returned, if their behavior	be returned, if their behavior	
	is not explicitly mentioned in	is not explicitly mentioned in	
	this appendix.	this sub-appendix.	
	ина аррении.	τιιο σαν-αρμετιαίλ.	

3.5	(2nd paragraph) Additional relevant details, related to cryptographic operations involved, are given in Appendix 11 Common security mechanisms for	(2nd paragraph) Additional relevant details, related to cryptographic operations involved, are given in Sub-appendix 11 Common security mechanisms for	
	Tachograph Generation 1 and Generation 2.	Tachograph Generation 1 and Generation 2.	
3.5, TCS_33	(last paragraph) In general the commands are specified for the plain mode, i.e. without secure messaging, as the secure messaging layer is specified in Appendix 11. It is clear from the access rules for a command whether the command shall support secure messaging or not and whether the command shall support generation 1 and / or generation 2 secure messaging. Some command variants are described with secure messaging to illustrate the usage of secure messaging.	(last paragraph) In general the commands are specified for the plain mode, i.e. without secure messaging, as the secure messaging layer is specified in Sub-appendix 11. It is clear from the access rules for a command whether the command shall support secure messaging or not and whether the command shall support generation 1 and / or generation 2 secure messaging. Some command variants are described with secure messaging to illustrate the usage of secure messaging.	
3.5.1.2, TCS_40	TCS_40 A tachograph card shall support the generation 2 secure messaging as specified in Appendix 11 Part B for this command variant	TCS_40 A tachograph card shall support the generation 2 secure messaging as specified in Sub-appendix 11 Part B for this command variant	
3.5.2.1.1, TCS_44	(11th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B)	(11th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B)	
3.5.2.1.1, TCS_45	(9th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B)	(9th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B)	

25244	(Oth row in the table)	(Oth your in the table)	
3.5.2.1.1,	(9th row in the table)	(9th row in the table)	
TCS_46	LCC : Length of following	LCC : Length of following	
	cryptographic checksum '04h' for Generation 1 secure	cryptographic checksum '04h' for Generation 1 secure	
	messaging (see Appendix 11	messaging (see Sub-appendix	
	Part A)	11 Part A)	
	'08h', '0Ch' or '10h' depending	'08h', '0Ch' or '10h' depending	
	on AES key length for	on AES key length for	
	Generation 2 secure	Generation 2 secure	
	messaging (see Appendix 11	messaging (see Sub-appendix	
	Part B)	11 Part B)	
3.5.2.3.1,	(14th row in the table)	(14th row in the table)	
TCS 54	LCC : Length of following	LCC : Length of following	
	cryptographic checksum	cryptographic checksum	
	'08h', '0Ch' or '10h' depending	'08h', '0Ch' or '10h' depending	
	on AES key length for	on AES key length for	
	Generation 2 secure	Generation 2 secure messaging	
	messaging (see Appendix 11	(see Sub-appendix 11 Part B)	
25221	Part B)		
3.5.2.3.1,	(9th row in the table)	(9th row in the table)	
TCS_55	LCC : Length of following	LCC : Length of following	
	cryptographic checksum	cryptographic checksum	
	'08h', '0Ch' or '10h' depending	'08h', '0Ch' or '10h' depending	
	on AES key length for	on AES key length for	
	Generation 2 secure	Generation 2 secure messaging	
	messaging (see Appendix 11	(see Sub-appendix 11 Part B)	
25211	Part B) (11th row in the table)	(11th row in the table)	
3.5.3.1.1,	LCC : Length of following	LCC : Length of following	
TCS_58	cryptographic checksum'04h'	cryptographic checksum'04h'	
	for Generation 1 secure	for Generation 1 secure	
	messaging (see Appendix 11	messaging (see Sub-appendix	
	Part A)	11 Part A)	
	The state of the s	'08h', '0Ch' or '10h' depending	
	'08h', '0Ch' or '10h' depending	·	
	on AES key length for	on AES key length for	
	on AES key length for Generation 2 secure messaging	on AES key length for Generation 2 secure messaging	
35311	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B)	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B)	
3.5.3.1.1, TCS 59	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table)	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table)	
3.5.3.1.1, TCS_59	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following	
The state of the s	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum	
The state of the s	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure	
The state of the s	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Appendix 11	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix	
The state of the s	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix 11 Part A)	
The state of the s	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Appendix 11 Part A)	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix	
The state of the s	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Appendix 11 Part A) '08h', '0Ch' or '10h' depending	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix 11 Part A) '08h', '0Ch' or '10h' depending	
The state of the s	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for	
The state of the s	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging	
The second secon	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) '08h',	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B)	
The second secon	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) '08h', '0Ch' or '10h' depending on	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) '08h', '0Ch' or '10h' depending	
-	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) '08h', '0Ch' or '10h' depending on AES key length for Generation	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) '08h', '0Ch' or '10h' depending on AES key length for	
The second secon	on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see	on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) (6th row in the table) LCC: Length of following cryptographic checksum '04h' for Generation 1 secure messaging (see Sub-appendix 11 Part A) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B) '08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging	

	LCC : Length of following	LCC : Length of following	
	cryptographic checksum	cryptographic checksum	
	'08h', '0Ch' or '10h' depending	'08h', '0Ch' or '10h' depending	
	on AES key length for	on AES key length for	
	Generation 2 secure messaging	Generation 2 secure messaging	
	(see Appendix 11 Part B)	(see Sub-appendix 11 Part B)	
3.5.3.3.1,	(6th row in the table)	(6th row in the table)	
TCS_68	Lcc : Length of following	Lcc : Length of following	
	cryptographic checksum	cryptographic checksum	
	'08h', '0Ch' or '10h' depending	'08h', '0Ch' or '10h' depending	
	on AES key length for	on AES key length for	
	Generation 2 secure messaging	Generation 2 secure messaging	
	(see Appendix 11 Part B)	(see Sub-appendix 11 Part B)	
3.5.5,	TCS 72 The PIN entered	TCS 72 The PIN entered	
TCS_72	by the user must be ASCII	by the user must be ASCII	
_	encoded and right padded with	encoded and right padded with	
	'FFh' bytes up to a length of 8	'FFh' bytes up to a length of 8	
	bytes by the IFD, see also the	bytes by the IFD, see also the	
	data type WorkshopCardPIN in	data type WorkshopCardPIN in	
	Appendix 1.	Sub-appendix 1.	
3.5.7.1,	(7th row in the table)	(7th row in the table)	
TCS 84	Certificate : concatenation of	Certificate : concatenation of	
. 65_6 .	data elements (as described in	data elements (as described in	
	Appendix 11)	Sub-appendix 11)	
3.5.7.1,	(2 nd indent after the table)	(2 nd indent after the table)	
TCS_85	• If the certificate verification	• If the certificate verification	
100_00	fails, the processing state	fails, the processing state	
	returned is '6688'. The	returned is '6688'. The	
	verification and unwrapping	verification and unwrapping	
	process of the certificate is	process of the certificate is	
	described in Appendix 11 for	described in Sub-appendix 11	
	G1 and G2.	for G1 and G2.	
3.5.7.2	(2 nd paragraph)	(2 nd paragraph)	
3.3.7.2	The certificate structure and	The certificate structure and	
	the domain parameters are	the domain parameters are	
	defined in Appendix 11.	defined in Sub-appendix 11.	
3.5.7.2,	Note: According to Appendix	Note: According to Sub-	
TCS_89	11 the card stores the	appendix 11 the card stores	
103_69	certificate or the relevant	the certificate or the relevant	
	contents of the certificate and	contents of the certificate and	
	updates its	updates its currentAuthenticatedTime.	
2572	currentAuthenticatedTime. (2 nd indent)	(2 nd indent)	
3.5.7.2, TCS 90	• If the selected public key	• If the selected public key	
163_90	(used to unwrap the	(used to unwrap the	
	certificate) has a CHA.LSB	certificate) has a CHA.LSB	
	(CertificateHolderAuthorisatio	(CertificateHolderAuthorisatio	
	n.equipmentType) that is not	n.equipmentType) that is not	
	suitable for the certificate	suitable for the certificate	
	verification according to	verification according to Sub-	
	Appendix 11, the processing	appendix 11, the processing	
	state returned is '6985'.	state returned is '6985'.	

Using the INTERNAL AUTHENTICATE command, the IFD can authenticate the card. The authentication process is described in Appendix 11. Includes the following statements: 3.5.7.2, TCS_92 The INTERNAL AUTHENTICATE command uses the card Private Key (implicity selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (TS_94 Card authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication token (see Sub-appendix 11). 3.5.7.2, (7th row in the table) (Card authentication (see Sub-appendix 11). 3.5.7.2,		I and I am	a ad a a	
AUTHENTICATE command, the IFD can authenticate the card. The authentication process is described in Appendix 11. It includes the following statements: 3.5.7.2, TCS_92 The INTERNAL AUTHENTICATE command uses the card Private Key (implicitly selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) Card authentication token (more details in Appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (more details in Appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (more details in Appendix 11) 3.5.7.2, (1" row in the table) Card authentication token (more details in Appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (more details in Appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (see Appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (more details in Appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (see Sub-appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (see Sub-appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (see Sub-appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (see Sub-appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (see Sub-appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (see Sub-appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (see Sub-appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (see Sub-appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (see Sub-appendix 11) 3.5.7.2, (2"" row in the table) Card authentication token (see Sub-appendix 11) 3.5.7.2, (2"" row in the table) Card authentication row	3.5.7.2,	(2 nd paragraph)	(2 nd paragraph)	
IFD can authenticate the card. The authentication process is described in Appendix 11. It includes the following statements: 3.5.7.2, TCS_92 The INTERNAL TCS_92 The INTERNAL AUTHENTICATE command uses the card Private Key (implicitly selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) TCS_94 Appendix 11) 3.5.7.2, (7th row in the table) TCS_94 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_94 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_94 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_94 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_95 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_96 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_97 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_98 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11) 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11 3.5.7.2, (2var ow in the table) TCS_99 Appendix 11 3.5.7.2, (2var	TCS_91	Using the INTERNAL	Using the INTERNAL	
The authentication process is described in Appendix 11. It includes the following statements: 3.5.7.2, TCS_92 The INTERNAL TCS_92 The INTERNAL AUTHENTICATE command uses the card Private Key (implicitly selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the Jast MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, TCS_93 The INTERNAL AUTHENTICATE command uses the card Private Key (implicitly selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, TCS_93 The INTERNAL AUTHENTICATE command (more details in Appendix 11). 3.5.7.2, TCS_94 (2nd or win the table) TCS_94 (2nd or win the table) TCS_95 (2nd or win the table) TCS_95 (2nd or win the table) TCS_95 (2nd or win the table) TCS_96 (2nd or win the table) TCS_97 (2nd or win the table) TCS_98 (2nd or win the table) TCS_99 (2nd or win		AUTHENTICATE command, the	AUTHENTICATE command, the	
described in Appendix 11. It includes the following statements: 3.5.7.2, TCS_92 The INTERNAL AUTHENTICATE command uses the card Private Key (implicitly selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (2rd row in the table) (2rd authentication token (see Appendix 11) (2rd row in the table) (2rd authentication 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication or 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2rd paragraph) (2rd paragr		IFD can authenticate the card.	IFD can authenticate the card.	
includes the following statements: 3.5.7.2, TCS_92 The INTERNAL TCS_92 The INTERNAL AUTHENTICATE command uses the card Private Key (implicitly selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (7th row in the table) (7th Sylucure) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Sub-appendix 11) (2nd row in the table) (2nd authentication token (see Sub-appendix 11) (2nd row in the table) (2nd authentication token (see Sub-appendix 11) (2nd row in the table) (2nd authentication (authentication token (see Sub-appendix 11) (2nd row in the table) (2nd authentication (authentication (authentication (authentication (authentication (authentication (authentication (authentication (authentication (authentication) (authentication		The authentication process is	The authentication process is	
includes the following statements: 3.5.7.2, TCS_92 The INTERNAL TCS_92 The INTERNAL AUTHENTICATE command uses the card Private Key (implicitly selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (7th row in the table) (7th Sylucure) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Appendix 11) (2nd row in the table) (2nd authentication token (see Sub-appendix 11) (2nd row in the table) (2nd authentication token (see Sub-appendix 11) (2nd row in the table) (2nd authentication token (see Sub-appendix 11) (2nd row in the table) (2nd authentication (authentication token (see Sub-appendix 11) (2nd row in the table) (2nd authentication (authentication (authentication (authentication (authentication (authentication (authentication (authentication (authentication (authentication) (authentication		described in Appendix 11. It	described in Sub-appendix 11.	
Statements: Statements: Statements:				
3.5.7.2, TCS_92 The INTERNAL AUTHENTICATE command uses the card Private Key (implicitly selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) TCS_94 VU.CHR (see Appendix 11) VU.CHR (see Appendix 11) VU.CHR (see Appendix 11) VU.CHR (see Sub-appendix 11) VI.CHR (se				
TCS_92 AUTHENTICATE command uses the card Private Key (implicitly selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) TCS_93 TCS_94 TCS_94 TCS_95 TCS_95 TCS_95 TCS_96 TCS_96 TCS_97 TCS_97 TCS_97 TCS_98 TCS_98 TCS_98 TCS_98 TCS_99 TCS_90 TCS_90 TCS_90 TCS_90 TCS_91 TCS_90 TCS_91 TCS_90 TCS_91 TCS_90 TCS_91 TCS_91 TCS_91 TCS_91 TCS_92 TCS_93 TCS_95 TCS_95 TCS_95 TCS_96 TCS_97 TCS_98 TCS_98 TCS_98 TCS_98 TCS_99 TCS_90	3572	TCS 92 The INTERNAL	TCS 92 The INTERNAL	
the card Private Key (implicitly selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) 7.5.93 VU.CHR (see Appendix 11) 3.5.7.2, Crow in the table) Cord authentication token (see Appendix 11) 3.5.7.2, Note: For generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 session and destroys the generation 2 session and destroys the generation 2 session and destroys the generation 2 session had setroys the gener	The state of the s	_		
selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (2rd authentication token (see Appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th row in the table) (2rd authentication token (see Sub-appendix 11) 3.5.7.2, (7th ro	. 55_52			
authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) TCS_93 VU.CHR (see Appendix 11) VU.CHR (see Appendix 11) VU.CHR (see Sub-appendix 11) VU.CHR (see Sub-appendix 11) VU.CHR (see Sub-appendix 11) VU.CHR (see Sub-appendix 11) Card authentication token (see Appendix 11) CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 session keys. 3.5.9 (?"d paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys. 3.5.9, Note: For generation 2 session keys. 3.5.9, TCS_97 keys ee Appendix 11 CSM_193 and CSM_195. If				
K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11) 3.5.7.2, (7th row in the table) TCS_93 VU.CHR (see Appendix 11) 3.5.7.2, (2nd or win the table) TCS_94 Card authentication token (see Appendix 11) CSM_193 and CSM_195. If generation 2 session keys see established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 session keys. 3.5.9 (2nd or win the table) CSM_193 and CSM_195. If generation 2 session keys. 3.5.9 (2nd or win the table) CSM_193 and CSM_195. If card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (Vu authentication). K1 (first element for session key agreement) and RND1, and wey agreement) and RND1, and wey agreement) and RND1, and wey affected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Sub-appendix 11). (7th row in the table) (7th row in the table) VU.CHR (see Sub-appendix 11) VU.CHR (see Sub-appendix 11) VU.CHR (see Sub-appendix 11) Note: For generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (Vu authentication). 3.5.9, Note: For generation 2 session and destroys the generation 2 session heys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Sub-appendix 11 for Tachograph G1 and G2 (Vu authentication). 3.5.9, Note: For generation 2 session weys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command,			,	
key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) TCS_93 VU.CHR (see Appendix 11) 3.5.7.2, (2nd row in the table) Card authentication token (see Appendix 11) 3.5.7.2, (2nd row in the table) Card authentication token (see Appendix 11) 3.5.7.2, Note: For generation 2 session keys see astablished and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, APDU, it aborts the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, APDU, it aborts the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If CSM_193 and CSM_195. If				
uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (7th row in t		*	•	
selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (7th row in the tabl				
command) to encrypt the signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (7th row in the table) (2rd authentication token (see Appendix 11) (2rd row in the table) (2rd authentication token (see Appendix 11) (2rd row in the table) (2rd authentication token (see Appendix 11) (2rd row in the table) (2rd authentication token (see Appendix 11) (2rd row in the table) (2rd authentication token (see Appendix 11) (2rd row in the table) (2rd row in the table) (2rd authentication token (see Appendix 11) (2rd row in the table) (2rd row in the t				
signature and form the authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (7th r				
authentication token (more details in Appendix 11). 3.5.7.2, (7th row in the table) (7th r				
details in Appendix 11). 3.5.7.2, (7th row in the table) TCS_93 VU.CHR (see Appendix 11) VU.CHR (see Sub-appendix 11) 3.5.7.2, (2nd row in the table) Card authentication token (see Appendix 11) 3.5.7.2, Note: For generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, TCS_97 keys see Appendix 11 CSM_193 and CSM_195. If cSM_193 and CSM_195.		3		
3.5.7.2, (7th row in the table) TCS_93 VU.CHR (see Appendix 11) VU.CHR (see Sub-appendix 11) VU.CHR (see Sub-appendix 11) VU.CHR (see Sub-appendix 11) VU.CHR (see Sub-appendix 11) 3.5.7.2, (2nd row in the table) Card authentication token (see Appendix 11) Sub-appendix 11) 3.5.7.2, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd row in the table) VU.CHR (see Sub-appendix 11) VU.CHR (see Sub-appendix 11) VU.CHR (see Sub-appendix 11) VU.CHR (see Sub-appendix 11) Card authentication token (see Sub-appendix 11) Vo.CHR (see Sub-appendix 11) Card authentication token (see Sub-appendix 11) VIII (authentication token (see Sub-appendix 11) VIII (com on the table) Card authentication token (see Sub-appendix 11) VIII (com on the table) Card authentication token (see Sub-appendix 11) VIII (com on the table) Card authentication token (see Sub-appendix 11) VIII (com on the table) Card authentication token (see Sub-appendix 11) CSM_193 and CSM_195. If		,	•	
TCS_93	2572			
3.5.7.2, (2nd row in the table) Card authentication token (see Appendix 11) 3.5.7.2, Note: For generation 2 session keys see Appendix 11 (CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 session keys. 3.5.9 3.5.9 (2nd row in the table) Card authentication token (see Sub-appendix 11) Note: For generation 2 session keys see Sub-appendix 11 (CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session Note: For generation 2 session keys.				
TCS_94 Card authentication token (see Appendix 11) 3.5.7.2, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If	_			
Appendix 11) 3.5.7.2, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If generation 2 session keys see established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9 Appendix 11) Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If	-			
3.5.7.2, TCS_95 Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, TCS_97 Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If	TCS_94		-	
TCS_95 keys see Appendix 11 CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph) (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9 Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If				
CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If				
generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 session and destroys the generation 2 session keys. (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If	TCS_95			
established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 session and destroys the generation 2 session was ession and destroys the generation 2 session keys. (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If				
tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph)				
plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If				
AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Sub-appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If		.		
APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2 nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session Keys see Appendix 11 CSM_193 and CSM_195. If		plain INTERNAL	· ·	
2 secure messaging session and destroys the generation 2 session keys. 3.5.9 (2 nd paragraph) (2 nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys. 2 secure messaging session and destroys the generation 2 session to and destroys the generation 2 session keys. (2 nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If				
and destroys the generation 2 session keys. 3.5.9 (2 nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session TCS_97 keys see Appendix 11 CSM_193 and CSM_195. If (2 nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Sub-appendix 11 for Tachograph G1 and G2 (VU authentication). Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If		_		
session keys. 3.5.9 (2 nd paragraph) (2 nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, TCS_97 Note: For generation 2 session TCS_97 keys see Appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If				
3.5.9 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, TCS_97 (2nd paragraph) Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Sub-appendix 11 for Tachograph G1 and G2 (VU authentication). Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If		_		
Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD. The authenticate the IFD. The authentication process is described in Sub-appendix 11 for Tachograph G1 and G2 (VU authentication). Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If			,	
AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, TCS_97 Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If AUTHENTICATE command, the card can authenticate the IFD. The authentication process is described in Sub-appendix 11 for Tachograph G1 and G2 (VU authentication). Note: For generation 2 session keys see Sub-appendix 11 CSM_193 and CSM_195. If	3.5.9	(2 nd paragraph)		
card can authenticate the IFD. The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, TCS_97 Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If CSM_193 and CSM_195. If		Using the EXTERNAL	Using the EXTERNAL	
The authentication process is described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, TCS_97 Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If		-	AUTHENTICATE command, the	
described in Appendix 11 for Tachograph G1 and G2 (VU authentication). 3.5.9, TCS_97 Note: For generation 2 session keys see Appendix 11 (CSM_193 and CSM_195. If CSM_193 and CSM_195. If CSM_193 and CSM_195. If		card can authenticate the IFD.	card can authenticate the IFD.	
Tachograph G1 and G2 (VU authentication). 3.5.9, Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If		The authentication process is	The authentication process is	
authentication). 3.5.9, Note: For generation 2 session TCS_97 keys see Appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If		described in Appendix 11 for	described in Sub-appendix 11	
authentication). 3.5.9, Note: For generation 2 session TCS_97 keys see Appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If		Tachograph G1 and G2 (VU	for Tachograph G1 and G2 (VU	
TCS_97 keys see Appendix 11 keys see Sub-appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If		authentication).	authentication).	
TCS_97 keys see Appendix 11 keys see Sub-appendix 11 CSM_193 and CSM_195. If CSM_193 and CSM_195. If	3.5.9,	Note: For generation 2 session	Note: For generation 2 session	
CSM_193 and CSM_195. If CSM_193 and CSM_195. If	*			
	_			
generation 2 session keys are generation 2 session keys are		generation 2 session keys are	generation 2 session keys are	
established and the established and the				
tachograph card receives the tachograph card receives the				

	plain EXTERNAL	plain EXTERNAL	
	AUTHENTICATE command	AUTHENTICATE command	
	APDU, it aborts the generation	APDU, it aborts the generation	
	2 secure messaging session	2 secure messaging session	
	and destroys the generation 2	and destroys the generation 2	
	session keys.	session keys.	
3.5.9,	(7th row in the table)	(7th row in the table)	
TCS_98	Generation 1 authentication:	Generation 1 authentication:	
	Cryptogram (see Appendix 11	Cryptogram (see Sub-appendix	
	Part A)	11 Part A)	
	Generation 2 authentication:	Generation 2 authentication:	
	Signature generated by the IFD	Signature generated by the IFD	
	(see Appendix 11 Part B)	(see Sub-appendix 11 Part B)	
3.5.10	This command is used for the	This command is used for the	
	generation 2 chip	generation 2 chip	
	authentication protocol	authentication protocol	
	specified in Appendix 11 Part B	specified in Sub-appendix 11	
	and is compliant with ISO/IEC	Part B and is compliant with	
	7816-4.	ISO/IEC 7816-4.	
3.5.10,	(7th row in the table)	(7th row in the table)	
TCS_101	DER-TLV encoded ephemeral	DER-TLV encoded ephemeral	
	public key value (see Appendix	public key value (see Sub-	
	11)	appendix 11)	
	The VU shall send the data	The VU shall send the data	
	objects in this order.	objects in this order.	
3.5.10,	(2 nd row in the table)	(2 nd row in the table)	
TCS_102	DER-TLV encoded Dynamic	DER-TLV encoded Dynamic	
	Authentication Data: nonce	Authentication Data: nonce	
	and authentication token (see	and authentication token (see	
	Appendix 11)	Sub-appendix 11)	
3.5.11.1,	(9 th row in the table)	(9 th row in the table)	
TCS_106	Key identifier as specified in	Key identifier as specified in	
	Appendix 11	Sub-appendix 11	
3.5.11.2.1,	(7 th row in the table)	(7 th row in the table)	
TCS_109	DER-TLV encoded	DER-TLV encoded	
	cryptographic mechanism	cryptographic mechanism	
	reference: Object Identifier of	reference: Object Identifier of	
	Chip Authentication (value	Chip Authentication (value	
	only, Tag '06h' is omitted).	only, Tag '06h' is omitted).	
	See Appendix 1 for the values	See Sub-appendix 1 for the	
	of object identifiers; the byte	values of object identifiers; the	
	notation shall be used. See	byte notation shall be used.	
	Appendix 11 for guidance on	See Sub-appendix 11 for	
	how to select one of these	guidance on how to select one	
	object identifiers.	of these object identifiers.	
3.5.11.2.2,	(6 th row in the table)	(6 th row in the table)	
TCS_111	DER-TLV encoded	DER-TLV encoded	
	cryptographic mechanism	cryptographic mechanism	
	reference: Object Identifier of	reference: Object Identifier of	
	VU Authentication (value only,	VU Authentication (value only,	
	Tag '06h' is omitted).	Tag '06h' is omitted).	

	See Appendix 1 for the values	See Sub-appendix 1 for the	
	of object identifiers; the byte	values of object identifiers; the	
	_	I	
	notation shall be used. See	byte notation shall be used.	
	Appendix 11 for guidance on	See Sub-appendix 11 for	
	how to select one of these	guidance on how to select one	
	object identifiers.	of these object identifiers.	
3.5.11.2.2,	(8 th row in the table)	(8 th row in the table)	
TCS_111	DER-TLV encoded compressed	DER-TLV encoded compressed	
	representation of the	representation of the	
	ephemeral public key of the VU	ephemeral public key of the VU	
	that will be used during Chip	that will be used during Chip	
	Authentication (see Appendix	Authentication (see Sub-	
	11)	appendix 11)	
3.5.11.2.3,	(7 th row in the table)	(7 th row in the table)	
TCS_113	DER-TLV encoded reference of	DER-TLV encoded reference of	
	a public key, i.e. the Certificate	a public key, i.e. the Certificate	
	Holder Reference in the	Holder Reference in the	
	certificate of the public key	certificate of the public key	
	(see Appendix 11)	(see Sub-appendix 11)	
3.5.11.2.3,	Note: In the case of a MSE: SET	Note: In the case of a MSE: SET	
TCS_114	AT for VU Authentication	AT for VU Authentication	
	command, the referenced key	command, the referenced key	
	is a VU_MA public key. The	is a VU MA public key. The	
	card shall set the VU MA	card shall set the VU MA	
	public key for use, if available	public key for use, if available	
	in its memory, which matches	in its memory, which matches	
	the Certificate Holder	the Certificate Holder	
	Reference (CHR) given in the	Reference (CHR) given in the	
	command data field (the card	command data field (the card	
	can identify VU_MA public	can identify VU_MA public	
	keys by means of the	keys by means of the	
	certificate's CHA field). A card	certificate's CHA field). A card	
	shall return "6A 88" to this	shall return "6A 88" to this	
	command in case only the	command in case only the	
	VU_Sign public key or no public	VU_Sign public key or no public	
	key of the Vehicle Unit is	key of the Vehicle Unit is	
	available. See the definition of	available. See the definition of	
	the CHA field in Appendix 11	the CHA field in Sub-appendix	
	and of data type	11 and of data type	
	equipmentType in Appendix 1.	/1	
	ечириненстуре ит Аррениіх 1.	equipmentType in Sub- appendix 1.	
	Similarly, in case an MSE: SET	appendix 1.	
	DST command referencing an	Similarly, in case an MSE: SET	
	EQT (i.e. a VU or a card) is sent	The state of the s	
	· · · · · · · · · · · · · · · · · · ·	DST command referencing an	
	to a control card, according to	EQT (i.e. a VU or a card) is sent	
	CSM_234 the referenced key is	to a control card, according to	
	always an EQT_Sign key that	CSM_234 the referenced key is	
	has to be used for the	always an EQT_Sign key that	
	verification of a digital	has to be used for the	
	signature. According to Figure	verification of a digital	
	13 in Appendix 11, the control	signature. According to Figure	
	card will always have stored	13 in Sub-appendix 11, the	

	the relevant EQT_Sign public	control card will always have	
	key. In some cases, the control	stored the relevant EQT_Sign	
	card may have stored the	public key. In some cases, the	
	corresponding EQT_MA public	control card may have stored	
	key. The control card shall	the corresponding EQT_MA	
	always set the EQT_Sign public	public key. The control card	
	key for use when it receives an	shall always set the EQT_Sign	
	MSE: SET DST command.	public key for use when it	
		receives an MSE: SET DST	
		command.	
3.5.12,	(8 th row in the table)	(8 th row in the table)	
TCS_116	Length L of the hash code:	Length L of the hash code:	
105_110	'14h' in Generation 1	'14h' in Generation 1	
	application (see Appendix 11	application (see Sub-appendix	
	Part A)	11 Part A)	
	'20h', '30h' or '40h' in	'20h', '30h' or '40h' in	
	Generation 2 application (see	Generation 2 application (see	
	Appendix 11 Part B)	Sub-appendix 11 Part B)	
3.5.13,	TCS_123 The Tachograph	TCS_123 The Tachograph	
TCS_123	Generation 2 application shall	Generation 2 application shall	
	support the SHA-2 algorithm	support the SHA-2 algorithm	
	(SHA-256, SHA-384 or SHA-	(SHA-256, SHA-384 or SHA-	
	512, specified by the cipher	512, specified by the cipher	
	suite in Appendix 11 Part B for	suite in Sub-appendix 11 Part B	
	the card signature key	for the card signature key	
	Card_Sign.	Card_Sign.	
3.5.13,	(5 th row in the table, 3 rd	(5 th row in the table, 3 rd	
TCS_124	paragraph)	paragraph)	
_	For the Tachograph	For the Tachograph	
	Generation 2 application: SHA-	Generation 2 application: SHA-	
	2 algorithm (SHA-256, SHA-384	2 algorithm (SHA-256, SHA-384	
	or SHA-512) defined by the	or SHA-512) defined by the	
	cipher suite in Appendix 11	cipher suite in Sub-appendix 11	
	Part B for the card signature	Part B for the card signature	
	key Card_Sign	key Card_Sign	
3.5.14,	TCS 128 The Generation	TCS 128 The Generation	
TCS 128	1 tachograph application	1 tachograph application	
103_120	performs a digital signature	•	
		performs a digital signature	
	using a padding method	using a padding method	
	compliant with PKCS1 (see	compliant with PKCS1 (see	
2.5.44	Appendix 11 for details).	Sub-appendix 11 for details).	
3.5.14,	TCS_129 The Generation	TCS_129 The Generation	
TCS_129	2 tachograph application	2 tachograph application	
	computes an elliptic curve	computes an elliptic curve	
	based digital signature (see	based digital signature (see	
	Appendix 11 for details).	Sub-appendix 11 for details).	
3.5.15,	(8 th row in the table, 2 nd and 3 rd	(8 th row in the table, 2 nd and 3 rd	
TCS_133	paragraph)	paragraph)	
	128 bytes coded in accordance	128 bytes coded in accordance	
	with Annondiv 11 Dart A for	with Sub-appendix 11 Part A	
	with Appendix 11 Part A for	With Jub-appendix II Fait A	
	Tachograph Generation 1	for Tachograph Generation 1	

	Depending on the colored	Depending on the colored	
	Depending on the selected curve for Tachograph	Depending on the selected	
	curve for Tachograph Generation 2 application (see	curve for Tachograph Generation 2 application (see	
	Appendix 11 Part B).	Sub-appendix 11 Part B).	
3.5.15,	(2 nd indent after the table)	(2 nd indent after the table)	
TCS_134	If the verification of the	If the verification of the	
103_134			
	signature fails, the processing state returned is '6688'. The	signature fails, the processing state returned is '6688'. The	
	verification process is	verification process is	
	described in Appendix 11.	described in Sub-appendix 11.	
3.5.15,	(8 th indent after the table)	(8 th indent after the table)	
TCS_134	If the selected public key	If the selected public key	
165_154	(used to verify the digital	(used to verify the digital	
	signature) has a CHA.LSB	signature) has a CHA.LSB	
	(CertificateHolderAuthorisatio	(CertificateHolderAuthorisatio	
	n.equipmentType) that is not	n.equipmentType) that is not	
	suitable for the digital	suitable for the digital	
	signature verification	signature verification	
	according to Appendix 11, the	according to Sub-appendix 11,	
	processing state returned is	the processing state returned	
	"6985".	is "6985".	
3.5.16	This command is used to verify	This command is used to verify	
	the integrity and authenticity	the integrity and authenticity	
	of the DSRC message and to	of the DSRC message and to	
	decipher the data	decipher the data	
	communicated from a VU to a	communicated from a VU to a	
	control authority or a	control authority or a	
	workshop over the DSRC link.	workshop over the DSRC link.	
	The card derives the	The card derives the	
	encryption key and the MAC	encryption key and the MAC	
	key used to secure the DSRC	key used to secure the DSRC	
	message as described in	message as described in Sub-	
2 5 16	Appendix 11 Part B chapter 13.	appendix 11 Part B chapter 13.	
3.5.16,	(7 th row in the table, 1 st	(7 th row in the table, 1 st	
TCS_138	paragraph)	paragraph)	
	DER-TLV encoded padding- content indicator byte	DER-TLV encoded padding- content indicator byte	
	content indicator byte followed by encrypted	content indicator byte followed by encrypted	
	tachograph payload. For the	tachograph payload. For the	
	padding-content indicator byte	padding-content indicator byte	
	the value '00h' ('no further	the value '00h' ('no further	
	indication' according to	indication' according to	
	ISO/IEC 7816-4:2013 Table 52)	ISO/IEC 7816-4:2013 Table 52)	
	shall be used. For the	shall be used. For the	
	encryption mechanism see	encryption mechanism see	
	Appendix 11, Part B chapter	Sub-appendix 11, Part B	
	13.	chapter 13.	
3.5.16,	(8 th row in the table, 1 st	(8 th row in the table, 1 st	
TCS_138	paragraph)	paragraph)	
	DER-TLV encoded Control	DER-TLV encoded Control	
	Reference Template for	Reference Template for	

	Confidentiality nesting the	,	
	concatenation of the following	concatenation of the following	
	data elements (see Appendix 1	data elements (see Sub-	
	dSRCSecurityData and	appendix 1 dSRCSecurityData	
	Appendix 11 Part B chapter	and Sub-appendix 11 Part B	
	13):	chapter 13):	
3.5.16,	(9 th row in the table, 1 st	(9 th row in the table, 1 st	
TCS_138	paragraph)	paragraph)	
	DER-TLV encoded MAC over	DER-TLV encoded MAC over	
	the DSRC message. For the	the DSRC message. For the	
	MAC algorithm and calculation	MAC algorithm and calculation	
	see Appendix 11, Part B	see Sub-appendix 11, Part B	
	chapter 13.	chapter 13.	

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 3 FOR AETR V0.2 20190112

Point or article	Text Appendix 3	Proposed text for AETR	Comments
TITLE/TABLE	(Title)		
OF	APPENDIX 3. PICTOGRAMS	SUB-APPENDIX 3.	
CONTENTS		PICTOGRAMS	
1	Note: Additional pictogram	Note: Additional pictogram	
	combinations to form printout	combinations to form printout	
	blocks or record identifiers are	blocks or record identifiers are	
	defined in Appendix 4.	defined in Sub-Appendix 4.	

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 4 FOR AETR V0.2 20190112

Point or article	Text Appendix 4	Proposed text for AETR	Comments
TITLE/TABLE OF CONTENTS	(Title) APPENDIX 4. PRINTOUTS	SUB-APPENDIX 4. PRINTOUTS	
2	In this chapter the following format notation conventions have been used: - Characters printed in bold denote plain text to be printed (printing remains in normal characters), - Normal characters denote variables (pictograms or data) to be replaced by their values for printing, - Variable names have been padded with underscores to show the data item length available for the variable, - Dates are specified with a "dd/mm/yyyy" (day, month, year) format. A "dd.mm.yyyy" format may also be used, - The term "card identification" denotes the composition of: the type of card through a card pictograms combination, the card issuing Member State code, a forward slash character and the card number with the replacement index and the renewal index separated with a space:	In this chapter the following format notation conventions have been used: - Characters printed in bold denote plain text to be printed (printing remains in normal characters), - Normal characters denote variables (pictograms or data) to be replaced by their values for printing, - Variable names have been padded with underscores to show the data item length available for the variable, - Dates are specified with a "dd/mm/yyyy" (day, month, year) format. A "dd.mm.yyyy" format may also be used, - The term "card identification" denotes the composition of: the type of card through a card pictograms combination, the card issuing Contracting Party code, a forward slash character and the card number with the replacement index and the renewal index separated with a space:	
2	(in the table) Issuing Member State code	(in the table) Issuing Contracting Party code	
2, PRT_007	Block 2 Type of printout. Block identifier Printout pictogram combination (see App. 3), Speed limiting device setting (Over speeding printout only)	Block 2 Type of printout. Block identifier Printout pictogram combination (see Sub-App. 3), Speed limiting device setting (Over speeding printout only)	
2, PRT_007	Block 4 Vehicle identification. Block identifier	Block 4 Vehicle identification. Block identifier	

	VINI	VINI	
	VIN	VIN	
	Registering Member State and	Registering Contracting Party	
2 DDT 007	VRN	and VRN	
2, PRT_007	Block 8.2	Block 8.2 Card insertion in slot S	
	Card insertion in slot S		
	Record identifier; S = Slot	Record identifier; S = Slot	
	pictogram Vahiala registering Mambar	pictogram	
	Vehicle registering Member State and VRN	Vehicle registering Contracting	
		Party and VRN	
	Vehicle odometer at card	Vehicle odometer at card	
2 DDT 007	insertion Block 12.4	insertion Block 12.4	
2, PRT_007			
	Event and/or Fault record Record identifier	Event and/or Fault record Record identifier	
	Event/fault pictogram, record	Event/fault pictogram, record	
	purpose, date time of start,	purpose, date time of start,	
	Additional event/fault code (if	Additional event/fault code (if	
	any), duration	any), duration	
	Registering Member State &	Registering Contracting Party	
	VRN of vehicle in which the	& VRN of vehicle in which the	
	event or fault occurred	event or fault occurred	
2, PRT_007	Block 17.1	Block 17.1	
2,111_007	Calibration record	Calibration record	
	Record identifier	Record identifier	
	Workshop having performed	Workshop having performed	
	the calibration	the calibration	
	Workshop address	Workshop address	
	Workshop card identification	Workshop card identification	
	Workshop card expiry date	Workshop card expiry date	
	Blank line	Blank line	
	Calibration date + calibration	Calibration date + calibration	
	purpose	purpose	
	VIN	VIN	
	Registering Member State &	Registering Contracting Party	
	VRN	& VRN	
	Characteristic coefficient of	Characteristic coefficient of	
	vehicle	vehicle	
	Constant of the recording	Constant of the control device	
	equipment	Effective circumference of	
	Effective circumference of	wheel tyres	
	wheel tyres	Size of tyres mounted	
	Size of tyres mounted	Speed limiting device setting	
	Speed limiting device setting	Old and new odometer values	
	Old and new odometer values		

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 5 FOR AETR V0.2 20190112

Point or article	Text Appendix 5	Proposed text for AETR	Comments
TITLE/TABLE	(Title)		
OF	APPENDIX 5. DISPLAY	SUB-APPENDIX 5. DISPLAY	
CONTENTS			

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 6 FOR AETR V0.2 20190112

Point or article	Text Appendix 6	Proposed text for AETR	Comments
TITLE/TABLE	(Title)		
OF	APPENDIX 6. FRONT	SUB-APPENDIX 6. FRONT	
CONTENTS	CONNECTOR FOR	CONNECTOR FOR	
	CALIBRATION AND	CALIBRATION AND	
	DOWNLOAD	DOWNLOAD	

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 7 FOR AETR V0.2 20190112

Point or	Text Appendix 7	Proposed text for	Comments
article	Toat appendix /	AETR	
TITLE/TABLE	(Title)		
OF	APPENDIX 7. DATA	SUB-APPENDIX 7. DATA	
CONTENTS	DOWNLOADING PROTOCOLS	DOWNLOADING PROTOCOLS	
1	This appendix specifies the	This Sub-appendix specifies	
	procedures to follow in order	the procedures to follow in	
	to perform the different types	order to perform the different	
	of data download to an	types of data download to an	
	External Storage Medium,	External Storage Medium,	
	together with the protocols	together with the protocols	
	that must be implemented to	that must be implemented to	
	assure the correct data	assure the correct data	
	transfer and the full	transfer and the full	
	compatibility of the downloaded data format to	compatibility of the downloaded data format to	
	allow any controller to inspect these data and be able to	allow any controller to inspect these data and be able to	
	control their authenticity and	control their authenticity and	
	their integrity before analysing	their integrity before analysing	
	them.	them.	
1.1	Data may be downloaded to	Data may be downloaded to	
1.1	an ESM:	an ESM:	
	- from a Vehicle Unit by an	- from a Vehicle Unit by an	
	Intelligent Dedicated	Intelligent Dedicated	
	Equipment (IDE) connected to	Equipment (IDE) connected to	
	the VU,	the VU,	
	- from a tachograph card by an	- from a tachograph card by an	
	IDE fitted with a card interface	IDE fitted with a card interface	
	device (IFD),	device (IFD),	
	- from a tachograph card via a	- from a tachograph card via a	
	vehicle unit by an IDE	vehicle unit by an IDE	
	connected to the VU.	connected to the VU.	
	To give the possibility to verify	To give the possibility to verify	
	the authenticity and integrity	the authenticity and integrity	
	of downloaded data stored on	of downloaded data stored on	
	an ESM, data is downloaded	an ESM, data is downloaded	
	with a signature appended in	with a signature appended in	
	accordance with Appendix 11	accordance with Sub-appendix	
	Common Security	11 Common Security	
	Mechanisms. The source	Mechanisms. The source	
	equipment (VU or card)	equipment (VU or card)	
	identification and its security	identification and its security	
	certificates (Member state	certificates (Contracting Party	
	and equipment) are also	and equipment) are also	
	downloaded. The verifier of	downloaded. The verifier of	
	the data must possess	the data must possess	

independently a trusted European public key. Data downloaded from a VU are signed using Appendix 11 Common Security Mechanisms Part B (Second-generation tachograph system), except when drivers' control is performed by a non EU control authority, using a first generation control card, in which case data are signed using Appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. Similarly, there are two types
Data downloaded from a VU are signed using Appendix 11 Common Security Mechanisms Part B (Second-generation tachograph system), except when drivers' control is performed by a non EU control authority, using a first generation control card, in which case data are signed using Appendix 11 Common Security Mechanisms Part B (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: - Generation 2 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, - Generation 2 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms
are signed using Appendix 11 Common Security Mechanisms Part B (Second-generation tachograph system), except when drivers' control is performed by a non EU control authority, using a first generation control card, in which case data are signed using Appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms
Common Security Mechanisms Part B (Second-generation tachograph system), except when drivers' control is performed by a non EU control authority, using a first generation control card, in which case data are signed using Appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: Generation 2 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, Generation 2 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms
Part B (Second-generation tachograph system), except when drivers' control is performed by a non EU control authority, using a first generation control card, in which case data are signed using Appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A.
tachograph system), except when drivers' control is performed by a non EU control authority, using a first generation control card, in which case data are signed using Appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A.
when drivers' control is performed by a non EU control authority, using a first generation control card, in which case data are signed using Appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: Generation 2 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. Common Security Mechanisms Part B, Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part A. Common Security Mechanisms Part B, Generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, Generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms
control authority, using a first generation control card, in which case data are signed using Appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part A.
control authority, using a first generation control card, in which case data are signed using Appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. EU control authority, using a first generation control card, in which case data are signed using Sub-appendix 11 Common Security Mechanisms Part A (First-generation on Security Mechanisms Part A (First-generation Using Sub-appendix 11 Common Security Mechanisms Part A (First-generation Using Sub-appendix 15 Common Security Mechanisms Part A (First-generation Using Sub-appendix 15 Common Security Mechanisms Part A (First-generation Using Sub-appendix 11 Common Security Mechanisms Part A (First-generation Using Sub-appendix 11 Common Security Mechanisms Part A (First-generation Using Sub-appendix 11 Common Security Mechanisms Part B, - Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providin
generation control card, in which case data are signed using Appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. Girst generation control card, in which case data are signed using Sub-appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Sub-appendix 15 Migration, requirement MIG_015. This Sub-appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part A.
using Appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. using Sub-appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Sub-appendix 15 Migration, requirement MIG_015. This Sub-appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part A.
Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms
(First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: Generation 2 type of VU data download, providing the generation 2 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. Part A (First-generation tachograph system), as requested by Sub-appendix 15 Migration, requirement MIG_015. This Sub-appendix specifies therefore two types of data downloads from the VU: Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part A. Common Security Mechanisms
system), as requested by Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 2 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. tachograph system), as requested by Sub-appendix 15 Migration, requirement MIG_015. This Sub-appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 2 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part A.
Appendix 15 Migration, requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: Generation 2 type of VU data download, providing the generation 2 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. requested by Sub-appendix 15 Migration, requirement MIG_015. This Sub-appendix specifies therefore two types of data downloads from the VU: Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. Common Security Mechanisms
requirement MIG_015. This Appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 2 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. Migration, requirement MIG_015. This Sub-appendix specifies therefore two types of data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms
This Appendix specifies therefore two types of data downloads from the VU: Generation 2 type of VU data download, providing the generation 2 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part A. MIG_015. This Sub-appendix specifies therefore two types of data downloads from the VU: Generation 2 type of VU data download, providing the generation 2 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part A.
therefore two types of data downloads from the VU: Generation 2 type of VU data download, providing the generation 2 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data downloads from the VU: Generation 2 type of VU data download, providing the generation 1 type of VU data downloads from the VU: Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data downloads from the VU: Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data downloads from the VU: Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 2 data structure, signed using Sub-appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 2 data structure, signed using Sub-appendix 11 Common Security Mechanisms
downloads from the VU: - Generation 2 type of VU data download, providing the generation 2 data structure, signed using Appendix 11 Common Security Mechanisms - Generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 type of VU data downloads from the VU: - Generation 2 type of VU data download, providing the generation 1 type of VU data downloads from the VU: - Generation 2 type of VU data download, providing the generation 2 data structure, signed using Sub-appendix 11 Common Security Mechanisms
- Generation 2 type of VU data download, providing the generation 2 data structure, signed using Appendix 11 Common Security Mechanisms - Generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data generation 1 data structure, signed using Appendix 11 Common Security Mechanisms - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. Common Security Mechanisms Common Security Mechanisms
download, providing the generation 2 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. Generation 2 type of VU data download, providing the generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms
generation 2 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 type of VU data generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Fart A. download, providing the generation 1 type of VU data download, providing the generation 1 type of VU data download, providing the signed using Sub-appendix 11 Common Security Mechanisms
signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. generation 2 data structure, signed using Sub-appendix 11 Common Security Mechanisms Sub-appendix 11 Common Security Mechanisms
Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms Fart A. Common Security Mechanisms
Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part B, Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Signed using Sub-appendix 11 Common Security Mechanisms
- Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. Part B, - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms
download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. - Generation 1 type of VU data download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms
generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A. download, providing the generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms
signed using Appendix 11 Common Security Mechanisms Part A. generation 1 data structure, signed using Sub-appendix 11 Common Security Mechanisms
Common Security Mechanisms signed using Sub-appendix 11 Part A. Common Security Mechanisms
Part A. Common Security Mechanisms
Similarly, there are two types Part A.
of data downloads from Similarly, there are two types
second generation driver of data downloads from
cards inserted in a VU, as second generation driver
specified in paragraphs 3 and cards inserted in a VU, as
4 of this Appendix. specified in paragraphs 3 and
4 of this Sub-appendix.
The following acronyms are The following acronyms are
used in this appendix: used in this Sub-appendix:
2.2.6 This paragraph specifies the This paragraph specifies the
content of the data fields of content of the data fields of
the various positive the various positive
response messages. response messages.
Data elements are defined in Data elements are defined in
Appendix 1 data dictionary. Sub-appendix 1 data
dictionary.

2.2.6.1, DDP_029	(Data structure generation 2 (TREP 21 Hex), Comment column.) Member state certificate	(Data structure generation 2 (TREP 21 Hex), Comment column.) Contracting Party certificate	
3.3, DDP_035	(DDP_35, 4 th indent) - Download the other application data EFs (within Tachograph DF) except EF Card_Download. This information is secured with a digital signature, using Appendix 11 Common Security Mechanisms Part A.	(DDP_35, 4th indent) - Download the other application data EFs (within Tachograph DF) except EF Card_Download. This information is secured with a digital signature, using Sub- appendix 11 Common Security Mechanisms Part A.	
3.3, DDP_035	(DDP_35, 9 th indent) - Download the other application data EFs (within Tachograph_G2 DF) except EF Card_Download. This information is secured with a digital signature, using Appendix 11 Common Security Mechanisms Part B.	(DDP_35, 9th indent) - Download the other application data EFs (within Tachograph_G2 DF) except EF Card_Download. This information is secured with a digital signature, using Sub- appendix 11 Common Security Mechanisms Part B.	
3.3.3, DDP_038	(3 rd row in the table) Calculates the hash value over the data content of the selected file using the prescribed hash algorithm in accordance with Appendix 11, part A or B. This command is not an ISO-Command.	(3 rd row in the table) Calculates the hash value over the data content of the selected file using the prescribed hash algorithm in accordance with Sub-appendix 11, part A or B. This command is not an ISO-Command.	

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 8 FOR AETR V0.2 20190112

Point or article	Text Appendix 8	Proposed text for AETR	Comments
TITLE/TABLE	(Title)		
OF	APPENDIX 8. CALIBRATION	SUB-APPENDIX 8.	
CONTENTS	PROTOCOL	CALIBRATION PROTOCOL	
1	This appendix describes how	This Sub-appendix describes	
	data is exchanged between a	how data is exchanged	
	vehicle unit and a tester via	between a vehicle unit and a	
	the K-line which forms part of	tester via the K-line which	
	the calibration interface	forms part of the calibration	
	described in Appendix 6. It	interface described in Sub-	
	also describes control of the	appendix 6. It also describes	
	input / output signal line on	control of the input / output	
	the calibration connector.	signal line on the calibration	
	Establishing K-line	connector.	
	communications is described	Establishing K-line	
	in Section 4 "Communication	communications is described	
	Services".	in Section 4 "Communication	
	This appendix uses the idea of	Services".	
	diagnostic "sessions" to	This Sub-appendix uses the	
	determine the scope of K-line	idea of diagnostic "sessions"	
	control under different	to determine the scope of K-	
	conditions. The default session	line control under different	
	is the	conditions. The default session	
	"StandardDiagnosticSession"	is the	
	where all data can be read	"StandardDiagnosticSession"	
	from a vehicle unit but no data can be written to a vehicle	where all data can be read from a vehicle unit but no data	
	unit.	can be written to a vehicle	
	Selection of the diagnostic	unit.	
	session is described in Section	Selection of the diagnostic	
	5 "Management Services".	session is described in Section	
	This appendix has to be	5 "Management Services".	
	considered as relevant for	This Sub-appendix has to be	
	both generations of VUs and	considered as relevant for	
	of workshop cards, in	both generations of VUs and	
	compliance with the	of workshop cards, in	
	interoperability requirements	compliance with the	
	laid down in this Regulation.	interoperability requirements	
		laid down in this Agreement.	
3.1,	(CPR_004 2 nd indent)	- The 2nd column includes the	
CPR_004	- The 2nd column includes the	section number in this Sub-	
	section number in this	appendix where of service is	
	appendix where of service is	further defined.	
	further defined.		
6.1.3,	(CPR_053 2 nd indent)		
CPR_053			

	- The 2nd column (Data element) specifies the data element of Appendix 1 on which the recordDataIdentifier is based (transcoding is sometimes necessary).	- The 2nd column (Data element) specifies the data element of Sub-appendix 1 on which the recordDataIdentifier is based (transcoding is sometimes necessary).	
8.2, CPR 078	(Table 42, 2 nd column)		
5.75	Code Page (as defined in Appendix 1)	Code Page (as defined in Subappendix 1)	
	Vehicle Registration Number (as defined in Appendix 1)	Vehicle Registration Number (as defined in Sub-appendix 1)	

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 9 FOR AETR V0.2 20190112

Point or article	Text Appendix 9	Proposed text for AETR	Comments
TITLE/TABLE OF CONTENTS			To be updated as needed, according to the validated changes
1.1	(1st Paragraph) The EC type approval for a recording equipment (or component) or a tachograph card is based on: - a security certification, based on Common Criteria specifications, against a security target fully compliant with Appendix 10 to this Annex), - a functional certification performed by a Member State authority certifying that the item tested fulfils the requirements of this Annex in terms of functions performed, measurement accuracy and environmental characteristics, - an interoperability certifying that the recording equipment (or tachograph card) is fully interoperable with the necessary tachograph card (or recording equipment) models (see Chapter 8 of this Annex).	(1st Paragraph) The EC type approval for a control device (or component) or a tachograph card is based on: - a security certification, based on Common Criteria specifications, against a security target fully compliant with Sub-appendix 10 to this Annex), - a functional certification performed by a Contracting Party authority certifying that the item tested fulfils the requirements of this Appendix in terms of functions performed, measurement accuracy and environmental characteristics, - an interoperability certifying that the competent body certifying that the control device (or tachograph card) is fully interoperable with the necessary tachograph card (or control device) models (see Chapter 8 of this Annex).	

This Appendix specifies which tests, as a minimum, must be performed by a Member State authority during the functional tests, and which tests, as a minimum, must be performed by the competent body during the interoperability tests. Procedures to follow to carry out the tests or the type of tests are not specified further. The security certification aspects are not covered by this Appendix. If some tests requested for type approval are performed during the security evaluation and certification process, then these tests do not need to be performed again. In this case, only the results of these security tests may be inspected. For information, the requirements expected to be tested (or closely related to tests expected to be performed) during the security certification, are marked with a "*" in this Appendix. The numbered requirements refer to the Annex corpus, while the other requirements refer to the other appendixes (e.g. PIC 001 refers to requirement PIC_001 of Appendix 3 Pictograms). This Appendix considers separately the type approval of the motion sensor, of the vehicle unit, and of the external GNSS facility as components of

This Sub-appendix specifies which tests, as a minimum, must be performed by a **Contracting Party authority** during the functional tests, and which tests, as a minimum, must be performed by the competent body during the interoperability tests. Procedures to follow to carry out the tests or the type of tests are not specified further. The security certification aspects are not covered by this Sub-appendix. If some tests requested for type approval are performed during the security evaluation and certification process, then these tests do not need to be performed again. In this case, only the results of these security tests may be inspected. For information, the requirements expected to be tested (or closely related to tests expected to be performed) during the security certification, are marked with a "*" in this Sub-appendix. The numbered requirements refer to the Appendix corpus, while the other requirements refer to the other sub-appendixes (e.g. PIC 001 refers to requirement PIC 001 of Sub-appendix 3 Pictograms). This Sub-appendix considers separately the type approval of the motion sensor, of the vehicle unit, and of the external GNSS facility as

7, 2.1	Annex 1C, chapter 4.1 'Visible data', 234)	Appendix 1C, chapter 4.1 'Visible data', 234)	
4, 2.1	[Colour]	on the front page of the card. [Colour]	
	numbered items which appear on the front page of the card.	numbered items which appear	
	an explanation of the	an explanation of the	
	contain:	contain:	
	The reverse page shall	The reverse page shall	
	data', 232)	'Visible data', 232)	
4, 2.1	Annex 1C, chapter 4.1 'Visible	Appendix 1C, chapter 4.1	
4, 2.1	[Enumeration]	12 yellow stars. [Enumeration]	
	rectangle and encircled by 12 yellow stars.	blue rectangle and encircled by	
	printed in negative in a blue	card, printed in negative in a	
	Member State issuing the card,	Contracting Party issuing the	
	the distinguishing sign of the	the distinguishing sign of the	
	The front page shall contain:	The front page shall contain:	
	data', 229)	'Visible data', 229)	
.,	Annex 1C, chapter 4.1 'Visible	Appendix 1C, chapter 4.1	
4, 2.1	[Sign]	[Sign]	
	(optional).	(optional).	
	State issuing the card	the name of the Contracting Party issuing the card	
	The front page shall contain: the name of the Member	The front page shall contain:	
	data', 228)	'Visible data', 228)	
	Annex 1C, chapter 4.1 'Visible	Appendix 1C, chapter 4.1	
4, 2.1	[Member State name]	[Contracting Party name]	
	of the card.	the type of the card.	
	the card, according to the type	issuing the card, according to	
	of the Member State issuing	of the Contracting Party	
	official language or languages	official language or languages	
	printed in capital letters in the	printed in capital letters in the	
	card" or "Company card"	card" or "Company card"	
	"Control card" or "Workshop	"Control card" or "Workshop	
	the words "Driver card" or	the words "Driver card" or	
	The front page shall contain:	The front page shall contain:	
	data', 227)	'Visible data', 227)	
,	Annex 1C, chapter 4.1 'Visible	Appendix 1C, chapter 4.1	
4, 2.1	[Designator]	[Designator]	
	used in this Appendix:	used in this Sub-appendix:	
1.2	The following references are	The following references are	
	vehicle unit and vice versa.		
	done together with the		
	(or external GNSS facility) is	and vice versa.	
	test of the motion sensor	together with the vehicle unit	
	indicated. The functional	external GNSS facility) is done	
	components will be	test of the motion sensor (or	
	other compatible	be indicated. The functional	
	certificate in which the	compatible components will	
	own type approval	certificate in which the other	
	Each component will get its	get its own type approval	
	the recording equipment.	device. Each component will	
	the recording equipment	components of the control	

	Table and because the Hills	Talah a sasah sasah ahali ba	
	Tachograph cards shall be	Tachograph cards shall be	
	printed with the following	printed with the following	
	background predominant	background predominant	
	colours:	colours:	
	- driver card: white,	- driver card: white,	
	- workshop card: red,	- workshop card: red,	
	- control card: blue,	- control card: blue,	
	- company card: yellow.	- company card: yellow.	
4, 2.1	[Security]	[Security]	
	Annex 1C, chapter 4.1 'Visible	Appendix 1C, chapter 4.1	
	data', 235)	'Visible data', 235)	
	Tachograph cards shall bear at	Tachograph cards shall bear at	
	least the following features for	least the following features for	
	protection of the card body	protection of the card body	
	against counterfeiting and	against counterfeiting and	
	tampering:	tampering:	
	- a security design background	- a security design background	
	with fine guilloche patterns	with fine guilloche patterns	
	and rainbow printing,	and rainbow printing,	
	- at least one two-coloured	- at least one two-coloured	
	microprint line.	microprint line.	
4, 2.1	[Markings]	[Markings]	
	Annex 1C, chapter 4.1 'Visible	Appendix 1C, chapter 4.1	
	data', 236)	'Visible data', 236)	
	Member States may add	Contracting Parties may add	
	colours or markings, such as	colours or markings, such as	
	national symbols and security	national symbols and security	
	features.	features.	
4, 2.2	[Durability]	[Durability]	
	Annex 1C, chapter 4.4	Appendix 1C, chapter 4.4	
	'Environmental and electrical	(For the consense) and all exists of	
	Lifviroinnental and electrical	'Environmental and electrical	
	specifications', 241)	specifications', 241)	
	specifications', 241) Tachograph cards shall be	specifications', 241) Tachograph cards shall be	
	specifications', 241) Tachograph cards shall be capable of operating correctly	specifications', 241) Tachograph cards shall be capable of operating correctly	
	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used	
	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and	
<i>A A</i> 1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications.	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications.	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity]	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity]	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241)	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241)	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in AETR	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in Community territory and at	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in AETR territory and at least in the	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in Community territory and at least in the temperature range	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in AETR	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in Community territory and at	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in AETR territory and at least in the	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in Community territory and at least in the temperature range	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in AETR territory and at least in the temperature range -25°C to	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in Community territory and at least in the temperature range -25°C to +70°C with occasional	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in AETR territory and at least in the temperature range -25°C to +70°C with occasional peaks of	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in Community territory and at least in the temperature range -25°C to +70°C with occasional peaks of up to +85°C,	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in AETR territory and at least in the temperature range -25°C to +70°C with occasional peaks of up to +85°C, "occasional"	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in Community territory and at least in the temperature range -25°C to +70°C with occasional peaks of up to +85°C, "occasional" meaning not more than 4 hours each time	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in AETR territory and at least in the temperature range -25°C to +70°C with occasional peaks of up to +85°C, "occasional" meaning not more than 4 hours each time and not over	
4, 4.1	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in Community territory and at least in the temperature range -25°C to +70°C with occasional peaks of up to +85°C, "occasional" meaning not	specifications', 241) Tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications. [Temperature and humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 241) Tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in AETR territory and at least in the temperature range -25°C to +70°C with occasional peaks of up to +85°C, "occasional" meaning not more than 4	

	T		
	The Tachograph cards are	The Tachograph cards are	
	exposed in consecutive steps	exposed in consecutive steps	
	to the following temperatures	to the following temperatures	
	and humidities for the given	and humidities for the given	
	time. After each step the	time. After each step the	
	Tachograph cards are tested	Tachograph cards are tested	
	for electrical functionality.	for electrical functionality.	
	1. Temperature of – 20 °C for 2	1. Temperature of – 20 °C for 2	
	h.	h.	
	2. Temperature of +/- 0 °C for 2	2. Temperature of +/- 0 °C for 2	
	h.	h.	
	3. Temperature of + 20 °C, 50 %	3. Temperature of + 20 °C, 50 %	
	RH, for 2 h.	RH, for 2 h.	
	4. Temperature of + 50 °C, 50 %	4. Temperature of + 50 °C, 50 %	
	RH, for 2 h.	RH, for 2 h.	
	5. Temperature of + 70 °C, 50 %	5. Temperature of + 70 °C, 50 %	
	RH, for 2 h.	RH, for 2 h.	
	The temperature is increased	The temperature is increased	
	intermittently to + 85 °C, 50 %	intermittently to + 85 °C, 50 %	
	RH, for 60 min.	RH, for 60 min.	
	6. Temperature of + 70 °C, 85 %	6. Temperature of + 70 °C, 85 %	
	RH, for 2 h.	RH, for 2 h.	
	The temperature is	The temperature is	
	increased intermittently to +	increased intermittently to +	
	85 °C, 85 % RH, for 30 min.	85 °C, 85 % RH, for 30 min.	
4, 4.1	[Humidity]	[Humidity]	
	Annex 1C, chapter 4.4	Appendix 1C, chapter 4.4	
	'Environmental and electrical	'Environmental and electrical	
	specifications', 242)	specifications', 242)	
	Tachograph cards shall be	Tachograph cards shall be	
	capable of operating correctly	capable of operating correctly	
	in the humidity range 10% to	in the humidity range 10% to	
	90%.	90%.	
4, 4.1	[Electromagnetic compatibility	[Electromagnetic compatibility	
	- EMC]	- EMC]	
	Annex 1C, chapter 4.4	Appendix 1C, chapter 4.4	
	'Environmental and electrical	'Environmental and electrical	
	specifications' 244)	specifications' 244)	
	During operation, Tachograph	During operation, Tachograph	
	cards shall conform to ECE R10	cards shall conform to ECE R10	
	related to electromagnetic	related to electromagnetic	
	compatibility.	compatibility.	
4, 4.1	[Static electricity]	[Static electricity]	
	Annex 1C, chapter 4.4	Appendix 1C, chapter 4.4	
	'Environmental and electrical	'Environmental and electrical	
	specifications', 244)	specifications', 244)	
	During operation, Tachograph	During operation, Tachograph	
	cards shall be protected	cards shall be protected	
	against electrostatic	against electrostatic	
	discharges.	discharges.	
	Tachograph cards must	Tachograph cards must	
	conform to standard	conform to standard	

	ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.4] Static electricity [9.4.1] Contact IC cards Test voltage: 4000 V.	ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.4] Static electricity [9.4.1] Contact IC cards Test voltage: 4000 V.	
4, 7.2	Test at least once each error message (as specified in Appendix 2) for each command Test at least once every generic error (except '6400' integrity errors checked during security certification)	Test at least once each error message (as specified in Subappendix 2) for each command Test at least once every generic error (except '6400' integrity errors checked during security certification)	
4, 8.1	Annex 1C, chapter 4.1 'Visible data', 230) The front page shall contain: information specific to the card issued.	Appendix 1C, chapter 4.1 'Visible data', 230) The front page shall contain: information specific to the card issued.	
4, 8.1	Annex 1C, chapter 4.1 'Visible data', 231) The front page shall contain: dates using a "dd/mm/yyyy" or "dd.mm.yyyy" format (day, month, year).	Appendix 1C, chapter 4.1 'Visible data', 231) The front page shall contain: dates using a "dd/mm/yyyy" or "dd.mm.yyyy" format (day, month, year).	
4, 8.1	Annex 1C, chapter 4.1 'Visible data', 235) Tachograph cards shall bear at least the following features for protection of the card body against counterfeiting and tampering: - in the area of the photograph, the security design background and the photograph shall overlap.	Appendix 1C, chapter 4.1 'Visible data', 235) Tachograph cards shall bear at least the following features for protection of the card body against counterfeiting and tampering: - in the area of the photograph, the security design background and the photograph shall overlap.	
6, 3.3	Appendix 14	Sub-appendix 14	
7, 2.3	The printer shall support characters specified in Appendix 1 Chapter 4 "Character sets".	The printer shall support characters specified in Subappendix 1 Chapter 4 "Character sets".	

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 10 FOR AETR V0.2 20190116

Point or article	Text Appendix 10	Proposed text for AETR	Comments
TITLE/TABLE	(Title)		
OF	APPENDIX 10. SECURITY	SUB-APPENDIX 10. SECURITY	
CONTENTS	REQUIREMENTS	REQUIREMENTS	
1 st	This appendix specifies the IT	This Sub-appendix specifies	
paragraph	security requirements for the	the IT security requirements	
	smart tachograph system	for the smart tachograph	
	components (second-	system components (second-	
	generation tachograph).	generation tachograph).	
		_	_

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 11 FOR AETR V0.2 20190112

Point or article	Text Appendix 11	Proposed text for AETR	Comments
TITLE/TABLE	(Title)		
OF	APPENDIX 11. COMMON	SUB-APPENDIX 11. COMMON	
CONTENTS	SECURITY MECHANISMS	SECURITY MECHANISMS	
Table of		(to be updated after having	
contents		applied all the changes)	
Preamble	This Appendix specifies the	This Sub-appendix specifies	
	security mechanisms ensuring	the security mechanisms	
	- mutual authentication	ensuring	
	between different	- mutual authentication	
	components of the	between different	
	tachograph system.	components of the	
	- confidentiality,	tachograph system.	
	integrity, authenticity and/or	- confidentiality,	
	non-repudiation of data	integrity, authenticity and/or	
	transferred between different	non-repudiation of data	
	components of the	transferred between different	
	tachograph system or	components of the	
	downloaded to external	tachograph system or	
	storage media.	downloaded to external	
	This Assessment of the second	storage media.	
	This Appendix consists of two	This Cub appared to some interest	
	parts. Part A defines the	This Sub-appendix consists of	
	security mechanisms for the	two parts. Part A defines the	
	first-generation tachograph	security mechanisms for the	
	system (digital tachograph). Part B defines the security	first-generation tachograph	
	mechanisms for the second-	system (digital tachograph). Part B defines the security	
	generation tachograph system	mechanisms for the second-	
	(smart tachograph).	generation tachograph system	
	(Sinart tachograph).	(smart tachograph).	
	The mechanisms specified in		
	Part A of this Appendix shall	The mechanisms specified in	
	apply if at least one of the	Part A of this Sub-appendix	
	components of the	shall apply if at least one of	
	tachograph system involved in	the components of the	
	a mutual authentication	tachograph system involved in	
	and/or data transfer process is	a mutual authentication	
	of the first generation.	and/or data transfer process is	
	The mechanisms specified in	of the first generation.	
	Part B of this Appendix shall	The mechanisms specified in	
	apply if both components of	Part B of this Sub-appendix	
	the tachograph system	shall apply if both components	
	involved in the mutual	of the tachograph system	
	authentication and/or data	involved in the mutual	

	tuenefer musees f the	and and adding and for the	
	transfer process are of the	authentication and/or data	
	second generation.	transfer process are of the	
		second generation.	
	Appendix 15 provides more	Cub amandin 45	
	information regarding the use	Sub-appendix 15 provides	
	of first generation	more information regarding	
	components in combination	the use of first generation	
	with second-generation components.	components in combination with second-generation	
	components.	components.	
1.1	The following references	The following references	
1.1		are used in this Sub-	
	are used in this Appendix:		
		appendix:	
1.2	The following notations and	The following notations and	
	abbreviated terms are used	abbreviated terms are used	
	in this Appendix:	in this Sub-appendix:	
3.1.1,	RSA keys shall be generated	RSA keys shall be generated	
CSA_006	through three functional	through three functional	
	hierarchical levels:	hierarchical levels:	
	- European level,	- Root level,	
	- Member State level,	- National level,	
	- Equipment level.	- Equipment level.	
3.1.1,	CSM_007 At European	CSM_007 At root level, a	
CSA_007	level, a single European key	single root key pair (EUR.SK	
_	pair (EUR.SK and EUR.PK)	and EUR.PK) shall be	
	shall be generated. The	generated. The root private	
	European private key shall	key shall be used to certify	
	be used to certify the	the Contracting Parties	
	Member States public keys.	public keys. Records of all	
	Records of all certified keys	certified keys shall be kept.	
	shall be kept. These tasks	These tasks shall be	
	shall be handled by a	handled by a Root	
	European Certification	Certification Authority,	
	Authority, under the	under the authority and	
	authority and responsibility	responsibility of the	
	of the European	European Commission.	
	Commission.		
3.1.1,	CSM_008 At Member State	CSM_008 At National level,	
CSM_008	level, a Member State key	a Contracting Party key pair	
	pair (MS.SK and MS.PK)	(MS.SK and MS.PK) shall be	
	shall be generated.	generated. Contracting	
	Member States public keys	Parties public keys shall be	
	shall be certified by the	certified by the Root	
	European Certification	Certification Authority. The	
	1	-	
	Authority. The Member	Contracting Party private	
	State private key shall be	key shall be used to certify	
	used to certify public keys	public keys to be inserted in	
	to be inserted in equipment	equipment (vehicle unit or	

	(vehicle unit or tachograph	tachograph card). Records	
	card). Records of all	of all certified public keys	
	certified public keys shall	shall be kept with the	
	be kept with the	identification of the	
	identification of the	equipment to which it is	
	equipment to which it is	intended. These tasks shall	
	intended. These tasks shall	be handled by a	
	be handled by a Member	Contracting Party	
	State Certification	Certification Authority. A	
	Authority. A Member State	Contracting Party may	
	may regularly change its	regularly change its key	
	key pair.	pair.	
3.1.1,	CSM_009 At equipment	CSM_009 At equipment	
CSM_009	level, one single key pair	level, one single key pair	
	(EQT.SK and EQT.PK) shall	(EQT.SK and EQT.PK) shall	
	be generated and inserted	be generated and inserted	
	in each equipment.	in each equipment.	
	Equipment public keys shall	Equipment public keys shall	
	be certified by a Member	be certified by a	
	State Certification	Contracting Party	
	Authority. These tasks may	Certification Authority.	
	be handled by equipment	These tasks may be	
	manufacturers, equipment	handled by equipment	
	personalisers or Member State authorities. This key	manufacturers, equipment personalisers or	
	pair is used for	Contracting Party	
	authentication, digital	authorities. This key pair is	
	signature and	used for authentication,	
	encipherement services	digital signature and	
	Chaipher ement services	encipherement services	
3.1.1,	Image in CSM 010	New image (see at the end	
CSM_010		of this document)	
3.1.2,	CSM 011 For the purpose	CSM 011 For the purpose	
CSM_011	of equipment testing	of equipment testing	
	(including interoperability	(including interoperability	
	tests) the European	tests) the Root Certification	
	Certification Authority shall	Authority shall generate a	
	generate a different single	different single root test	
	European test key pair and	key pair and at least two	
	at least two Member State	Contracting Party test key	
	test key pairs, the public	pairs, the public keys of	
	keys of which shall be	which shall be certified with	
	certified with the European	the root private test key.	
	private test key.	Manufacturers shall insert,	
	Manufacturers shall insert,	in equipment undergoing	
	in equipment undergoing	type approval tests, test	
	type approval tests, test	keys certified by one of	

	keys certified by one of	these Contracting Party	
	these Member State test	test keys.	
	keys.		
3.1.3	The confidentiality of the	The confidentiality of the	
	three Triple DES keys	three Triple DES keys	
	described below shall be	described below shall be	
	appropriately maintained	appropriately maintained	
	during generation,	during generation,	
	transport (if any) and	transport (if any) and	
	storage.	storage.	
	In order to support	In order to support	
	tachograph components	tachograph components	
	compliant with ISO 16844,	compliant with ISO 16844,	
	the European Certification	the Root Certification	
	Authority and the Member	Authority and the	
	State Certification	Contracting Party	
	Authorities shall, in	Certification Authorities	
	addition, ensure the	shall, in addition, ensure	
	following:	the following:	
3.1.3,	CSM_036 The European	CSM_036 The Root	
CSM_036	Certification authority shall	Certification authority shall	
	generate KmVU and KmWC,	generate KmVU and KmWC,	
	two independent and	two independent and	
	unique Triple DES keys, and	unique Triple DES keys, and	
	generate Km as : Km =	generate Km as : Km =	
	KmVU XOR KmWC . The	KmVU XOR KmWC . The	
	European Certification Authority shall forward	Root Certification Authority	
	these keys, under	shall forward these keys, under appropriately	
	appropriately secured	secured procedures, to	
	procedures, to Member	Contracting Parties	
	States Certification	Certification Authorities at	
	Authorities at their request.	their request.	
3.1.3,	CSM_037 Member States	CSM_037 Contracting	
CSM_037	Certification Authorities	Parties Certification	
	shall:	Authorities shall:	
	- use Km to encrypt	- use Km to encrypt	
	motion sensor data	motion sensor data	
	requested by motion	requested by motion	
	sensor manufacturers (data	sensor manufacturers (data	
	to be encrypted with Km is	to be encrypted with Km is	
	defined in ISO 16844-3),	defined in ISO 16844-3),	
	- forward KmVU to	 forward KmVU to 	
	vehicle unit manufacturers,	vehicle unit manufacturers,	
	under appropriately	under appropriately	
	secured procedures, for	secured procedures, for	
	insertion in vehicle units,	insertion in vehicle units,	

	- ensure that KmWC	- ensure that KmWC	
	will be inserted in all	will be inserted in all	
	workshop cards	workshop cards	
	(SensorInstallationSecData	(SensorInstallationSecData	
	in Sensor_Installation_Data	in Sensor_Installation_Data	
	elementary file) during card	elementary file) during card	
	personalisation.	personalisation.	
3.3.1,	CSM_017, Notes	CSM 017, Notes	
CSM_017	3. The "Certificate Holder	3. The "Certificate Holder	
	Authorisation" (CHA) is	Authorisation" (CHA) is	
	used to identify the rights	used to identify the rights	
	of the certificate holder. It	of the certificate holder. It	
	consists of the Tachograph	consists of the Tachograph	
	Application ID and of the	Application ID and of the	
	type of equipment to which	type of equipment to which	
	the certificate is intended	the certificate is intended	
	(according to	(according to	
		EquipmentType data	
	EquipmentType data		
	element, '00' for a Member	element, '00' for a	
2.2.4	State).	Contracting Party).	
3.3.1,	CSM_017, Notes	CSM_017, Notes	
CSM_017	5.1 In the first case, the	5.1 In the first case, the	
	manufacturer will send the	manufacturer will send the	
	equipment identification	equipment identification	
	with the public key to its	with the public key to its	
	Member State authority for	Contracting Party authority	
	certification. The certificate	for certification. The	
	will then contain the	certificate will then contain	
	equipment identification,	the equipment	
	and the manufacturer must	identification, and the	
	ensure that keys and	manufacturer must ensure	
	certificate are inserted in	that keys and certificate are	
	the intended equipment.	inserted in the intended	
	The Key identifier has the	equipment. The Key	
	form shown above.	identifier has the form	
	In the later case, the	shown above.	
	manufacturer must	In the later case, the	
	uniquely identify each	manufacturer must	
	certificate request and send	uniquely identify each	
	this identification with the	certificate request and send	
	public key to its Member	this identification with the	
	State authority for	public key to its Contracting	
	certification. The certificate	Party authority for	
	will contain the request	certification. The certificate	
	identification. The		
	manufacturer must feed	will contain the request	
		identification. The	
	back its Member State	manufacturer must feed	

		1 1 2 2 2 2 2 2	
	authority with the	back its Contracting Party	
	assignment of key to	authority with the	
	equipment (i.e. certificate	assignment of key to	
	request identification,	equipment (i.e. certificate	
	equipment identification)	request identification,	
	after key installation in the	equipment identification)	
	equipment. The key	after key installation in the	
	identifier has the following	equipment. The key	
	form:	identifier has the following	
		form:	
3.3.1,	CSM_017, Notes	CSM_017, Notes	
CSM_017	5.2 The key serial number is	5.2 The key serial number is	
	used to distinguish the	used to distinguish the	
	different keys of a Member	different keys of a	
	State, in the case the key is	Contracting Party, in the	
	changed.	case the key is changed.	
4	Mutual authentication	Mutual authentication	
	between cards and VUs is	between cards and VUs is	
	based on the following	based on the following	
	principle :	principle :	
	Each party shall	Each party shall	
	demonstrate to the other	demonstrate to the other	
	that it owns a valid key pair,	that it owns a valid key pair,	
	the public key of which has	the public key of which has	
	been certified by a Member	been certified by a	
	State certification	Contracting Party	
	authority, itself being	certification authority, itself	
	certified by the European	being certified by the Root	
	certification authority.	certification authority.	
	Demonstration is made by	Demonstration is made by	
	signing with the private key	signing with the private key	
	a random number sent by	a random number sent by	
	the other party, who must	the other party, who must	
		recover the random	
	recover the random number sent when	number sent when	
	verifying this signature.	verifying this signature.	
	The mechanism is triggered	The mechanism is triggered	
	at card insertion by the VU.	at card insertion by the VU.	
	It starts with the exchange	It starts with the exchange of certificates and	
	of certificates and		
	unwrapping of public keys,	unwrapping of public keys,	
	and ends with the setting of	and ends with the setting of	
4 CCN4 030	a session key.	a session key.	
4, CSM_020	CSM_020 The following protocol shall be used (arrows	CSM_020 The following protocol shall be used (arrows	
	indicate commands and data	indicate commands and data	
	exchanged (see Appendix 2)):	exchanged (see Sub-appendix	
	(2)):	
		,,	

C 0014 000	CCNA 022 TI I I III	CCLA COO TI I I III	
6, CSM_032	CSM_032 The Intelligent	CSM_032 The Intelligent	
	Dedicated Equipment (IDE)	Dedicated Equipment (IDE)	
	stores data received from an	stores data received from an	
	equipment (VU or card) during	equipment (VU or card) during	
	one download session within	one download session within	
	one physical data file. This file	one physical data file. This file	
	must contain the certificates	must contain the certificates	
	MSi.C and EQT.C. The file	MSi.C and EQT.C. The file	
	contains digital signatures of	contains digital signatures of	
	data blocks as specified in	data blocks as specified in	
	Appendix 7 Data Downloading	Sub-appendix 7 Data	
	Protocols.	Downloading Protocols.	
6.2,	CSM_035 Data signature	CSM 035 Data signature	
CSM_035	verification on downloaded	verification on downloaded	
	data shall follow the signature	data shall follow the signature	
	scheme with appendix defined	scheme with appendix defined	
	in reference [PKCS1] with the	in reference [PKCS1] with the	
	SHA-1 hash function.	SHA-1 hash function.	
	The European public key	The root public key EUR.PK	
	EUR.PK needs to be known	needs to be known	
	independently (and trusted)		
	by the verifier.	independently (and trusted)	
7.4	•	by the verifier.	
7.1	The following references	The following references	
	are used in this part of this	are used in this part of this	
	Appendix.	Sub-appendix.	
7.2	The following notations and	The following notations and	
	abbreviated terms are used	abbreviated terms are used	
	in this Appendix:	in this Sub-appendix:	
7.3	The definitions of terms used	The definitions of terms used	
	in this Appendix are included	in this Sub-appendix are	
	in section I of Annex 1C.	included in section I of	
	and desired a service of the service	Appendix 1C.	
8.1, CSM_43	Notes, 1 st bullet point	Notes, 1 st bullet point	
, , , , , , , , , , , , , , , , , , ,	 Properly speaking, 	Properly speaking, data is	
	data is transmitted	transmitted from a vehicle	
	from a vehicle unit to	unit to a remote interrogator	
	a remote interrogator	under the control of a control	
	under the control of a	officer, using a remote	
	control officer, using a	communication facility that	
	remote	may be internal or external to	
	communication		
		the VU, see Sub-appendix 14. However, the remote	
	facility that may be		
	internal or external to	interrogator sends the	
	the VU, see Appendix	received data to a control card	
	14. However, the	for decryption and validation	
	remote interrogator	of authenticity. From a	
	sends the received	security point of view, the	
	data to a control card	remote communication facility	
	for decryption and	and the remote interrogator	
	validation of	are fully transparent.	
	authenticity. From a		

	security point of view,		
	the remote		
	communication facility and the		
	facility and the remote interrogator		
	are fully transparent.		
8.2.4,	Note: ECC keys sizes of 512	Note: ECC keys sizes of 512	
CSM_50	bits and 521 bits are	bits and 521 bits are	
33.11_33	considered to be equal in	considered to be equal in	
	strength for all purposes	strength for all purposes	
	within this Appendix.	within this Sub-appendix.	
9.1.1	Note: the keys described in	Note: the keys described in	
	this section are used for	this section are used for	
	mutual authentication and	mutual authentication and	
	secure messaging between	secure messaging between	
	vehicle units and tachograph	vehicle units and tachograph	
	cards and between vehicle	cards and between vehicle	
	units and external GNSS	units and external GNSS	
	facilities. These processes are	facilities. These processes are	
	described in detail in chapters	described in detail in chapters	
	Error! Reference source	Error! Reference source	
	not found. and Error!	not found. and Error!	
	Reference source not	Reference source not	
	found. of this Appendix.	found. of this Sub-appendix.	
9.1.1,	CSM_51 Within the	CSM_51 Within the	
CSM_51	European Smart Tachograph	Smart Tachograph system,	
	system, ECC key pairs and	ECC key pairs and	
	corresponding certificates	corresponding certificates	
	shall be generated and	shall be generated and	
	managed through three	managed through three	
	functional hierarchical levels:	functional hierarchical levels:	
	- European level,	- Root level,	
	- Member State level,	- National level,	
0.1.1	- Equipment level.	- Equipment level.	
9.1.1,	CSM_52 Within the	CSM_52 Within the	
CSM_52	entire European Smart	entire Smart Tachograph	
	Tachograph system, public and private keys and	system, public and private keys and certificates shall be	
	certificates shall be generated,	generated, managed and	
	managed and communicated	communicated using	
	using standardized and secure	standardized and secure	
	methods.	methods.	
9.1.2 title	European Level	Root Level	
9.1.2,	CSM_53 At European	CSM_53 At Root level, a	
CSM_53	level, a single unique ECC key	single unique ECC key pair	
	pair designated as EUR shall	designated as EUR shall be	
	be generated. It shall consist	generated. It shall consist of a	
	of a private key (EUR.SK) and a	private key (EUR.SK) and a	
	public key (EUR.PK). This key	public key (EUR.PK). This key	
	pair shall form the root key	pair shall form the root key	
	pair of the entire European	pair of the entire Smart	

	I	I	
	Smart Tachograph PKI. This	Tachograph PKI. This task shall	
	task shall be handled by a	be handled by a European	
	European Root Certificate	Root Certificate Authority	
	Authority (ERCA), under the	(ERCA), under the authority	
	authority and responsibility of	and responsibility of the	
	the European Commission.	European Commission.	
9.1.2,	CSM_54 The ERCA shall	CSM_54 The ERCA shall	
CSM_54	use the European private key	use the root private key to	
	to sign a (self-signed) root	sign a (self-signed) root	
	certificate of the European	certificate of the root public	
	public key, and shall	key, and shall communicate	
	communicate this European	this root certificate to all	
	root certificate to all Member	Contracting Parties or	
	States.	Member States.	
9.1.2,	CSM 55 The ERCA shall	CSM 55 The ERCA shall	
CSM_55	use the European private key	use the root private key to	
C3IVI_33	to sign the certificates of the	sign the certificates of the	
	Member States public keys		
		Contracting Parties public	
	upon request. The ERCA shall	keys upon request. The ERCA	
	keep records of all signed	shall keep records of all signed	
	Member State public key	Contracting Party public key	
	certificates.	certificates.	
9.1.2,	CSM_56 As shown in	CSM_56 As shown in	
CSM_56	Figure 1 in section 9.1.7, the	Figure 1 in section 9.1.7, the	
	ERCA shall generate a new	ERCA shall generate a new	
	European root key pair every	root key pair every 17 years.	
	17 years. Whenever the ERCA	Whenever the ERCA generates	
	generates a new European	a new root key pair, it shall	
	root key pair, it shall create a	create a new self-signed root	
	new self-signed root	certificate for the new root	
	certificate for the new	public key. The validity period	
	European public key. The	of a root certificate shall be 34	
	validity period of a European	years plus 3 months.	
	root certificate shall be 34	, ,	
	years plus 3 months.		
9.1.2,	CSM_57 Before	CSM 57 Before	
CSM_57	generating a new European	generating a new root key	
	root key pair, the ERCA shall	pair, the ERCA shall conduct	
	conduct an analysis of the	an analysis of the	
	cryptographic strength that is	cryptographic strength that is	
	needed for the new key pair,	needed for the new key pair,	
	given it should stay secure for	given it should stay secure for	
	the next 34 years. If found	the next 34 years. If found	
	necessary, the ERCA shall	necessary, the ERCA shall	
	switch to a cipher suite that is	switch to a cipher suite that is	
	stronger than the current one,	stronger than the current one,	
	_	_	
0.1.2	as specified in CSM_50.	as specified in CSM_50.	
9.1.2,	CSM_58 Whenever it	CSM_58 Whenever it	
CSM_58	generates a new European	generates a new root key pair,	
	root key pair, the ERCA shall	the ERCA shall create a link	
	create a link certificate for the	certificate for the new root	
	new European public key and	public key and sign it with the	

	1 1 1 1 1		
	sign it with the previous	previous root private key. The	
	European private key. The	validity period of the link	
	validity period of the link	certificate shall be 17 years	
	certificate shall be 17 years	plus 3 months. This is shown	
	plus 3 months. This is shown in Figure 1 in section 9.1.7 as	in Figure 1 in section 9.1.7 as well.	
	well.	weii.	
9.1.2,	CSM 61 At Member	CSM 61 At National	
CSM_61	State level, all Member States	level, all Contracting Parties	
00111_01	required to sign tachograph	required to sign tachograph	
	card certificates shall generate	card certificates shall generate	
	one or more unique ECC key	one or more unique ECC key	
	pairs designated as	pairs designated as	
	MSCA_Card. All Member	MSCA_Card. All Contracting	
	States required to sign	Parties required to sign	
	certificates for vehicle units or	certificates for vehicle units or	
	external GNSS facilities shall	external GNSS facilities shall	
	additionally generate one or	additionally generate one or	
	more unique ECC key pairs	more unique ECC key pairs	
	designated as MSCA_VU-EGF.	designated as MSCA_VU-EGF.	
9.1.2,	CSM_62 The task of	CSM_62 The task of	
CSM_62	generating Member State key	generating Contracting Party	
	pairs shall be handled by a	key pairs shall be handled by a	
	Member State Certificate	Contracting Party Certificate	
	Authority (MSCA). Whenever a	Authority (MSCA). Whenever a	
	MSCA generates a Member	MSCA generates a Contracting	
	State key pair, it shall send the	Party key pair, it shall send the	
	public key to the ERCA in	public key to the ERCA in	
	order to obtain a	order to obtain a	
	corresponding Member State	corresponding Contracting	
	certificate signed by the ERCA.	Party certificate signed by the	
0.4.2	CCNA CO A NACCOA I II	ERCA.	
9.1.2,	CSM_63 An MSCA shall	CSM_63 An MSCA shall	
CSM_63	choose the strength of a	choose the strength of a	
	Member State key pair equal	Contracting Party key pair	
	to the strength of the European root key pair used	equal to the strength of the	
	to sign the corresponding	root key pair used to sign the	
	Member State certificate.	corresponding Contracting Party certificate.	
9.1.4,	CSM 75 A vehicle unit shall	CSM_75 A vehicle unit shall	
CSM_75	use its VU_MA key pair,	use its VU_MA key pair,	
	consisting of private key	consisting of private key	
	VU_MA.SK and public key	VU_MA.SK and public key	
	VU_MA.PK, exclusively to	VU MA.PK, exclusively to	
	perform VU Authentication	perform VU Authentication	
	towards tachograph cards and	towards tachograph cards and	
	external GNSS facilities, as	external GNSS facilities, as	
	specified in sections 10.3 and	specified in sections 10.3 and	
	11.4 of this Appendix.	11.4 of this Sub-appendix.	
9.1.4,	CSM_76 A vehicle unit shall be	CSM_76 A vehicle unit shall be	
CSM_76	capable of generating	capable of generating	
	ephemeral ECC key pairs and	ephemeral ECC key pairs and	

	T	T	,
	shall use an ephemeral key	shall use an ephemeral key	
	pair exclusively to perform	pair exclusively to perform	
	session key agreement with a	session key agreement with a	
	tachograph card or external	tachograph card or external	
	GNSS facility, as specified in	GNSS facility, as specified in	
	sections 10.4 and 11.4 of this	sections 10.4 and 11.4 of this	
	Appendix.	Sub-appendix.	
9.1.4,	CSM_77 A vehicle unit shall	CSM_77 A vehicle unit shall	
CSM_77	use the private key	use the private key	
_	VU_Sign.SK of its VU_Sign key	VU_Sign.SK of its VU_Sign key	
	pair exclusively to sign	pair exclusively to sign	
	downloaded data files, as	downloaded data files, as	
	specified in chapter 14 of this	specified in chapter 14 of this	
	Appendix. The corresponding	Sub-appendix. The	
	public key VU_Sign.PK shall be	corresponding public key	
	used exclusively to verify	VU_Sign.PK shall be used	
	signatures created by the	exclusively to verify signatures	
	vehicle unit.		
0.1.4	Notes:	created by the vehicle unit. Notes:	
9.1.4, CSM 78	- The extended validity period	- The extended validity period	
C3IVI_76			
	of a VU_Sign certificate allows a Vehicle Unit to create valid	of a VU_Sign certificate allows a Vehicle Unit to create valid	
	signatures over downloaded	signatures over downloaded	
	data during the first three	data during the first three	
	months after it has expired, as	months after it has expired.	
	required in Regulation (EU) N°.	required in Regulation (EU) N°.	
	581/2010.	581/2010.	
9.1.4,	CSM_82 In addition to the	CSM_82 In addition to the	
CSM_82	cryptographic keys and	cryptographic keys and	
	certificates listed in CSM_81,	certificates listed in CSM_81,	
	vehicle units shall also contain	vehicle units shall also contain	
	the keys and certificates	the keys and certificates	
	specified in Part A of this	specified in Part A of this Sub-	
	Appendix, allowing a vehicle	appendix, allowing a vehicle	
	unit to interact with first-	unit to interact with first-	
	generation tachograph cards.	generation tachograph cards.	
9.1.5,	CSM_86 A tachograph card	CSM_86 A tachograph card	
CSM_86	shall use its Card_MA key pair,	shall use its Card_MA key pair,	
	consisting of private key	consisting of private key	
	Card_MA.SK and public key	Card_MA.SK and public key	
	Card_MA.PK, exclusively to	Card_MA.PK, exclusively to	
	perform mutual	perform mutual	
	authentication and session key	authentication and session key	
	agreement towards vehicle	agreement towards vehicle	
	units, as specified in sections	units, as specified in sections	
	10.3 and 10.4 of this	10.3 and 10.4 of this Sub-	
	Appendix.	appendix.	
9.1.5,	CSM_87 A driver card or	CSM_87 A driver card or	
CSM_87	workshop card shall use the	workshop card shall use the	
	private key Card_Sign.SK of its	private key Card_Sign.SK of its	
1			
	Card_Sign key pair exclusively	Card_Sign key pair exclusively	
	to sign downloaded data files,	to sign downloaded data files,	

	as specified in chanter 14 of	as specified in chapter 14 of	
	as specified in chapter 14 of	as specified in chapter 14 of	
	this Appendix. The	this Sub-appendix. The	
	corresponding public key	corresponding public key	
	Card_Sign.PK shall be used	Card_Sign.PK shall be used	
	exclusively to verify signatures	exclusively to verify signatures	
0.4.5	created by the card.	created by the card.	
9.1.5,	Note: the extended validity	Note: the extended validity	
CSM_89	period of a Card_Sign	period of a Card_Sign	
	certificate allows a driver	certificate allows a driver	
	card to create valid	card to create valid	
	signatures over	signatures over	
	downloaded data during	downloaded data during	
	the first month after it has	the first month after it has	
	expired. This is necessary in	expired. This is necessary in	
	view of Regulation (EU) N°.	view of Regulation (EU) N°.	
		, ,	
	581/2010, which requires	581/2010, which requires	
	that a data download from	that a data download from	
	a driver card must be	a driver card must be	
	possible up to 28 days after	possible up to 28 days after	
	the last data has been	the last data has been	
	recorded.	recorded.	
9.1.5,	Note to last bullet: For	Note to last bullet: For	
CSM_91	example, in the first three	example, in the first three	
	months of the ERCA(3)	months of the ERCA(3)	
	certificate (see Figure 1), the	certificate (see Figure 1), the	
	mentioned cards shall contain	mentioned cards shall contain	
	the ERCA(1) certificate. This is	the ERCA(1) certificate. This is	
	needed to ensure that these	needed to ensure that these	
	cards can be used to perform	cards can be used to perform	
	data downloads from ERCA(1)	data downloads from ERCA(1)	
	VUs whose normal 15-year life	VUs whose normal 15-year life	
	period plus the 3-months data	period plus the 3-months data	
	downloading period expires	downloading period expires	
	during these months; see the	during these months; see the	
	last bullet of requirement 13)	last bullet of requirement 13)	
	in Annex 1C.	in Appendix 1C.	
9.1.5,	CSM_92 In addition to	CSM_92 In addition to	
CSM_92	the cryptographic keys and	the cryptographic keys and	
	certificates listed in CSM_91,	certificates listed in CSM_91,	
	tachograph cards shall also	tachograph cards shall also	
	contain the keys and	contain the keys and	
	certificates specified in Part A	certificates specified in Part A	
	of this Appendix, allowing	of this Sub-appendix, allowing	
	these cards to interact with	these cards to interact with	
0.4.6	first-generation VUs.	first-generation VUs.	
9.1.6,	CSM_95 An external	CSM_95 An external	
CSM_95	GNSS facility shall use its	GNSS facility shall use its	
	EGF_MA key pair, consisting of	EGF_MA key pair, consisting of	
	private key EGF_MA.SK and	private key EGF_MA.SK and	
	public key EGF_MA.PK,	public key EGF_MA.PK,	

	T	Ι	
	exclusively to perform mutual	exclusively to perform mutual	
	authentication and session key	authentication and session key	
	agreement towards vehicle	agreement towards vehicle	
	units, as specified in section	units, as specified in section	
	11.4 of this Appendix.	11.4 of this Sub-appendix.	
9.2.1.1	Note: readers of this section	Note: readers of this section	
	are supposed to be familiar	are supposed to be familiar	
	with the contents of [ISO	with the contents of [ISO	
	16844-3] describing the	16844-3] describing the	
	interface between a vehicle	interface between a vehicle	
	unit and a motion sensor. The	unit and a motion sensor. The	
	pairing process between a VU	pairing process between a VU	
	and a motion sensor is	and a motion sensor is	
	described in detail in chapter	described in detail in chapter	
	12 of this Appendix.	12 of this Sub-appendix.	
9.2.1.1,	CSM_100 A number of	CSM_100 A number of	
CSM_100	symmetric keys is needed for	symmetric keys is needed for	
	pairing vehicle units and	pairing vehicle units and	
	motion sensors, for mutual	motion sensors, for mutual	
	authentication between	authentication between	
	vehicle units and motion	vehicle units and motion	
	sensors and for encrypting	sensors and for encrypting	
	communication between	communication between	
	vehicle units and motion	vehicle units and motion	
	sensors, as shown in Table 3.	sensors, as shown in Table 3.	
	All of these keys shall be AES	All of these keys shall be AES	
	keys, with a key length equal	keys, with a key length equal	
	to the length of the motion	to the length of the motion	
	sensor master key, which shall	sensor master key, which shall	
	be linked to the length of the	be linked to the length of the	
	(foreseen) European root key	(foreseen) root key pair as	
	pair as described in CSM_50.	described in CSM_50.	
9.2.1.1,	CSM_101 The European Root	CSM_101 The European Root	
CSM_101	Certificate Authority shall	Certificate Authority shall	
	generate KM-VU and KM-WC,	generate KM-VU and KM-WC,	
	two random and unique AES	two random and unique AES	
	keys from which the motion	keys from which the motion	
	sensor master key KM can be	sensor master key KM can be	
	calculated as KM-VU XOR KM-	calculated as KM-VU XOR KM-	
	WC. The ERCA shall	WC. The ERCA shall	
	communicate KM, KM-VU and	communicate KM, KM-VU and	
	KM-WC to Member State	KM-WC to Contracting Party	
	Certificate Authorities upon	Certificate Authorities upon	
	their request.	their request.	
9.2.1.1,	CSM_103 A Member State	CSM_103 A Contracting Party	
CSM_103	Certificate Authority shall	Certificate Authority shall	
	forward KM-VU, together	forward KM-VU, together	
	with its version number, to	with its version number, to	
	vehicle unit manufacturers	vehicle unit manufacturers	
	upon their request. The VU	upon their request. The VU	
	The state of the s	1 -	
	manufacturers shall insert	manufacturers shall insert	

	KM-VU and its version number in all manufactured VUs.	KM-VU and its version number in all manufactured VUs.	
9.2.1.1, CSM_104	CSM_104 A Member State Certificate Authority shall ensure that KM-WC, together with its version number, is inserted in every workshop card issued under its responsibility.	CSM_104 A Contracting Party Certificate Authority shall ensure that KM-WC, together with its version number, is inserted in every workshop card issued under its responsibility.	
9.2.1.1, CSM_104	Notes: - See the description of data type SensorInstallationSecData in Appendix 2 as explained in section 9.2.1.2, in fact multiple generations of KM-WC may have to be inserted in a single workshop card.	Notes: - See the description of data type SensorInstallationSecData in Sub-appendix 2 as explained in section 9.2.1.2, in fact multiple generations of KM-WC may have to be inserted in a single workshop card.	
9.2.1.1, CSM_105	CSM_105 In addition to the AES key specified in CSM_104, a MSCA shall ensure that the TDES key KmWC, specified in requirement CSM_037 in Part A of this Appendix, is inserted in every workshop card issued under its responsibility.	CSM_105 In addition to the AES key specified in CSM_104, a MSCA shall ensure that the TDES key KmWC, specified in requirement CSM_037 in Part A of this Sub-appendix, is inserted in every workshop card issued under its responsibility.	
9.2.1.1, CSM_105	Notes: • This allows a second-generation workshop card to be used for coupling a first-generation VU. • A second-generation workshop card will contain two different applications, one complying with Part B of this Appendix and one complying with Part A. The latter will contain the TDES key KmWC.	Notes: • This allows a second- generation workshop card to be used for coupling a first- generation VU. • A second-generation workshop card will contain two different applications, one complying with Part B of this Sub-appendix and one complying with Part A. The latter will contain the TDES key KmWC.	
9.2.1.1, CSM_107	CSM_107 Each motion sensor manufacturer shall generate a random and unique pairing key KP for every motion sensor, and shall send each pairing key to its Member State Certificate Authority. The MSCA shall encrypt each pairing key separately with the motion sensor master key KM	CSM_107 Each motion sensor manufacturer shall generate a random and unique pairing key KP for every motion sensor, and shall send each pairing key to its Contracting Party Certificate Authority. The MSCA shall encrypt each pairing key separately with the motion sensor master key KM	

	and shall return the encrypted	and shall return the encrypted	
	key to the motion sensor	key to the motion sensor	
	manufacturer. For each	manufacturer. For each	
	encrypted key, the MSCA shall	encrypted key, the MSCA shall	
	notify the motion sensor	notify the motion sensor	
	manufacturer of the version	manufacturer of the version	
	number of the associated KM.	number of the associated KM.	
9.2.1.1,	CSM_108 Each motion sensor	CSM_108 Each motion sensor	
CSM_108	manufacturer shall generate a	manufacturer shall generate a	
	unique serial number for	unique serial number for	
	every motion sensor, and shall	every motion sensor, and shall	
	send all serial numbers to its	send all serial numbers to its	
	Member State Certificate	Contracting Party Certificate	
	Authority. The MSCA shall	Authority. The MSCA shall	
	encrypt each serial number	encrypt each serial number	
	separately with the	separately with the	
	identification key KID and shall	identification key KID and shall	
	return the encrypted serial	return the encrypted serial	
	number to the motion sensor	number to the motion sensor	
	manufacturer. For each	manufacturer. For each	
	encrypted serial number, the	encrypted serial number, the	
	MSCA shall notify the motion	MSCA shall notify the motion	
	sensor manufacturer of the	sensor manufacturer of the	
	version number of the	version number of the	
	associated KID.	associated KID.	
9.2.1.1,	CSM 111 In addition to the	CSM 111 In addition to the	
CSM 111	AES-based cryptographic	AES-based cryptographic	
_	material specified in	material specified in	
	CSM_110, a motion sensor	CSM_110, a motion sensor	
	manufacturer may also store	manufacturer may also store	
	in each motion sensor the	in each motion sensor the	
	TDES-based cryptographic	TDES-based cryptographic	
	material specified in	material specified in	
	requirement CSM_037 in Part	requirement CSM_037 in Part	
	A of this Appendix.	A of this Sub-appendix.	
9.2.1.2,	CSM_114 At least one year	CSM 114 At least one year	
CSM_114	before generating a new	before generating a new root	
3311	European root key pair, as	key pair, as described in	
	described in CSM_56, the	CSM_56, the ERCA shall	
	ERCA shall generate a new	generate a new motion sensor	
	motion sensor master key KM	master key KM by generating	
	by generating a new KM-VU	a new KM-VU and KM-WC.	
	and KM-WC. The length of the	The length of the motion	
	motion sensor master key	sensor master key shall be	
	shall be linked to the foreseen	linked to the foreseen	
	strength of the new European	strength of the new European	
	root key pair, according to	root key pair, according to	
	CSM_50. The ERCA shall	CSM_50. The ERCA shall	
	communicate the new KM,	communicate the new KM,	
	KM-VU and KM-WC to the	KM-VU and KM-WC to the	
	MSCAs upon their request,	MSCAs upon their request,	
	iviscas upon their request,	wischs upon their request,	

	together with their version	together with their version	
	number.	number.	
9.2.2.1,	CSM 120 The DSRC master	CSM_120 The DSRC master	
CSM_120	key KMDSRC shall be an AES	key KMDSRC shall be an AES	
55	key that is securely generated,	key that is securely generated,	
	stored and distributed by the	stored and distributed by the	
	ERCA. The key length may be	ERCA. The key length may be	
	128, 192 or 256 bits and shall	128, 192 or 256 bits and shall	
	be linked to the length of the	be linked to the length of the	
	European root key pair, as	root key pair, as described in	
	described in CSM_50.	CSM_50.	
9.2.2.1,	CSM_121 The ERCA shall	CSM_121 The ERCA shall	
CSM_121	communicate the DSRC	communicate the DSRC	
	master key to Member State	master key to Contracting	
	Certificate Authorities upon	Party Certificate Authorities	
	their request in a secure	upon their request in a secure	
	manner, to allow them to	manner, to allow them to	
	derive VU-specific DSRC keys	derive VU-specific DSRC keys	
	and to ensure that the DSRC	and to ensure that the DSRC	
	master key is inserted in all	master key is inserted in all	
	control cards and workshop cards issued under their	control cards and workshop cards issued under their	
	responsibility.	responsibility.	
9.2.2.1,	CSM_123 For every vehicle	CSM_123 For every vehicle	
CSM_123	unit, the vehicle unit	unit, the vehicle unit	
C31VI_123	manufacturer shall create a	manufacturer shall create a	
	unique VU serial number and	unique VU serial number and	
	shall send this number to its	shall send this number to its	
	Member State Certificate	Contracting Party Certificate	
	Authority in a request to	Authority in a request to	
	obtain a set of two VU-specific	obtain a set of two VU-specific	
	DSRC keys. The VU serial	DSRC keys. The VU serial	
	number shall have data type	number shall have data type	
	VuSerialNumber.	VuSerialNumber.	
9.2.2,	Note:	Note:	
CSM_123	This VU serial number shall	 This VU serial number shall 	
	be identical to the	be identical to the	
	vuSerialNumber element of	vuSerialNumber element of	
	Vuldentification, see Appendix	Vuldentification, see Sub-	
	1 and to the Certificate Holder	appendix 1 and to the	
	Reference in the VU's	Certificate Holder Reference in the VU's certificates.	
0222	certificates. CSM 130 At least two years		
9.2.2.2, CSM_130	before generating a new	CSM_130 At least two years before generating a new root	
C3IVI_13U	European root key pair, as	key pair, as described in	
	described in CSM 56, the	CSM_56, the ERCA shall	
	ERCA shall generate a new	generate a new DSRC master	
	DSRC master key. The length	key. The length of the DSRC	
	of the DSRC key shall be linked	key shall be linked to the	
	to the foreseen strength of	foreseen strength of the new	
	the new European root key	root key pair, according to	
	pair, according to CSM_50.	CSM_50. The ERCA shall	

	The ERCA shall communicate	communicate the new DSRC	
	the new DSRC master key to	master key to the MSCAs upon	
	the MSCAs upon their request,	their request, together with its	
	together with its version	version number.	
	number.		
9.3.1,	CSM 134 All certificates in the	CSM 134 All certificates in the	
CSM_134	European Smart Tachograph	European Smart Tachograph	
_	system shall be self-	system shall be self-	
	descriptive, card-verifiable	descriptive, card-verifiable	
	(CV) certificates according to	(CV) certificates according to	
	[ISO 7816-4] and [ISO 7816-8].	[ISO 7816-4] and [ISO 7816-8].	
9.3.2,	Table 4, title	Table 4, title	
CSM_136	ASN.1 data type	ASN.1 data type	
C31VI_130	(see Appendix 1)	(see Sub-appendix 1)	
9.3.2,	Note: the Field ID will be used	Note: the Field ID will be used	
	in later sections of this	in later sections of this Sub-	
CSM_136			
	Appendix to indicate individual fields of a	appendix to indicate individual	
		fields of a certificate, e.g.	
	certificate, e.g. X.CAR is the	X.CAR is the Certificate	
	Certificate Authority	Authority Reference	
	Reference mentioned in the	mentioned in the certificate of	
	certificate of user X.	user X.	
9.3.2.3,	CSM_141 The Certificate	CSM_141 The Certificate	
CSM_141	Holder Authorisation shall be	Holder Authorisation shall be	
	used to identify the type of	used to identify the type of	
	certificate. It consists of the six	certificate. It consists of the six	
	most significant bytes of the	most significant bytes of the	
	Tachograph Application ID,	Tachograph Application ID,	
	concatenated with the	concatenated with the	
	equipment type, which	equipment type, which	
	indicates the type of	indicates the type of	
	equipment for which the	equipment for which the	
	certificate is intended. In the	certificate is intended. In the	
	case of a VU certificate, a	case of a VU certificate, a	
	driver card certificate or a	driver card certificate or a	
	workshop card certificate, the	workshop card certificate, the	
	equipment type is also used to	equipment type is also used to	
	differentiate between a	differentiate between a	
	certificate for Mutual	certificate for Mutual	
	Authentication and a	Authentication and a	
	certificate for creating digital	certificate for creating digital	
	signatures (see section 9.1 and	signatures (see section 9.1 and	
	Appendix 1, data type	Sub-appendix 1, data type	
	EquipmentType).	EquipmentType).	
9.3.2.5,	CSM 145 For card	CSM 145 For card	
CSM_145	certificates and external GNSS	certificates and external GNSS	
	facility certificates, the	facility certificates, the	
	Certificate Holder Reference	Certificate Holder Reference	
	shall have the	shall have the	
	ExtendedSerialNumber data	ExtendedSerialNumber data	
	type specified in Appendix 1.	type specified in Sub-appendix	
	type specified in Appendix 1.	1.	
<u></u>		4.	

022F	CSM 146 For vehicle	CSM 146 For vehicle	
9.3.2.5, CSM 146	CSM_146 For vehicle units, the manufacturer, when	CSM_146 For vehicle units, the manufacturer, when	
C3IVI_146			
	requesting a certificate, may	requesting a certificate, may	
	or may not know the	or may not know the manufacturer-specific serial	
	manufacturer-specific serial number of the VU for which	number of the VU for which	
	that certificate and the	that certificate and the	
	associated private key is intended. In the first case, the	associated private key is intended. In the first case, the	
	Certificate Holder Reference	Certificate Holder Reference	
	shall have the	shall have the	
	ExtendedSerialNumber data	ExtendedSerialNumber data	
	type specified in Appendix 1.	type specified in Sub-appendix	
	In the latter case, the	1. In the latter case, the	
	Certificate Holder Reference	Certificate Holder Reference	
	shall have the	shall have the	
	CertificateRequestID data type	CertificateRequestID data type	
	specified in Appendix 1.	specified in Appendix 1.	
9.3.2.5,	Note: For a card certificate,	Note: For a card certificate,	
CSM_146	the value of the CHR shall be	the value of the CHR shall be	
	equal to the value of the	equal to the value of the	
	cardExtendedSerialNumber in	cardExtendedSerialNumber in	
	EF_ICC; see Appendix 2. For an	EF ICC; see Sub-appendix 2.	
	EGF certificate, the value of	For an EGF certificate, the	
	the CHR shall be equal to the	value of the CHR shall be	
	value of the	equal to the value of the	
	sensorGNSSSerialNumber in	sensorGNSSSerialNumber in	
	EF_ICC; see Appendix 14. For a	EF_ICC; see Sub-appendix 14.	
	VU certificate, the value of the	For a VU certificate, the value	
	CHR shall be equal to the	of the CHR shall be equal to	
	vuSerialNumber element of	the vuSerialNumber element	
	Vuldentification, see Appendix	of Vuldentification, see Sub-	
	1, unless the manufacturer	appendix 1, unless the	
	does not know the	manufacturer does not know	
	manufacturer-specific serial	the manufacturer-specific	
	number at the time the	serial number at the time the	
0.2.2.5	certificate is requested.	certificate is requested.	
9.3.2.5,	CSM_147 For ERCA and	CSM_147 For ERCA and	
CSM_147	MSCA certificates, the	MSCA certificates, the	
	Certificate Holder Reference shall have the	Certificate Holder Reference shall have the	
	CertificationAuthorityKID data	CertificationAuthorityKID data	
	type specified in Appendix 1.	type specified in Sub-appendix	
	type specified iff Appendix 1.	1.	
9.3.3,	CSM_152 In addition to the	CSM_152 In addition to the	
CSM_152	data in CSM_151, an MSCA	data in CSM_151, an MSCA	
	shall send the following data	shall send the following data	
	in a certificate request to the	in a certificate request to the	
	ERCA, allowing the ERCA to	ERCA, allowing the ERCA to	
	create the Certificate Holder	create the Certificate Holder	

			<u> </u>
	Reference of the new MSCA certificate:	Reference of the new MSCA certificate:	
	certificate.	certificate.	
	- The numerical nation code of	- The numerical nation code of	
	the Certification Authority	the Certification Authority	
	(data type NationNumeric	(data type NationNumeric	
	defined in Appendix 1)	defined in Sub-appendix 1)	
	- The alphanumerical nation	- The alphanumerical nation	
	code of the Certification	code of the Certification	
	Authority (data type	Authority (data type	
	NationAlpha defined in	NationAlpha defined in	
	Appendix 1)	Appendix 1)	
	The 1 had covied wavelends	The 1 had covied acceptants	
	- The 1-byte serial number to distinguish the different keys	 The 1-byte serial number to distinguish the different keys 	
	of the Certification Authority	of the Certification Authority	
	in the case keys are changed	in the case keys are changed	
	the base keys are onanged	the base keys are onanged	
	- The two-byte field containing	- The two-byte field containing	
	Certification Authority specific	Certification Authority specific	
	additional info	additional info	
10.1,	CSM_155 On a high level,	CSM_155 On a high level,	
CSM_155	secure communication	secure communication	
	between a vehicle unit and a	between a vehicle unit and a	
	tachograph card shall be	tachograph card shall be	
	based on the following steps:	based on the following steps:	
	First and party shall	First and party shall	
	- First, each party shall demonstrate to the other that	 First, each party shall demonstrate to the other that 	
	it owns a valid public key	it owns a valid public key	
	certificate, signed by a	certificate, signed by a	
	Member State Certificate	Contracting Party Certificate	
	Authority. In turn, the MSCA	Authority. In turn, the MSCA	
	public key certificate must be	public key certificate must be	
	signed by the European root	signed by the European root	
	certificate authority. This step	certificate authority. This step	
	is called certificate chain	is called certificate chain	
	verification and is specified in	verification and is specified in	
10.2.1	detail in section 10.2	detail in section 10.2	
10.2.1,	CSM_157 Vehicle units shall use the protocol depicted in	CSM_157 Vehicle units shall use the protocol depicted in	
CSM_157	Figure 4 for verifying a	Figure 4 for verifying a	
	tachograph card's certificate	tachograph card's certificate	
	chain. For every certificate it	chain. For every certificate it	
	reads from the card, the VU	reads from the card, the VU	
	shall verify that the Certificate	shall verify that the Certificate	
	Holder Authorisation (CHA)	Holder Authorisation (CHA)	
	field is correct:	field is correct:	
<u> </u>	-		

	- The CHA field of the Card certificate shall indicate a card certificate for mutual authentication (see Appendix 1, data type EquipmentType). - The CHA of the Card.CA certificate shall indicate an MSCA. - The CHA of the Card.Link certificate shall indicate the ERCA	- The CHA field of the Card certificate shall indicate a card certificate for mutual authentication (see Subappendix 1, data type EquipmentType). - The CHA of the Card.CA certificate shall indicate an MSCA. - The CHA of the Card.Link certificate shall indicate the ERCA	
10.2.1, CSM_157	Notes to Error! Reference source not found.:	Notes to Error! Reference source not found.:	
C31VI_137	- The Card	- The Card	
	certificates and	certificates and	
	public keys	public keys	
	mentioned in the	mentioned in the	
	figure are those for	figure are those for	
	mutual	mutual	
	authentication. Section Error!	authentication.	
	Reference source	Section Error!	
	not found. denotes	Reference source	
	these as Card_MA.	not found. denotes	
	- The Card.CA	these as Card_MA.	
	certificates and	- The Card.CA certificates and	
	public keys	public keys	
	mentioned in the	mentioned in the	
	figure are those for signing card	figure are those for	
	certificates and it is	signing card	
	indicated in the	certificates and it is	
	CAR of the Card	indicated in the CAR	
	certificate. Section	of the Card	
	Error! Reference	certificate. Section	
	source not found.	Error! Reference	
	denotes these as	source not found.	
	MSCA_Card The Card.CA.EUR	denotes these as	
	certificate	MSCA_Card The Card.CA.EUR	
	mentioned in the	certificate	
	figure is the	mentioned in the	
	European root	figure is the root	
	certificate that is indicated in the	certificate that is	
	CAR of the	indicated in the CAR	
	Card.CA certificate.		

	- The Card.Link certificate mentioned in the figure is the card's link certificate, if present. As specified in section Error! Reference source not found., this is a link certificate for a new European root key pair created by the ERCA and signed by the previous European private key The Card.Link.EUR certificate is the European root certificate that is indicated in the CAR of the Card.Link certificate.	of the Card.CA certificate. The Card.Link certificate mentioned in the figure is the card's link certificate, if present. As specified in section Error! Reference source not found., this is a link certificate for a new root key pair created by the ERCA and signed by the previous root private key. The Card.Link.EUR certificate is the root certificate that is indicated in the CAR of the Card.Link certificate.	
10.2.2, CSM_161	CSM_161 Tachograph cards shall use the protocol depicted in Figure 5 for verifying a VU's certificate chain. For every certificate presented by the VU, the card shall verify that the Certification Holder Authorisation (CHA) field is correct: - The CHA of the VU.Link certificate shall indicate the	CSM_161 Tachograph cards shall use the protocol depicted in Figure 5 for verifying a VU's certificate chain. For every certificate presented by the VU, the card shall verify that the Certification Holder Authorisation (CHA) field is correct: - The CHA of the VU.Link certificate shall indicate the	
	 ERCA. The CHA of the VU.CA certificate shall indicate an MSCA. The CHA field of the VU certificate shall indicate a VU certificate for mutual authentication (see Appendix 1, data type EquipmentType). 	ERCA. - The CHA of the VU.CA certificate shall indicate an MSCA. - The CHA field of the VU certificate shall indicate a VU certificate for mutual authentication (see Subappendix 1, data type EquipmentType).	

40.2.2	Natara ta Elavora E.	Notes to Elever E.	
10.2.2, CSM_161	Notes to Figure 5:	Notes to Figure 5:	
	- The VU certificates and public keys mentioned in the figure are those for mutual authentication. Section 9.1.4 denotes these as VU_MA.	- The VU certificates and public keys mentioned in the figure are those for mutual authentication. Section 9.1.4 denotes these as VU_MA.	
	- The VU.CA certificates and public keys mentioned in the figure are those for signing VU and external GNSS facility certificates. Section 9.1.3 denotes these as MSCA_VU-EGF.	- The VU.CA certificates and public keys mentioned in the figure are those for signing VU and external GNSS facility certificates. Section 9.1.3 denotes these as MSCA_VU-EGF.	
	- The VU.CA.EUR certificate mentioned in the figure is the European root certificate that is indicated in the CAR of the VU.CA certificate.	- The VU.CA.EUR certificate mentioned in the figure is the root certificate that is indicated in the CAR of the VU.CA certificate.	
	- The VU.Link certificate mentioned in the figure is the VU's link certificate, if present. As specified in section 9.1.2, this is a link certificate for a new European root key pair created by the ERCA and signed by the previous European private key.	- The VU.Link certificate mentioned in the figure is the VU's link certificate, if present. As specified in section 9.1.2, this is a link certificate for a new root key pair created by the ERCA and signed by the previous root private key. - The VU.Link.EUR	
	- The VU.Link.EUR certificate is the European root certificate that is indicated in the CAR of the VU.Link certificate.	certificate is the root certificate that is indicated in the CAR of the VU.Link certificate.	
10.2.2, CSM_163	CSM_163 The VU shall use the MSE: Set AT command to set its public key for use in the tachograph card. As specified in Appendix 2, this command contains an indication of the cryptographic mechanism that will be used with the key that is set. This mechanism shall be 'VU Authentication using the ECDSA algorithm, in	CSM_163 The VU shall use the MSE: Set AT command to set its public key for use in the tachograph card. As specified in Sub-appendix 2, this command contains an indication of the cryptographic mechanism that will be used with the key that is set. This mechanism shall be 'VU Authentication using the	
	combination with the hashing algorithm linked to the key	ECDSA algorithm, in combination with the hashing	

	T	Г	T
	size of the VU's VU_MA key	algorithm linked to the key	
	pair, as specified in CSM_50'.	size of the VU's VU_MA key	
		pair, as specified in CSM_50'.	
10.5.1,	CSM_182 Except when	CSM_182 Except when	
CSM_182	reading from a file with access	reading from a file with access	
	condition SM-R-ENC-MAC-G2	condition SM-R-ENC-MAC-G2	
	(see Appendix 2, section 4),	(see Sub-appendix 2, section	
	Secure Messaging shall be	4), Secure Messaging shall be	
	used in authentication-only	used in authentication-only	
	mode. In this mode, a	mode. In this mode, a	
	cryptographic checksum	cryptographic checksum	
	(a.k.a. MAC) is added to all	(a.k.a. MAC) is added to all	
	commands and responses to	commands and responses to	
	ensure message authenticity	ensure message authenticity	
	and integrity.	and integrity.	
10 5 3			
10.5.2,	Note: As specified in Appendix	Note: As specified in Appendix	
CSM_188	2, tachograph cards may	2, tachograph cards may	
	support the READ BINARY and	support the READ BINARY and	
	UPDATE BINARY command	UPDATE BINARY command	
	with an odd INS byte ('B1'	with an odd INS byte ('B1'	
	resp. 'D7'). These command	resp. 'D7'). These command	
	variants are required to read	variants are required to read	
	and update files with more	and update files with more	
	than 32768 bytes or more. In	than 32768 bytes or more. In	
	case such a variant is used, a	case such a variant is used, a	
	data object with tag 'B3' shall	data object with tag 'B3' shall	
	be used instead of an object	be used instead of an object	
	with tag '81'. See Appendix 2	with tag '81'. See Sub-	
	for more information.	appendix 2 for more	
		information.	
10.5.2,	CSM_190 APDUs protected by	CSM_190 APDUs protected by	
CSM_190	Secure Messaging shall be	Secure Messaging shall be	
	created as follows:	created as follows:	
		3.23.00.00.00.00.00	
	The command has day shall	- The command header shall	
	- The command header shall		
	be included in the MAC	be included in the MAC	
	calculation, therefore value	calculation, therefore value	
	'OC'shall be used for the class	'0C'shall be used for the class	
	byte CLA.	byte CLA.	
	- As specified in Appendix 2, all	- As specified in Sub-appendix	
	INS bytes shall be even, with	2, all INS bytes shall be even,	
	the possible exception of odd	with the possible exception of	
	INS bytes for the READ BINARY	odd INS bytes for the READ	
	and UPDATE BINARY	BINARY and UPDATE BINARY	
	commands.	commands.	
	- The actual value of Lc will be	- The actual value of Lc will be	
	modified to Lc' after	modified to Lc' after	
	modified to LC after	modified to LC after	

	application of secure	application of secure	
	messaging.	messaging.	
	- The Data field shall consist of	- The Data field shall consist of	
	SM data objects.	SM data objects.	
	- In the protected command	- In the protected command	
	APDU the new Le byte shall be	APDU the new Le byte shall be	
	set to '00'. If required, a data	set to '00'. If required, a data	
	object '97' shall be included in	object '97' shall be included in	
	the Data field in order to	the Data field in order to	
	convey the original value of	convey the original value of	
	Le.	Le.	
11.1,	CSM_200 For communication	CSM_200 For communication	
CSM_200	between a vehicle unit and an	between a vehicle unit and an	
	EGF, APDU commands and	EGF, APDU commands and	
	responses based on [ISO 7816-	responses based on [ISO 7816-	
	4] and [ISO 7816-8] shall be	4] and [ISO 7816-8] shall be	
	used. The exact structure of	used. The exact structure of	
	these APDUs is defined in	these APDUs is defined in Sub-	
	Appendix 2 of this Annex.	appendix 2 of this Appendix.	
11.3.2,	Notes to Figure 4 within this	Notes to Figure 4 within this	
CSM_206	context:	context:	
	- Communication control is	- Communication control is	
	out of the scope of this	out of the scope of this Sub-	
	Appendix. However, an EGF is	appendix. However, an EGF is	
	not a smart card and hence	not a smart card and hence	
	the VU will probably not send	the VU will probably not send	
	a Reset to initiate the	a Reset to initiate the	
	communication and will not receive an ATR.	communication and will not	
	- The Card certificates and	receive an ATR. - The Card certificates and	
	public keys mentioned in the	public keys mentioned in the	
	figure shall be interpreted as	figure shall be interpreted as	
	the EGF's certificates and	the EGF's certificates and	
	public keys for mutual	public keys for mutual	
	authentication. Section 9.1.6	authentication. Section 9.1.6	
	denotes these as EGF_MA.	denotes these as EGF MA.	
	- The Card.CA certificates and	- The Card.CA certificates and	
	public keys mentioned in the	public keys mentioned in the	
	figure shall be interpreted as	figure shall be interpreted as	
	the MSCA's certificates and	the MSCA's certificates and	
	public keys for signing EGF	public keys for signing EGF	
	certificates. Section 9.1.3	certificates. Section 9.1.3	
	denotes these as MSCA_VU-	denotes these as MSCA_VU-	
	EGF.	EGF.	
	- The Card.CA.EUR certificate	- The Card.CA.EUR certificate	
	mentioned in the figure shall	mentioned in the figure shall	
	be interpreted as the	be interpreted as the root	
	European root certificate that	certificate that is indicated in	
	is indicated in the CAR of the	the CAR of the MSCA_VU-EGF	
	MSCA_VU-EGF certificate.	certificate.	
	_		

	- The Card.Link certificate	- The Card.Link certificate	
	mentioned in the figure shall	mentioned in the figure shall	
	be interpreted as the EGF's	be interpreted as the EGF's	
	link certificate, if present. As	link certificate, if present. As	
	specified in section 9.1.2, this	specified in section 9.1.2, this	
	is a link certificate for a new	is a link certificate for a new	
	European root key pair	root key pair created by the	
	created by the ERCA and	ERCA and signed by the	
	signed by the previous	previous European private	
	European private key.	key.	
	- The Card.Link.EUR certificate	- The Card.Link.EUR certificate	
	is the European root		
	certificate that is indicated in	is the root certificate that is	
		indicated in the CAR of the	
	the CAR of the Card.Link	Card.Link certificate.	
	certificate.	- Instead of the	
	- Instead of the	cardExtendedSerialNumber,	
	cardExtendedSerialNumber,	the VU shall read the	
	the VU shall read the	sensorGNSSserialNumber	
	sensorGNSSserialNumber	from EF ICC.	
	from EF ICC.	- Instead of selecting the	
	- Instead of selecting the	Tachograph AID, the VU shall	
	Tachograph AID, the VU shall	select the EGF AID.	
	select the EGF AID.	- 'Ignore Card' shall be	
	- 'Ignore Card' shall be	interpreted as 'Ignore EGF'.	
	interpreted as 'Ignore EGF'.	interpreted as ignore Edi .	
11.3.2,	Notes to Figure 5 within this	Notes to Figure 5 within this	
CSM_208	context:	context:	
	- The VU shall generate a fresh	- The VU shall generate a fresh	
	ephemeral key pair using the	ephemeral key pair using the	
	domain parameters in the EGF	domain parameters in the EGF	
	certificate.	certificate.	
	- The VU certificates and	- The VU certificates and	
	public keys mentioned in the	public keys mentioned in the	
		figure are those for mutual	
	figure are those for mutual		
	authentication. Section 9.1.4	authentication. Section 9.1.4	
	denotes these as VU_MA.	denotes these as VU_MA.	
	- The VU.CA certificates and	- The VU.CA certificates and	
	public keys mentioned in the	public keys mentioned in the	
	figure are those for signing VU	figure are those for signing VU	
	and external GNSS facility	and external GNSS facility	
	certificates. Section 9.1.3	certificates. Section 9.1.3	
	denotes these as MSCA_VU-	denotes these as MSCA_VU-	
	EGF.	EGF.	
	- The VU.CA.EUR certificate	- The VU.CA.EUR certificate	
	mentioned in the figure is the	mentioned in the figure is the	
	European root certificate that	root certificate that is	
	is indicated in the CAR of the	indicated in the CAR of the	
	VU.CA certificate.	VU.CA certificate.	
	- The VU.Link certificate	- The VU.Link certificate	
1	•	1	i l
	mentioned in the figure is the	mentioned in the figure is the	
	mentioned in the figure is the VU's link certificate, if present.	_	
	_	mentioned in the figure is the VU's link certificate, if present. As specified in section 9.1.2,	

	this is a link certificate for a new European root key pair	this is a link certificate for a new root key pair created by	
	created by the ERCA and	the ERCA and signed by the	
	signed by the previous European private key.	previous root private key The VU.Link.EUR certificate is	
	- The VU.Link.EUR certificate is	the root certificate that is	
	the European root certificate	indicated in the CAR of the	
	that is indicated in the CAR of the VU.Link certificate.	VU.Link certificate.	
11.3.3,	Note that Figure 11 in essence	Note that Figure 11 in essence	
CSM_211	consists of the first steps shown in Figure 4 and Figure	consists of the first steps shown in Figure 4 and Figure	
	5. Again, note that since an	5. Again, note that since an	
	EGF is not a smart card, the	EGF is not a smart card, the	
	VU will probably not send a	VU will probably not send a	
	Reset to initiate the	Reset to initiate the	
	communication and will not	communication and will not	
	receive an ATR. In any case this is out of the scope of this	receive an ATR. In any case this is out of the scope of this	
	Appendix.	Sub-appendix.	
12.3,	Note: in [ISO 16844-3], the	Note: in [ISO 16844-3], the	
CSM_220	number of plaintext data	number of plaintext data	
	bytes is always a multiple of 8,	bytes is always a multiple of 8,	
	such that padding is not	such that padding is not	
	necessary when using TDES. The definition of data and	necessary when using TDES. The definition of data and	
	messages in [ISO 16844-3] is	messages in [ISO 16844-3] is	
	not changed by this part of	not changed by this part of	
	this Appendix, thus	this Sub-appendix, thus	
	necessitating the application	necessitating the application	
	of padding.	of padding.	
12.4,	CSM_222 As explained in	CSM_222 As explained in	
CSM_222	section 9.2.1, a second-	section 9.2.1, a second- generation motion sensor may	
	generation motion sensor may contain the TDES-based	contain the TDES-based	
	encryption of the pairing data	encryption of the pairing data	
	(as defined in Part A of this	(as defined in Part A of this	
	Appendix), which allows the	Sub-appendix), which allows	
	motion sensor to be paired to	the motion sensor to be	
	a first-generation VU. If this is	paired to a first-generation	
	the case, a first-generation VU	VU. If this is the case, a first-	
	and a second-generation motion sensor shall be paired	generation VU and a second- generation motion sensor	
	as described in Part A of this	shall be paired as described in	
	Appendix and in [ISO 16844-	Part A of this Sub-appendix	
	3]. For the pairing process	and in [ISO 16844-3]. For the	
	either a first-generation or a	pairing process either a first-	
	second-generation workshop	generation or a second-	
	card may be used.	generation workshop card	
13.1	As specified in Appendix 14, a	may be used. As specified in Appendix 14, a	
13.1	VU regularly generates	VU regularly generates	
L	- 5 . 50 mm. 17 Berner acco		<u> </u>

Remote Tachograph Remote Tachograph Monitoring (RTM) data and Monitoring (RTM) data and sends this data to the (internal sends this data to the (internal or external) Remote or external) Remote Communication Facility (RCF). Communication Facility (RCF). The remote communication The remote communication facility is responsible for facility is responsible for sending this data over the sending this data over the DSRC interface described in DSRC interface described in Appendix 14 to the remote Sub-appendix 14 to the interrogator. Appendix 1 remote interrogator. Subspecifies that the RTM data is appendix 1 specifies that the the concatenation of: RTM data is the concatenation Encrypted tachograph of: the encryption Encrypted tachograph payload of the plaintext tachograph payload the encryption of the plaintext tachograph payload DSRC security data payload described below DSRC security data described below The plaintext tachograph payload data format is The plaintext tachograph specified in Appendix 1 and payload data format is specified in Sub-appendix 1 further described in Appendix 14. This section describes the and further described in Substructure of the DSRC security appendix 14. This section describes the structure of the data; the formal specification is in Appendix 1 DSRC security data; the formal specification is in Subappendix 1 13.2. CSM_226 Given a plaintext CSM_226 Given a plaintext CSM 226 data element with data type data element with data type TachographPayload as TachographPayload as described in Appendix 14, a described in Sub-appendix 14, VU shall encrypt this data as a VU shall encrypt this data as shown in Figure 12: the VU's shown in Figure 12: the VU's DSRC key for encryption DSRC key for encryption K VUDSRC ENC (see section K VUDSRC ENC (see section 9.2.2) shall be used with AES 9.2.2) shall be used with AES in the Cipher Block Chaining in the Cipher Block Chaining (CBC) mode of operation, as (CBC) mode of operation, as defined in [ISO 10116], with defined in [ISO 10116], with an interleave parameter m = an interleave parameter m = 1. The initialization vector 1. The initialization vector shall be equal to IV = current shall be equal to IV = current date time || '00 00 00 00 00 date time || '00 00 00 00 00 00 00 00 00' || counter, 00 00 00 00' || counter, where current date time and where current date time and counter are specified in counter are specified in CSM 224. The data to be CSM 224. The data to be encrypted shall be padded encrypted shall be padded

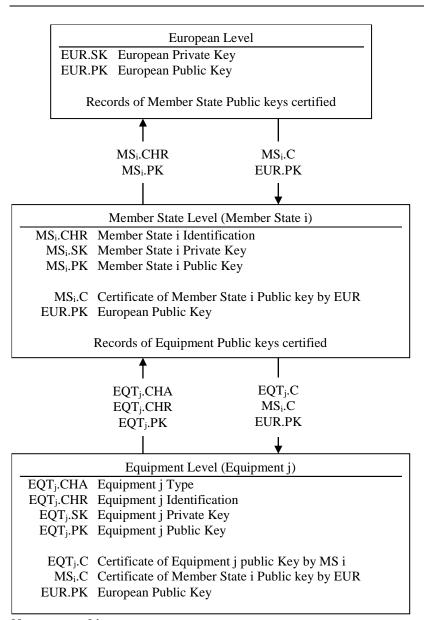
	using method 2 defined in USO	using mothed 2 defined in USO	
	using method 2 defined in [ISO 9797-1].	using method 2 defined in [ISO 9797-1].	
13.3,	CSM_228 When a remote	CSM_228 When a remote	
CSM_228	interrogator receives RTM	interrogator receives RTM	
C5WI_220	data from a VU, it shall send	data from a VU, it shall send	
	the entire RTM data to a	the entire RTM data to a	
	control card in the data field	control card in the data field	
	of a PROCESS DSRC MESSAGE	of a PROCESS DSRC MESSAGE	
	command, as described in	command, as described in	
	Appendix 2. Then:	Sub-appendix 2. Then:	
	1. The control card shall	1. The control card shall	
	inspect the DSRC master key	inspect the DSRC master key	
	version number in the DSRC	version number in the DSRC	
	security data. If the control	security data. If the control	
	card does not know the	card does not know the	
	indicated DSRC master key, it	indicated DSRC master key, it	
	shall return an error specified	shall return an error specified	
	in Appendix 2 and abort the	in Sub-appendix 2 and abort	
	process.	the process.	
	2. The control card shall use	2. The control card shall use	
	the indicated DSRC master key	the indicated DSRC master key	
	in combination with the VU	in combination with the VU	
	serial number or the	serial number or the	
	certificate request ID in the	certificate request ID in the	
	DSRC security data to derive	DSRC security data to derive	
	the VU-specific DSRC keys	the VU-specific DSRC keys	
	K_VUDSRC_ENC and	K_VUDSRC_ENC and	
	K_VUDSRC_MAC, as specified	K_VUDSRC_MAC, as specified	
	in CSM_124.	in CSM_124.	
	3. The control card shall use	3. The control card shall use	
	K_VUDSRC_MAC to verify the	K_VUDSRC_MAC to verify the	
	MAC in the DSRC security	MAC in the DSRC security	
	data, as specified in CSM_227.	data, as specified in CSM_227.	
	If the MAC is incorrect, the	If the MAC is incorrect, the	
	control card shall return an	control card shall return an	
	error specified in Appendix 2	error specified in Sub-	
	and abort the process.	appendix 2 and abort the	
	4. The control card shall use	process. 4. The control card shall use	
	K_VUDSRC_ENC to decrypt the encrypted tachograph		
	payload, as specified in	K_VUDSRC_ENC to decrypt the encrypted tachograph	
	CSM_226. The control card	payload, as specified in	
	shall remove the padding and	CSM_226. The control card	
	shall return the decrypted	shall remove the padding and	
	tachograph payload data to	shall return the decrypted	
	the remote interrogator.	tachograph payload data to	
	and terrote interrogator.	the remote interrogator.	
13.3,	Notes:	Notes:	
CSM_229	This requires the	This requires the	
55	remote interrogator to have	remote interrogator to have	
	an accurate and reliable	an accurate and reliable	
	source of time.	source of time.	

	Since Appendix 14	Since Sub-appendix 14	
	requires a VU to calculate a	requires a VU to calculate a	
	new set of RTM data every 60	new set of RTM data every 60	
	seconds, and the clock of the	seconds, and the clock of the	
	VU is allowed to deviate 1	VU is allowed to deviate 1	
	minute from the real time, a	minute from the real time, a	
	lower limit for the freshness of	lower limit for the freshness of	
	the RTM data is 2 minutes.	the RTM data is 2 minutes.	
	The actual freshness to be	The actual freshness to be	
	required also depends on the	required also depends on the	
	accuracy of the clock of the	accuracy of the clock of the	
	remote interrogator.	remote interrogator.	
13.3,	CSM 230 When a	CSM 230 When a	
CSM_230	workshop verifies the correct	workshop verifies the correct	
2377_230	functioning of the DSRC	functioning of the DSRC	
	functionality of a VU, it shall	functionality of a VU, it shall	
	send the entire RTM data	send the entire RTM data	
	received from the VU to a	received from the VU to a	
		workshop card in the data	
	workshop card in the data field of a PROCESS DSRC	field of a PROCESS DSRC	
	MESSAGE command, as		
		MESSAGE command, as	
	described in Appendix 2. The	described in Sub-appendix 2.	
	workshop card shall perform	The workshop card shall	
	all checks and actions	perform all checks and actions	
	specified in CSM_228.	specified in CSM_228.	
14.1,	CSM_231The Intelligent	CSM_231The Intelligent	
CSM_231	Dedicated Equipment (IDE)	Dedicated Equipment (IDE)	
	shall store data received from	shall store data received from	
	a VU or a card during one	a VU or a card during one	
	download session within one	download session within one	
	physical data file. Data may be	physical data file. Data may be	
	stored on an ESM (external	stored on an ESM (external	
	storage medium). This file	storage medium). This file	
	contains digital signatures	contains digital signatures	
	over data blocks, as specified	over data blocks, as specified	
	in Appendix 7. This file shall	in Sub-appendix 7. This file	
	also contain the following	shall also contain the following	
	certificates (refer to section	certificates (refer to section	
	9.1):	9.1):	
14.1,	CSM_232 The IDE shall also	CSM_232 The IDE shall also	
CSM_232	dispose of.	dispose of.	
	- In case it uses a control card	- In case it uses a control card	
	to verify the signature, as	to verify the signature, as	
	shown in Figure 13: The link	shown in Figure 13: The link	
	certificate linking the latest	certificate linking the latest	
	EUR certificate to the EUR	EUR certificate to the EUR	
	certificate whose validity	certificate whose validity	
	period directly precedes it, if	period directly precedes it, if	
	existing.	existing.	
	- In case it verifies the	- In case it verifies the	
	signature itself: all valid	signature itself: all valid root	
	European root certificates.	certificates.	
<u> </u>	Laropeur root certificates.	cordinates.	

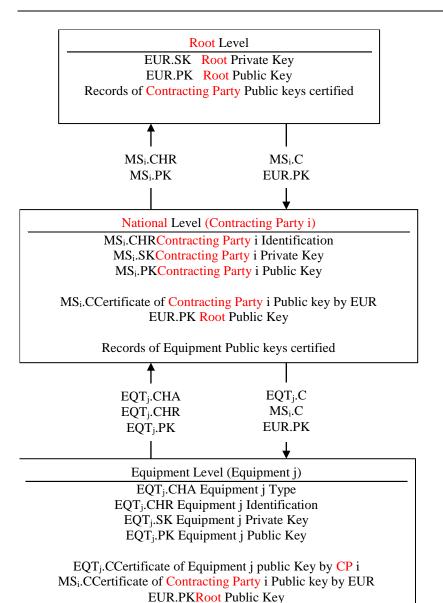
14.1,	Note: the method the IDE uses	Note: the method the IDE uses	
	to retrieve these certificates is	to retrieve these certificates is	
CSM_232			
	not specified in this Appendix.	not specified in this Sub-	
110	6014 6044 405	appendix.	
14.3,	CSM_234 An IDE may perform	CSM_234 An IDE may perform	
CSM_234	verification of a signature over	verification of a signature over	
	downloaded data itself or it	downloaded data itself or it	
	may use a control card for this	may use a control card for this	
	purpose. In case it uses a	purpose. In case it uses a	
	control card, signature	control card, signature	
	verification shall take place as	verification shall take place as	
	shown in Figure 13. For	shown in Figure 13. For	
	verifying the temporal validity	verifying the temporal validity	
	of a certificate presented by	of a certificate presented by	
	the IDE, the control card shall	the IDE, the control card shall	
	use its internal current time,	use its internal current time,	
	as specified in CSM_167. The	as specified in CSM_167. The	
	control card shall update its	control card shall update its	
	current time if the Effective	current time if the Effective	
	Date of an authentic 'valid	Date of an authentic 'valid	
	source of time' certificate is	source of time' certificate is	
	more recent than the card's	more recent than the card's	
	current time. The card shall	current time. The card shall	
	accept only the following	accept only the following	
	certificates as a valid source of	certificates as a valid source of	
	time:	time:	
	- Second-generation ERCA link	- Second-generation ERCA link	
	certificates	certificates	
	- Second-generation MSCA	- Second-generation MSCA	
	certificates	certificates	
	 Second-generation VU_Sign 	 Second-generation VU_Sign 	
	or Card_Sign certificates	or Card_Sign certificates	
	issued by the same country as	issued by the same country as	
	the control card's own card	the control card's own card	
	certificate.	certificate.	
	In case it performs signature	In case it performs signature	
	verification itself, the IDE shall	verification itself, the IDE shall	
	verify the authenticity and	verify the authenticity and	
	validity of all certificates in the	validity of all certificates in the	
	certificate chain in the data	certificate chain in the data	
	file, and it shall verify the	file, and it shall verify the	
	signature over the data	signature over the data	
	following the signature	following the signature	
	scheme defined in [DSS]. In	scheme defined in [DSS]. In	
	both cases, for every	both cases, for every	
	certificate read from the data	certificate read from the data	
	file, it is necessary to verify	file, it is necessary to verify	
	that the Certificate Holder	that the Certificate Holder	
	Authorisation (CHA) field is	Authorisation (CHA) field is	
	correct:	correct:	
	•		

	1		
	- The CHA field of the EQT	- The CHA field of the EQT	
	certificate shall indicate a VU	certificate shall indicate a VU	
	or Card (as applicable)	or Card (as applicable)	
	certificate for signing (see	certificate for signing (see Sub-	
	Appendix 1, data type	appendix 1, data type	
	EquipmentType).	EquipmentType).	
	- The CHA of the EQT.CA	- The CHA of the EQT.CA	
	certificate shall indicate an	certificate shall indicate an	
	MSCA.	MSCA.	
	- The CHA of the EQT.Link	- The CHA of the EQT.Link	
	certificate shall indicate the	certificate shall indicate the	
	ERCA.	ERCA.	
14.3,	Notes to Figure 13:	Notes to Figure 13:	
CSM_234	- The equipment that signed	- The equipment that signed	
_	the data to be analysed is	the data to be analysed is	
	denoted EQT.	denoted EQT.	
	- The EQT certificates and	- The EQT certificates and	
	public keys mentioned in the	public keys mentioned in the	
	figure are those for signing,	figure are those for signing,	
	i.e. VU Sign or Card Sign.	i.e. VU_Sign or Card_Sign.	
	- The EQT.CA certificates and	- The EQT.CA certificates and	
	public keys mentioned in the	public keys mentioned in the	
	figure are those for signing VU	figure are those for signing VU	
	or Card certificates, as	or Card certificates, as	
	applicable.	applicable.	
	- The EQT.CA.EUR certificate	- The EQT.CA.EUR certificate	
	mentioned in the figure is the	mentioned in the figure is the	
	European root certificate that	root certificate that is	
	is indicated in the CAR of the	indicated in the CAR of the	
	EQT.CA certificate.	EQT.CA certificate.	
	- The EQT.Link certificate	- The EQT.Link certificate	
	mentioned in the figure is the	mentioned in the figure is the	
	EQT's link certificate, if	EQT's link certificate, if	
	present. As specified in	present. As specified in	
	section 9.1.2, this is a link	section 9.1.2, this is a link	
	certificate for a new European	certificate for a new root key	
	root key pair created by the	pair created by the ERCA and	
	ERCA and signed with the	signed with the previous root	
	previous European private	private key.	
	key.	- The EQT.Link.EUR certificate	
	- The EQT.Link.EUR certificate	is the root certificate that is	
	is the European root	indicated in the CAR of the	
	certificate that is indicated in	EQT.Link certificate.	
	the CAR of the EQT.Link		
	certificate.		
	oci dificate:		

Current image in CSM_010



New proposed image



LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 12 FOR AETR V0.2 20190113

Point or article	Text Appendix 12	Proposed text for AETR	Comments
TITLE/TABLE OF CONTENTS			To be updated as needed, according to the validated changes
1	This Appendix provides the technical requirements for the GNSS data used by the Vehicle Unit, including the protocols that must be implemented to assure the secure and correct data transfer of the positioning information. The main articles in this Regulation (EU) No. 165/2014 driving these requirements are: "Article 8 Recording of the position of the vehicle at certain points during the daily working period", "Article 10 Interface with Intelligent Transport Systems" and "Article 11 Detailed provisions for smart tachographs".	This Sub-appendix provides the technical requirements for the GNSS data used by the Vehicle Unit, including the protocols that must be implemented to assure the secure and correct data transfer of the positioning information.	References to Regulation (EU) No. 165/2014 have been suppressed.
1.2	The following acronyms are used in this appendix:	The following acronyms are used in this Sub-appendix:	
1.2		Add new acronym after RMC Recommended Minimum Specific: SBAS Satellite-Based Augmentation System	
2	Regardless of the configuration of the Smart Tachograph with or without an external GNSS facility, the provision of accurate and reliable positioning information is an essential element of the effective operation of the Smart Tachograph. Therefore, it is appropriate to require its compatibility with the services provided by the Galileo and European Geostationary Navigation Overlay Service (EGNOS) programmes as set	To be deleted.	

	aut in Doculation (CII) No.		
	out in Regulation (EU) No.		
	1285/2013 of the European		
	Parliament and of the Council .		
	The system established under		
	the Galileo programme is an		
	independent global satellite		
	navigation system and the one		
	established under the EGNOS		
	programme is a regional		
	satellite navigation system		
	improving the quality of the		
	Global Positioning System		
	signal.		
2	Footnote 1:	To be deleted	
	Regulation (EU) No.		
	1285/2013 of the European		
	Parliament and of the Council		
	of 11 December 2013 on the		
	implementation and		
	exploitation of European		
	satellite navigation systems		
	and repealing Council		
	Regulation (EC) No. 876/2002		
	and Regulation (EC) No.		
	683/2008 of the European		
	Parliament and of the Council		
	(OJ L 347, 20.12.2013, p. 1).		
2, GNS_2	GNS_2 Manufacturers shall	GNS_2 Manufacturers shall	
	ensure that the GNSS	ensure that the GNSS	
	receivers in the Smart	receivers in the smart	
	Tachographs are compatible	tachographs are compatible	
	with the positioning services	with the positioning services	
	provided by the Galileo and	provided by GPS, GLONASS	
	the EGNOS systems.	and Galileo. Manufacturers	
	Manufacturers may also	may also choose, in addition,	
	choose, in addition,	compatibility with other	
	compatibility with other	satellite navigation systems.	
	satellite navigation systems.		
2, GNS_3a		GNS_3a GNSS receivers may	
(new)		be also capable of receiving	
		and processing SBAS signals.	
3, GNS_5	GNS_5The Vehicle Unit shall	GNS_5 The Vehicle Unit shall	
	store in the VU database the	store in the VU database the	
	position information for	position information for	
	latitude and longitude with a	latitude and longitude with a	
	resolution of 1/10 of minute	resolution of 1/10 of minute	
	or 1/600 of a degree as	or 1/600 of a degree as	
	described in Appendix 1 for	described in Sub-appendix 1	
4.0.1	type GeoCoordinates.	for type GeoCoordinates.	
4.2.1,	GNS_18 Regarding the	GNS_18 Regarding the	
GNS_18	functions 1) the collection and	functions 1) the collection and	
	distribution of GNSS data and	distribution of GNSS data and	

	T = 1	I	1
	2) the collection of the configuration data of the external GNSS facility and 3) management protocol, the GNSS Secure Transceiver shall simulate a smart card with a file system architecture composed by a Master File (MF), a Dedicated File (DF) with Application Identifier specified in Appendix 1 chapter 6.2 ('FF 44 54 45 47 4D') and with 3 EFs containing certificates and one single Elementary File (EF.EGF) with file identifier equal to '2F2F' as described in Table 1.	2) the collection of the configuration data of the external GNSS facility and 3) management protocol, the GNSS Secure Transceiver shall simulate a smart card with a file system architecture composed by a Master File (MF), a Dedicated File (DF) with Application Identifier specified in Sub-appendix 1 chapter 6.2 ('FF 44 54 45 47 4D') and with 3 EFs containing certificates and one single Elementary File (EF.EGF) with file identifier equal to '2F2F' as described in Table 1.	
4.2.1, GNS_21	GNS_21 The file structure is provided in Table 1. For the access conditions (ALW, NEV, SM-MAC) see Appendix 2 chapter 3.5.	GNS_21 The file structure is provided in Table 1. For the access conditions (ALW, NEV, SM-MAC) see Sub-appendix 2 chapter 3.5.	
4.2.1, GNS_21	EF.EGF 7th line Extended serial-number of the external GNSS facility defined in Appendix 1 as SensorGNSSSerialNumber.	EF.EGF 7th line Extended serial-number of the external GNSS facility defined in Sub-appendix 1 as SensorGNSSSerialNumber.	
4.2.1, GNS_21	EF.EGF 8th line Operating system identifier of the GNSS Secure Transceiver defined in Appendix 1 as SensorOSIdentifier.	EF.EGF 8th line Operating system identifier of the GNSS Secure Transceiver defined in Sub-appendix 1 as SensorOSIdentifier.	
4.2.1, GNS_21	EF.EGF 9th line Type approval number of the external GNSS facility defined in Appendix 1 as SensorExternalGNSSApproval Number.	EF.EGF 9th line Type approval number of the external GNSS facility defined in Sub-appendix 1 as SensorExternalGNSSApproval Number.	
4.2.1, GNS_21	EF.EGF 10th line Identifier of the security component of the external GNSS facility defined in Appendix 1 as SensorExternalGNSSSCIdentifi er	EF.EGF 10th line Identifier of the security component of the external GNSS facility defined in Sub- appendix 1 as SensorExternalGNSSSCIdentifi er	
4.2.2 GNS_22	GNS_22 The secure transfer of GNSS position data shall be allowed only in the following conditions: 1. The coupling process has been completed as described	GNS_22 The secure transfer of GNSS position data shall be allowed only in the following conditions: 1. The coupling process has been completed as described	

	in Appendix 11. Common security mechanisms. 2. The periodic mutual authentication and session key agreement between the VU and the external GNSS facility also described in Appendix 11. Common security mechanisms has been executed with the indicated frequency.	in Sub-appendix 11. Common security mechanisms. 2. The periodic mutual authentication and session key agreement between the VU and the external GNSS facility also described in Sub-appendix 11. Common security mechanisms has been executed with the indicated frequency.	
4.2.2, GNS_23	1. The VU requests location data from the External GNSS facility together with Dilution of Precision data (from the GSA NMEA sentence). The VU Secure Transceiver shall use the ISO/IEC 7816-4:2013 SELECT and READ RECORD(S) command in secure messaging authentication-only mode as described in Appendix 11 section 11.5 with the file identifier "2F2F" and RECORD number equal to "01" for RMC NMEA sentence and '02','03','04','05','06' for GSA NMEA sentence.	1. The VU requests location data from the External GNSS facility together with Dilution of Precision data (from the GSA NMEA sentence). The VU Secure Transceiver shall use the ISO/IEC 7816-4:2013 SELECT and READ RECORD(S) command in secure messaging authentication-only mode as described in Sub-appendix 11 section 11.5 with the file identifier "2F2F" and RECORD number equal to "01" for RMC NMEA sentence and '02','03','04','05','06' for GSA NMEA sentence.	
4.2.2, GNS_23	3. The GNSS Secure Transceiver sends the response to the VU Secure Transceiver by using the APDU response message in secure messaging authentication-only mode as described in Appendix 11 section 11.5.	3. The GNSS Secure Transceiver sends the response to the VU Secure Transceiver by using the APDU response message in secure messaging authentication-only mode as described in Subappendix 11 section 11.5.	
4.2.2, GNS_23	6. The VU processor stores the received and processed information such as latitude, longitude, time and speed in the VU in the format defined in Appendix 1 Data Dictionary as GeoCoordinates together with the value of HDOP calculated as the minimum of the HDOP values collected on the available GNSS systems	6. The VU processor stores the received and processed information such as latitude, longitude, time and speed in the VU in the format defined in Sub-appendix 1 Data Dictionary as GeoCoordinates together with the value of HDOP calculated as the minimum of the HDOP values collected on the available GNSS systems	
4.2.3	This section describes in detail the structure of the Read Record command. Secure	This section describes in detail the structure of the Read Record command. Secure	

	massaging (authoritisation	massaging (authoritisation	
	messaging (authentication-	messaging (authentication-	
	only mode) is added as	only mode) is added as	
	described in Appendix 11	described in Sub-appendix 11	
	Common security	Common security	
	mechanisms.	mechanisms.	
4.2.3,	This section describes in detail	This section describes in detail	
GNS_24	the structure of the Read	the structure of the Read	
	Record command. Secure	Record command. Secure	
	messaging (authentication-	messaging (authentication-	
	only mode) is added as	only mode) is added as	
	described in Appendix 11	described in Sub-appendix 11	
	Common security	Common security	
	mechanisms.	mechanisms.	
4.2.3,	GNS 27 The GNSS Secure	GNS 27 The GNSS Secure	
GNS_27	Transceiver shall support the	Transceiver shall support the	
_	following tachograph	following tachograph	
	generation 2 commands	generation 2 commands	
	specified in Appendix 2:	specified in Sub-appendix 2:	
	Command Reference	Command Reference	
	Select Appendix 2 chapter	Select Sub-appendix 2 chapter	
	3.5.1	3.5.1	
	Read Binary Appendix 2	Read Binary Sub-appendix 2	
	chapter 3.5.2	chapter 3.5.2	
	Get Challenge Appendix 2	Get Challenge Sub-appendix 2	
	chapter 3.5.4	chapter 3.5.4	
	PSO: Verify Certificate	PSO: Verify Certificate Sub-	
	Appendix 2 chapter 3.5.7	appendix 2 chapter 3.5.7	
	External Authenticate	External Authenticate Sub-	
	Appendix 2 chapter 3.5.9	appendix 2 chapter 3.5.9	
	General Authenticate	General Authenticate Sub-	
	Appendix 2 chapter 3.5.10	appendix 2 chapter 3.5.10	
	MSE:SET Appendix 2	MSE:SET Sub-appendix 2	
	chapter 3.5.11	chapter 3.5.11	
4.3	The coupling, mutual	The coupling, mutual	
	authentication and session key	authentication and session key	
	agreement of the external	agreement of the external	
	GNSS facility with the vehicle	GNSS facility with the vehicle	
	unit is described in Appendix	unit is described in Sub-	
	11. Common security	appendix 11. Common security	
	mechanisms, Chapter 11.	mechanisms, Chapter 11.	
4.4, GNS_31	GNS 31 If the VU detects	GNS 31 If the VU detects	
- 1.1, GN3_31	that the EGF certificate used	that the EGF certificate used	
	for mutual authentication is	for mutual authentication is	
	not valid any longer, the VU	not valid any longer, the VU	
	shall generate and record a	shall generate and record a	
	recording equipment fault of	control device fault of type	
	type EventFaultType enum	EventFaultType enum '1B'H	
	'1B'H External GNSS facility	External GNSS facility	
	certificate expired with a	certificate expired with a	
	timestamp equal to the current	timestamp equal to the current	
	value of time. The VU shall still	value of time. The VU shall still	
	value of time. The vo shall Still	value of time. The vo shall Still	

	use the received GNSS position data.	use the received GNSS position data.	
7, GNS_35	GNS_35 The VU shall trigger and record an Vehicle Motion Conflict event (see in requirement 84 in this Annex) with a timestamp equal to the current value of time, in case motion information calculated from the motion sensor is contradicted by motion information calculated from the internal GNSS receiver or from the external GNSS facility. For the purpose of detecting such contradictions, the median value of the speed differences between these sources shall be used, as specified below:	GNS_35 The VU shall trigger and record an Vehicle Motion Conflict event (see in requirement 84 in this Appendix) with a timestamp equal to the current value of time, in case motion information calculated from the motion sensor is contradicted by motion information calculated from the internal GNSS receiver or from the external GNSS facility. For the purpose of detecting such contradictions, the median value of the speed differences between these sources shall be used, as specified below:	

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 13 FOR AETR V0.2 20190113

Point or article	Text Appendix 13	Proposed text for AETR	Comments
TITLE/TABLE OF CONTENTS	(Title) APPENDIX 13. ITS INTERFACE	SUB-APPENDIX 13. ITS INTERFACE	
1	This Appendix specifies the design and the procedures to follow in order to implement the interface with Intelligent Transport Systems (ITS) as required in Article 10 of Regulation (EU) N°. 165/2014 (the Regulation).	This Sub-appendix specifies the design and the procedures to follow in order to implement the interface with Intelligent Transport Systems (ITS) as required in Article 10 of Regulation (EU) N°. 165/2014 (the EU Regulation).	
1	The Regulation specifies that the tachographs of vehicles may be equipped with standardised interfaces allowing the data recorded or produced by tachograph to be used in operational mode, by an external device, provided that the following conditions are met: (a) the interface does not affect the authenticity and the integrity of the data of the tachograph; (b) the interface complies with the detailed provisions of Article 11 of the Regulation; (c) the external device connected to the interface has access to personal data, including geopositioning data, only after the verifiable consent of the driver to whom the data relates.	The EU Regulation specifies that The tachographs of vehicles may be equipped with standardised interfaces allowing the data recorded or produced by tachograph to be used in operational mode, by an external device, provided that the following conditions are met: (a) the interface does not affect the authenticity and the integrity of the data of the tachograph; (b) the interface complies with the detailed provisions of this Sub-appendix; (c) the external device connected to the interface has access to personal data, including geopositioning data, only after the verifiable consent of the driver to whom the data relates.	
2	The scope of this Appendix is to specify how applications hosted on external devices can via a Bluetooth® connection obtain data (the Data) from a tachograph. This Appendix specifies:	The scope of this Sub- appendix is to specify how applications hosted on external devices can via a Bluetooth® connection obtain data (the Data) from a tachograph. This Sub-appendix specifies:	

- The Data available through the ITS interface
- The Bluetooth®
 profile that is used to transfer the data
- The enquiry and download procedures and sequence of operations
- The pairing mechanism between the tachograph and the external device
- The consent mechanism available to the driver

For clarification, this Appendix does not specify:

- The collection of the Data operation and management within the VU (which shall be specified elsewhere within the Regulation or otherwise shall be a function of product design).
- The form of presentation of collected data to application hosted on the external device.
- Data security
 provisions above
 what provides
 Bluetooth® (such as
 encryption)
 concerning the
 content of the Data
 (which shall be
 specified elsewhere
 within the Regulation
 [Appendix 11
 Common Security
 Mechanisms]).

- The Data available through the ITS interface
- The Bluetooth® profile that is used to transfer the data
- The enquiry and download procedures and sequence of operations
- The pairing mechanism between the tachograph and the external device
- The consent mechanism available to the driver

For clarification, this Subappendix does not specify:

- The collection of the Data operation and management within the VU (which shall be specified elsewhere within this Agreement or otherwise shall be a function of product design).
- The form of presentation of collected data to application hosted on the external device.
- Data security
 provisions above
 what provides
 Bluetooth® (such as
 encryption)
 concerning the
 content of the Data
 (which shall be
 specified elsewhere
 within this
 Agreement [Subappendix 11 Common
 Security
 Mechanisms]).

	- The Bluetooth®		
	protocols used by the ITS interface	 The Bluetooth® protocols used by the ITS interface 	
2.1	The following acronyms and definitions specific to this Appendix are used in this appendix:	The following acronyms and definitions specific to this Sub-appendix are used in this appendix:	
2.1	the Regulation Regulation (EU) N°. 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) N°. 3821/85 on recording equipment in road transport and amending Regulation (EC) N°. 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport	the Regulation Regulation (EU) N°. 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) N°. 3821/85 on recording equipment in road transport and amending Regulation (EC) N°. 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport	Suppressed definition (not needed)
3, title	Referenced Regulations and Standards	Referenced standards	No references to Regulations remain
3	The specification defined in this Appendix refers to and depends upon all or parts of the following regulations and standards. Within the clauses of this Appendix the relevant standards, or relevant clauses of standards, are specified. In the event of any contradiction the clauses of this Appendix shall take precedence.	The specification defined in this Sub-appendix refers to and depends upon all or parts of the following regulations and standards. Within the clauses of this Sub-appendix the relevant standards, or relevant clauses of standards, are specified. In the event of any contradiction the clauses of this Sub-appendix shall take precedence.	Temalii
	Regulations and standards referenced in this Appendix are:	Regulations and Standards referenced in this Subappendix are:	
	• Regulation (EU) N°. 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) N°. 3821/85 on	• Regulation (EU) N°. 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) N°. 3821/85 on	

	recording equipment in road transport and amending Regulation (EC) N°. 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport. • Regulation (EC) N°. 561/2006 of the European Parliament and of the Council of 15 March 2006 on the harmonisation of certain social legislation relating to road transport and amending Council Regulations (EEC) N°. 3821/85 and (EC) No 2135/98 and repealing Council Regulation (EEC) N°. 3820/85. • ISO 16844 – 4: Road vehicles – Tachograph systems – Part 4: Can interface • ISO 16844 – 7: Road vehicles – Tachograph systems – Part 7: Parameters • Bluetooth® – Serial Port Profile – V1.2	recording equipment in road transport and amending Regulation (EC) N°. 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport. ISO 16844 – 4: Road vehicles – Tachograph systems – Part 4: Can interface ISO 16844 – 7: Road vehicles – Tachograph systems – Part 7: Parameters Bluetooth® – Serial Port Profile – V1.2 Bluetooth® – Core Version 4.2 NMEA 0183 V4.1 protocol	
4.1	Bluetooth® – Core Version 4.2 NMEA 0183 V4.1 protocol The VU shall be responsible to keep updated and maintain the data to be stored in the VU, without any involvement of the ITS interface. The means by which this is	The VU shall be responsible to keep updated and maintain the data to be stored in the VU, without any involvement of the ITS interface. The means by which this is	
4.1.1	achieved is internal to the VU, specified elsewhere in the Regulation, and is not specified in this Appendix. The VU shall be responsible to	achieved is internal to the VU, specified elsewhere in this Agreement, and is not specified in this Subappendix. The VU shall be responsible to	
	update the data that will be available through the ITS interface at a frequency determined within VU procedures, without any involvement of ITS interface. The VU data shall be used as a basis to populate and update the Data, the means by which	update the data that will be available through the ITS interface at a frequency determined within VU procedures, without any involvement of ITS interface. The VU data shall be used as a basis to populate and update the Data, the means by which	

	1		
	this is achieved is specified	this is achieved is specified	
	elsewhere in the Regulation or	elsewhere in this Agreement	
	if there is no such specification	or if there is no such	
	is a function of product design	specification is a function of	
	and is not specified in this	product design and is not	
	Appendix.	specified in Sub-appendix.	
4.1.2	The content of the Data shall	The content of the Data shall	
	be as specified in Annex 1 of	be as specified in Annex 1 of	
	this appendix.	this Sub-appendix.	
4.1.3	ITS applications will be using	ITS applications will be using	
	the data made available	the data made available	
	through the ITS interface for	through the ITS interface for	
	instance to optimize driver	instance to optimize driver	
	activities management while	activities management while	
	respecting the Regulation, to	respecting the provisions of	
	detect possible faults of the	this Agreement, to detect	
	tachograph or to use the GNSS	possible faults of the	
	data. The specification of the	tachograph or to use the GNSS	
	applications is not within the	data. The specification of the	
	scope of this Appendix.	applications is not within the	
		scope of this Sub-appendix.	
4.2	(3 rd paragraph)	(3 rd paragraph)	
	When an external device	When an external device	
	comes within range of the VU	comes within range of the VU	
	for the first time, the	for the first time, the	
	Bluetooth® pairing process	Bluetooth® pairing process	
	can be initiated (see also	can be initiated (see also	
	annex 2). The devices share	annex 2). The devices share	
	their addresses, names, and	their addresses, names, and	
	profiles and common secret	profiles and common secret	
	key, which allows them to	key, which allows them to	
	bond whenever they're	bond whenever they're	
	together in the future. Once	together in the future. Once	
	this step is completed, the	this step is completed, the	
	external device is trusted and	external device is trusted and	
	is in state to initiate requests	is in state to initiate requests	
	to download data from the	to download data from the	
	tachograph. It is not foreseen	tachograph. It is not foreseen	
	to add encryption mechanisms	to add encryption mechanisms	
	beyond what Bluetooth®	beyond what Bluetooth®	
	provides. However, if	provides. However, if	
	additional security	additional security	
	mechanisms are needed, this	mechanisms are needed, this	
	will be done in accordance	will be done in accordance	
	with Appendix 11 Common	with Sub-appendix 11	
	Security Mechanisms.	Common Security	
		Mechanisms.	
4.4, Table 3	See Annex 3 of this appendix	See Annex 3 of this Sub-	
	for more information about	appendix for more	
	the content of each data type.	information about the content	
		of each data type.	

	Cara America di 12 familia	Car Cult and and but 12 fa	
	See Appendix 12 for more	See Sub-appendix 12 for more	
	information about the format	information about the format	
	and content of GNSS data.	and content of GNSS data.	
	See Annex IB and IC for more	See Appendix IB and IC for	
	information about event data	more information about event	
	code and faults.	data code and faults.	
4.8	ITS units shall be able to	ITS units shall be able to	
	request events data	request events data	
	containing the list of all the	containing the list of all the	
	unexpected events. These	unexpected events. These	
	data are considered standard	data are considered standard	
	or personal, see Annex 3. The	or personal, see Annex 3. The	
	content of each event is in	content of each event is in	
	accordance with the	accordance with the	
	documentation provided in	documentation provided in	
	Annex 1 of this appendix.	Annex 1 of this Sub-appendix.	
Annex 1,	See Appendix 12 – GNSS	See Sub-appendix 12 – GNSS	
,	occinpondin == onco	See Sub appendix 12 Sites	
point 2		occount appendix 12	
-	Event codes table (available	New table, see at the end of	
point 2			
point 2 Annex 1,	Event codes table (available	New table, see at the end of	
point 2 Annex 1, point 3	Event codes table (available without driver consent)	New table, see at the end of thisdocument	
point 2 Annex 1, point 3 Annex 1,	Event codes table (available without driver consent) Event codes table (available	New table, see at the end of thisdocument New table, see at the end of	
point 2 Annex 1, point 3 Annex 1, point 4	Event codes table (available without driver consent) Event codes table (available with driver consent)	New table, see at the end of thisdocument New table, see at the end of thisdocument	
point 2 Annex 1, point 3 Annex 1, point 4 Annex 1,	Event codes table (available without driver consent) Event codes table (available with driver consent) Fault codes table (available	New table, see at the end of thisdocument New table, see at the end of thisdocument New table, see at the end of	
point 2 Annex 1, point 3 Annex 1, point 4 Annex 1, point 5	Event codes table (available without driver consent) Event codes table (available with driver consent) Fault codes table (available without driver consent)	New table, see at the end of thisdocument New table, see at the end of thisdocument New table, see at the end of thisdocument	
point 2 Annex 1, point 3 Annex 1, point 4 Annex 1, point 5 Annex 3,	Event codes table (available without driver consent) Event codes table (available with driver consent) Fault codes table (available without driver consent) See Appendix 1 for definition	New table, see at the end of thisdocument New table, see at the end of thisdocument New table, see at the end of thisdocument See Sub-appendix 1 for	
point 2 Annex 1, point 3 Annex 1, point 4 Annex 1, point 5 Annex 3, line 375	Event codes table (available without driver consent) Event codes table (available with driver consent) Fault codes table (available without driver consent) See Appendix 1 for definition of GeoCoordinates	New table, see at the end of thisdocument New table, see at the end of thisdocument New table, see at the end of thisdocument See Sub-appendix 1 for definition of GeoCoordinates	
point 2 Annex 1, point 3 Annex 1, point 4 Annex 1, point 5 Annex 3, line 375 Annex 3,	Event codes table (available without driver consent) Event codes table (available with driver consent) Fault codes table (available without driver consent) See Appendix 1 for definition of GeoCoordinates IMPORTS NationAlpha FROM	New table, see at the end of thisdocument New table, see at the end of thisdocument New table, see at the end of thisdocument See Sub-appendix 1 for definition of GeoCoordinates	
point 2 Annex 1, point 3 Annex 1, point 4 Annex 1, point 5 Annex 3, line 375 Annex 3,	Event codes table (available without driver consent) Event codes table (available with driver consent) Fault codes table (available without driver consent) See Appendix 1 for definition of GeoCoordinates IMPORTS NationAlpha FROM Appendix 1;See Appendix 1	New table, see at the end of thisdocument New table, see at the end of thisdocument New table, see at the end of thisdocument See Sub-appendix 1 for definition of GeoCoordinates IMPORTS NationAlpha FROM Sub-appendix 1;See Sub-	
point 2 Annex 1, point 3 Annex 1, point 4 Annex 1, point 5 Annex 3, line 375 Annex 3,	Event codes table (available without driver consent) Event codes table (available with driver consent) Fault codes table (available without driver consent) See Appendix 1 for definition of GeoCoordinates IMPORTS NationAlpha FROM Appendix1;See Appendix 1 for more information about	New table, see at the end of thisdocument New table, see at the end of thisdocument New table, see at the end of thisdocument See Sub-appendix 1 for definition of GeoCoordinates IMPORTS NationAlpha FROM Sub-appendix 1;See Sub-appendix 1 for more	
point 2 Annex 1, point 3 Annex 1, point 4 Annex 1, point 5 Annex 3, line 375 Annex 3,	Event codes table (available without driver consent) Event codes table (available with driver consent) Fault codes table (available without driver consent) See Appendix 1 for definition of GeoCoordinates IMPORTS NationAlpha FROM Appendix1;See Appendix 1 for more information about	New table, see at the end of thisdocument New table, see at the end of thisdocument New table, see at the end of thisdocument See Sub-appendix 1 for definition of GeoCoordinates IMPORTS NationAlpha FROM Sub-appendix 1;See Sub-appendix 1 for more information about	

Annex 1, point 3 Current table

Event	Storage rules	Data to be recorded per event
Insertion of a non-valid card	- the 10 most recent events.	 date and time of event, card(s) type, number, issuing Member State and generation of the card creating the event. number of similar events that day
Card conflict	- the 10 most recent events.	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of the two cards creating the conflict.
Last card session not correctly closed	- the 10 most recent events.	 date and time of card insertion, card(s) type, number, issuing Member State and generation, last session data as read from the card: date and time of card insertion, VRN, Member State of registration and VU generation.
Power supply interruption (2)	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Communication error with the remote communication facility	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Absence of position information from GNSS receiver	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Communication error with the external GNSS facility	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.

Motion data error	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Vehicle motion conflict	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Security breach attempt	- the 10 most recent events per type of event.	 date and time of beginning of event, date and time of end of event (if relevant), card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, type of event.
Time conflict	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 recording equipment date and time GNSS date and time, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.

New proposed table

Event	Storage rules	Data to be recorded per event
Insertion of a non-valid	- the 10 most recent events.	- date and time of event,
card		- card(s) type, number, issuing
		Contracting Party or Member State
		and generation of the card creating
		the event.
		- number of similar events that day
Card conflict	- the 10 most recent events.	- date and time of beginning of event,
		- date and time of end of event,
		- card(s) type, number, issuing
		Contracting Party or Member State
		and generation of the two cards
		creating the conflict.

Last card session not	- the 10 most recent events.	- date and time of card insertion,
correctly closed	- die 10 most fecent events.	 card(s) type, number, issuing Contracting Party or Member State and generation, last session data as read from the card: date and time of card insertion, VRN, Contracting Party or Member State of registration and VU generation.
Power supply interruption (2)	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party or Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Communication error with the remote communication facility	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party or Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Absence of position information from GNSS receiver	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party or Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Communication error with the external GNSS facility	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party or Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Motion data error	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party or Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Vehicle motion conflict	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party or Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.

Security breach attempt	- the 10 most recent events per type of	- date and time of beginning of event,
	event.	- date and time of end of event (if
		relevant),
		- card(s) type, number, issuing
		Contracting Party or Member State
		and generation of any card inserted
		at beginning and/or end of the event,
		- type of event.
Time conflict	- the longest event for each of the 10	- control device (recording
	last days of occurrence,	equipment) date and time
	- the 5 longest events over the last 365	- GNSS date and time,
	days.	- card(s) type, number, issuing
		Contracting Party or Member State
		and generation of any card inserted
		at beginning and/or end of the event,
		- number of similar events that day.

Annex 1, point 4 Current table

Event	Storage rules	Data to be recorded per event
Driving without an appropriate card	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Card insertion while driving	- the last event for each of the 10 last days of occurrence,	 date and time of the event, card(s) type, number, issuing Member State and generation, number of similar events that day
Over speeding (1)	 the most serious event for each of the 10 last days of occurrence (i.e. the one with the highest average speed), the 5 most serious events over the last 365 days. the first event having occurred after the last calibration 	 date and time of beginning of event, date and time of end of event, maximum speed measured during the event, arithmetic average speed measured during the event, card type, number, issuing Member State and generation of the driver card (if applicable), number of similar events that day.

New proposed table

Event	Storage rules	Data to be recorded per event
Driving without an appropriate card	 the longest event for each of the 10 last days of occurrence, the 5 longest events over the last 365 days. 	 date and time of beginning of event, date and time of end of event, card(s) type, number, issuing Contracting Party or Member State and generation of any card inserted at beginning and/or end of the event, number of similar events that day.
Card insertion while driving	- the last event for each of the 10 last days of occurrence,	 date and time of the event, card(s) type, number, issuing Contracting Party or Member State and generation, number of similar events that day
Over speeding (1)	 the most serious event for each of the 10 last days of occurrence (i.e. the one with the highest average speed), the 5 most serious events over the last 365 days. the first event having occurred after the last calibration 	 date and time of beginning of event, date and time of end of event, maximum speed measured during the event, arithmetic average speed measured during the event, card type, number, issuing Contracting Party or Member State and generation of the driver card (if applicable), number of similar events that day.

Annex 1, point 5 Current table

Fault	Storage rules	Data to be recorded per fault
Card fault	- the 10 most recent driver card faults.	 date and time of beginning of fault, date and time of end of fault, card(s) type, number, issuing
Recording equipment faults	 the 10 most recent faults for each type of fault, the first fault after the last calibration. 	Member State and generation. - date and time of beginning of fault, - date and time of end of fault, - type of fault, - card(s) type, number and issuing Member State and generation of any card inserted at beginning and/or end of the fault.

New proposed table

Fault	Storage rules	Data to be recorded per fault
Card fault	- the 10 most recent driver card faults.	 date and time of beginning of fault, date and time of end of fault, card(s) type, number, issuing Contracting Party or Member State and generation.
Control device (Recording equipment) faults	 the 10 most recent faults for each type of fault, the first fault after the last calibration. 	 date and time of beginning of fault, date and time of end of fault, type of fault, card(s) type, number and issuing Contracting Party or Member State and generation of any card inserted at beginning and/or end of the fault.

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 14 FOR AETR V0.2 20190113

Point or	Toyt Annondiy 14	Proposed text for	Commonts
article	Text Appendix 14	AETR	Comments
TITLE/TABLE	(Title)		
OF	APPENDIX 14. REMOTE	SUB-APPENDIX 14. REMOTE	
CONTENTS	COMMUNICATION FUNCTION	COMMUNICATION FUNCTION	
1	This Appendix specifies the	This Sub-appendix specifies	Reference suppressed (not
	design and the procedures to	the design and the procedures	needed)
	follow in order to perform the	to follow in order to perform	
	remote communication	the remote communication	
	function (the Communication)	function (the Communication)	
	as required in Article 9 of	as required in Article 9 of	
	Regulation (EU) No. 165/2014	Regulation (EU) No. 165/2014	
	(the Regulation).	(the Regulation).	
1, DSC_1	Regulation (EU) No. 165/2014	Regulation (EU) No. 165/2014	
	determines that the	determines that The	
	tachograph shall be equipped	tachograph shall be equipped	
	with a remote communication	with a remote communication	
	functionality that shall enable agents of the competent	functionality that shall enable agents of the competent	
	control authorities to read	control authorities to read	
	tachograph information from	tachograph information from	
	passing vehicles by using	passing vehicles by using	
	remote interrogation	remote interrogation	
	equipment (the Remote early	equipment (the Remote early	
	detection communication	detection communication	
	reader [REDCR]), specifically,	reader [REDCR]), specifically,	
	interrogation equipment	interrogation equipment	
	connecting wirelessly using	connecting wirelessly using	
	CEN 5.8 GHz Dedicated Short	CEN 5.8 GHz Dedicated Short	
	Range Communication (DSRC)	Range Communication (DSRC)	
	interfaces.	interfaces.	
	It is important to comprehend	It is important to comprehend	
	that this functionality is	that this functionality is	
	intended to serve only as a	intended to serve only as a	
	pre-filter in order to select	pre-filter in order to select	
	vehicles for closer inspection,	vehicles for closer inspection,	
	and it does not replace the	and it does not replace the	
	formal inspection process as	formal inspection process. as	
	determined in the provisions	determined in the provisions	
	of Regulation (EU) No.	of Regulation (EU) No.	
	165/2014. See recital 9 in the	165/2014. See recital 9 in the	
	preamble of this regulation,	preamble of this regulation,	
	stating that remote	stating that Remote	
	communication between the	communication between the	
	tachograph and control	tachograph and control	
	authorities for roadside	authorities for roadside	

	control purposes facilitates	control purposes facilitates	
1 800 0	targeted roadside checks.	targeted roadside checks.	
1, DSC_2	The Data shall be exchanged	The Data shall be exchanged	
	using the Communication	using the Communication	
	which shall be a wireless	which shall be a wireless	
	intercourse using 5.8 GHz	intercourse using 5.8 GHz	
	DSRC wireless	DSRC wireless	
	communications consistent	communications consistent	
	with this Appendix and tested	with this Sub-appendix and	
	against the appropriate	tested against the appropriate	
	parameters of EN 300 674-1,	parameters of EN 300 674-1,	
	{Electromagnetic compatibility	{Electromagnetic compatibility	
	and Radio spectrum Matters	and Radio spectrum Matters	
	(ERM); Road Transport and	(ERM); Road Transport and	
	Traffic Telematics (RTTT);	Traffic Telematics (RTTT);	
	Dedicated Short Range	Dedicated Short Range	
	Communication (DSRC)	Communication (DSRC)	
	transmission equipment (500	transmission equipment (500	
	kbit/s / 250 kbit/s) operating	kbit/s / 250 kbit/s) operating	
	in the 5,8 GHz Industrial,	in the 5,8 GHz Industrial,	
	Scientific and Medical (ISM)	Scientific and Medical (ISM)	
	band; Part 1: General	band; Part 1: General	
	characteristics and test	characteristics and test	
	methods for Road Side Units	methods for Road Side Units	
	(RSU) and On -Board Units	(RSU) and On -Board Units	
	(OBU)}.	(OBU)}.	
1, DSC_5	Access to the Data	Access to the Data	
	communicated shall be	communicated shall be	
	restricted to competent	restricted to competent	
	control authorities authorised	control authorities authorised	
	to check infringements of	to check infringements of	
	Regulation (EC) No. 561/2006 and of Regulation (EU) No.	Regulation (EC) No. 561/2006 and of Regulation (EU) No.	
	165/2014 and to workshops in	165/2014 and to workshops in	
	so far as it is necessary to	so far as it is necessary to	
	verify the correct functioning	verify the correct functioning	
	of the tachograph.	of the tachograph.	
1, DSC_7	Data integrity and security	Data integrity and security	
1, 030_/	shall be obtained by	shall be obtained by	
		_	
	securing the Data within	securing the Data within	
	the Vehicle Unit (VU) and	the Vehicle Unit (VU) and	
	by passing only the secured	by passing only the secured	
	payload data and security	payload data and security	
	related data (see 5.4.4)	related data (see 5.4.4)	
	across the wireless 5.8 GHz	across the wireless 5.8 GHz	
	DSRC remote	DSRC remote	
	communication medium,	communication medium,	
	meaning that only	meaning that only	
	authorised persons of	authorised persons of	
	competent control	competent control	
	authorities have the means	authorities have the means	
		T GOLD OF THE STREET	

	to understand the data	to understand the data	
	passed across the	passed across the	
	Communication and to	Communication and to	
	verify its authenticity. See	verify its authenticity. See	
	Appendix 11 Common	Sub-appendix 11 Common	
	Security Mechanisms.	Security Mechanisms.	
1, DSC_9	The content of the security	The content of the security	
	data shall be known only to	data shall be known only to	
	and within the control of the	and within the control of the	
	competent control authorities,	competent control authorities,	
	and those parties with whom	and those parties with whom	
	they share this information	they share this information	
	and is outwith the provisions	and is outwith the provisions	
	of the Communication that is	of the Communication that is	
	the subject of this Appendix,	the subject of this Sub-	
	save that the Communication	appendix, save that the	
	makes provision to transfer a	Communication makes	
	packet of security data with	provision to transfer a packet	
	every packet of payload data.	of security data with every	
		packet of payload data.	
1, DSC_11	For clarification, in accordance	For clarification, in accordance	
	with the provisions of	with the provisions of	
	Regulation (EU) No. 165/2014	Regulation (EU) No. 165/2014	
	(Article 7), data concerning	(Article 7), Data concerning	
	the identity of the driver shall	the identity of the driver shall	
	not be communicated across	not be communicated across	
	the Communication.	the Communication.	
2	The scope of this Appendix is	The scope of this Sub-	
	to specify how agents of the	appendix is to specify how	
	competent control authorities	agents of the competent	
	use a specified 5.8 GHz DSRC	control authorities use a	
	wireless communication to	specified 5.8 GHz DSRC	
	remotely obtain data (the	wireless communication to	
	Data) from a targeted vehicle	remotely obtain data (the	
	that identifies that the	Data) from a targeted vehicle	
	targeted vehicle is in potential	that identifies that the	
	violation of Regulation (EU) No. 165/2014 and should be	targeted vehicle is in potential violation of this Agreement	
	targeted for consideration to	and should be targeted for	
	be stopped for further	consideration to be stopped	
	investigation.	for further investigation.	
	investigation.	To Tartife investigation.	
	Regulation (EU) No. 165/2014	The Data collected shall be	
	requires that the Data	limited to data or pertaining	
	collected shall be limited to	to data that identifies a	
	data or pertaining to data that	potential infringement. as	
	identifies a potential	defined in Article 9 of	
	infringement, as defined in	Regulation (EU) No. 165/2014.	
	Article 9 of Regulation (EU)	, , , , , , , , , , , , , , , , , , , ,	
	No. 165/2014.		
	140. 103/2014.		

In this scenario, the time available for communication is limited, because the Communication is targeted and of a short-range design. Further, the same communication means for remote tachograph monitoring (RTM) may also be used by the competent control authorities for other applications (such as the maximal weights and dimensions for heavy goods vehicles defined in Directive (EU) 2015/719) and such operations may be separate or sequential at the discretion of the competent control authorities.

This Appendix specifies:

- The communications equipment, procedures and protocols to be used for the Communication
- The Standards and Regulations to which the radio equipment shall comply
- The presentation of the Data to the Communication equipment
- The enquiry and download procedures and sequence of operations
- The Data to be transferred
- Potential

 interpretation of the
 Data transferred
 across the

 Communication
- The provisions for security data relating to the Communication

In this scenario, the time available for communication is limited, because the Communication is targeted and of a short-range design. Further, the same communication means for remote tachograph monitoring (RTM) may also be used by the competent control authorities for other applications (such as the maximal weights and dimensions for heavy goods vehicles defined in Directive (EU) 2015/719) and such operations may be separate or sequential at the discretion of the competent control authorities.

This Sub-appendix specifies:

- The communications equipment, procedures and protocols to be used for the Communication
- The Standards and Regulations to which the radio equipment shall comply
- The presentation of the Data to the Communication equipment
- The enquiry and download procedures and sequence of operations
- The Data to be transferred
- Potential interpretation of the Data transferred across the Communication
- The provisions for security data relating to the Communication

- The availability of the Data to the competent control authorities
- How the Remote early detection communication reader can request different freight and fleet data concepts

For clarification, this Appendix does not specify:

- the collection of the Data operation and management within the VU (which shall be a function of product design unless specified elsewhere within Regulation (EU) No. 165/2014)
 - the form of presentation of collected data to the agent of the competent control authorities, nor the criteria which shall be used by the competent control authorities to decide which vehicles to stop (which shall be a function of product design unless specified elsewhere within Regulation (EU) No. 165/2014 or a policy decision of the competent control authorities). For clarification: the Communication only makes the Data available to the competent control authorities in order that they may make

informed decisions

- The availability of the Data to the competent control authorities
- How the Remote early detection communication reader can request different freight and fleet data concepts

For clarification, this Subappendix does not specify:

- the collection of the Data operation and management within the VU (which shall be a function of product design unless specified elsewhere within Regulation (EU) No. 165/2014)
- the form of presentation of collected data to the agent of the competent control authorities, nor the criteria which shall be used by the competent control authorities to decide which vehicles to stop (which shall be a function of product design unless specified elsewhere within Regulation (EU) No. 165/2014 or a policy decision of the competent control authorities). For clarification: the Communication only makes the Data available to the competent control authorities in order that they may make

informed decisions

	- Data security	- Data security	
	provisions (such as encryption) concerning the content of the Data (which shall be specified within Appendix 11 Common Security Mechanisms).	provisions (such as encryption) concerning the content of the Data (which shall be specified within Subappendix 11 Common Security Mechanisms).	
	- detail of any data concepts other than RTM which may be obtained using the same architecture and equipment	- detail of any data concepts other than RTM which may be obtained using the same architecture and equipment	
	- detail of the behaviour and management between VU's and the DSRC-VU, nor the behaviour within the DSRC-VU (other than to provide the Data when so requested	- detail of the behaviour and management between VU's and the DSRC-VU, nor the behaviour within the DSRC-VU (other than to provide the Data when so requested by an REDCR).	
3	by an REDCR). The following acronyms and definitions specific to this Appendix are used in this appendix:	The following acronyms and definitions specific to this Subappendix are used in this appendix:	
3	Regulation (EC) No. 165/2014 definition: Regulation (EU) No. 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) No. 3821/85 on recording equipment in road transport and amending Regulation (EC) No. 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport	Regulation (EU) No. 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) No. 3821/85 on recording equipment in road transport and amending Regulation (EC) No. 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport	Definition suppressed (no reference to this Regulation remaining)
3	DSC definition	DSC definition	

3	DSC (n) identifier of a requirement for a specific DSRC appendix DSRC-VU definition DSRC-VU DSRC – Vehicle Unit. This is the "remote early detection facility" defined in Annex 1C. REDCR definition REDCR Remote early detection communication reader. This is the "remote early detection communication communication reader.	DSC (n) identifier of a requirement for a specific DSRC Sub-appendix DSRC-VU definition DSRC – Vehicle Unit. This is the "remote early detection facility" defined in Appendix 1C. REDCR definition REDCR Remote early detection communication reader. This is the "remote early detection communication communication reader.	
	equipment" defined in Annex 1C.	equipment" defined in Appendix 1C.	
3	The specification defined in this Appendix refers to and depends upon all or parts of the following regulations and standards. Within the clauses of this Appendix the relevant standards, or relevant clauses of standards, are specified. In the event of any contradiction the clauses of this Appendix shall take precedence. In the event of any contradiction where no specification is clearly determined in this Appendix, operating within ERC 70-03 (and tested against the appropriate parameters of EN 300 674-1) shall take precedence, followed in descending order of preference by EN 12795, EN 12253 EN 12834 and EN 13372, 6.2, 6.3, 6.4 and 7.1. Regulations and standards referenced in this Appendix are: [1] Regulation (EU) No. 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) No. 3821/85 on	The specification defined in this Sub-appendix refers to and depends upon all or parts of the following regulations and standards. Within the clauses of this Sub-appendix the relevant standards, or relevant clauses of standards, are specified. In the event of any contradiction the clauses of this Sub-appendix shall take precedence. In the event of any contradiction where no specification is clearly determined in this Sub-appendix, operating within ERC 70-03 (and tested against the appropriate parameters of EN 300 674-1) shall take precedence, followed in descending order of preference by EN 12795, EN 12253 EN 12834 and EN 13372, 6.2, 6.3, 6.4 and 7.1. Regulations and Standards referenced in this Sub-appendix are: [1] Reserved [2] Reserved	Suppressed references to regulations

	recording equipment in road		
	transport and amending		
	Regulation (EC) No. 561/2006		
	of the European Parliament		
	and of the Council on the		
	harmonisation of certain social		
	legislation relating to road		
	transport.		
	[2] Regulation (EC) No.		
	561/2006 of the European		
	Parliament and of the Council		
	of 15 March 2006 on the		
	harmonisation of certain social		
	legislation relating to road		
	transport and amending		
	Council Regulations (EEC) No.		
	3821/85 and (EC) No. 2135/98		
	and repealing Council		
	Regulation (EEC) No. 3820/85		
	(Text with EEA relevance).		
4.1	Regulation (EU) No. 165/2014	The supported scenarios	
	provides specific and	within which the	
	controlled scenarios within	Communication is to be used	
	which the Communication is	are:	
	to be used.		
	The scenarios supported are:		
	"Communication Profile 1:	"Communication Profile 1:	
	Roadside inspection using a	Roadside inspection using a	
	short range wireless	short range wireless	
	communication Remote Early	communication Remote Early	
	Detection Communication	Detection Communication	
	Reader instigating a physical	Reader instigating a physical	
	roadside inspection (master-:-	roadside inspection (master-:-	
	slave)	slave)	
		- 1 - 61 - 1	
	Reader Profile 1a: via a hand	Reader Profile 1a: via a hand	
	aimed or temporary roadside	aimed or temporary roadside	
	mounted and aimed Remote	mounted and aimed Remote	
	Early Detection	Early Detection	
	Communication	Communication	
	Reader Profile 1b: via a vehicle mounted and directed Remote	Reader Profile 1b: via a vehicle mounted and directed Remote	
	Early Detection	Early Detection	
	Communication Reader".	Communication Reader".	
4.1.1.1,	The VU shall be responsible to	The VU shall be responsible to	
DSC_12	keep updated every 60	keep updated every 60	
	seconds and maintain the data	seconds and maintain the data	
	to be stored in the VU,	to be stored in the VU,	
	without any involvement of	without any involvement of	
	the DSRC communication	the DSRC communication	

	function. The means by which this is achieved is internal to the VU, specified in Regulation (EU) No. 165/2014, Annex 1 C, section 3.19 "Remote communication for targeted roadside checks" and is not specified in this Appendix.	function. The means by which this is achieved is internal to the VU, specified in Appendix 1C, section 3.19 "Remote communication for targeted roadside checks" and is not specified in this Sub-appendix.	
4.1.1.2, DSC_14	The VU data shall be used as a basis to populate and update the Data, the means by which this is achieved, is specified in Annex 1.C, section 3.19 "Remote communication for targeted roadside checks" or if there is no such specification it is a function of product design and is not specified in this Appendix. For the design of the connection between DSRC-VU facility and the VU, please refer to section 5.6.	The VU data shall be used as a basis to populate and update the Data, the means by which this is achieved, is specified in Appendix 1C, section 3.19 "Remote communication for targeted roadside checks" or if there is no such specification it is a function of product design and is not specified in this Sub-appendix. For the design of the connection between DSRC-VU facility and the VU, please refer to section 5.6.	
4.1.1.3, DSC_15	The content and format of the Data shall be such that, once decrypted, it shall be structured and made available in the form and format specified in 5.4.4 of this Appendix (Data structures).	The content and format of the Data shall be such that, once decrypted, it shall be structured and made available in the form and format specified in 5.4.4 of this Subappendix (Data structures).	
4.1.1.4, DSC_16	The Data, having been kept frequently updated in accordance with the procedures determined in 4.1.1.1, shall be secured prior to presentation to the DSRC-VU, and presented as a secured data concept value, for temporary storage in the DSRC-VU as the current version of the Data. This data is transferred from the VUSM to the DSRC function VUPM. The VUSM and VUPM are functions and not necessarily physical entities. The form of physical instantiation to perform these functions shall be a matter of product design unless specified elsewhere in Regulation (EU) No. 165/2014.	The Data, having been kept frequently updated in accordance with the procedures determined in 4.1.1.1, shall be secured prior to presentation to the DSRC-VU, and presented as a secured data concept value, for temporary storage in the DSRC-VU as the current version of the Data. This data is transferred from the VUSM to the DSRC function VUPM. The VUSM and VUPM are functions and not necessarily physical entities. The form of physical instantiation to perform these functions shall be a matter of product design unless specified elsewhere in this Agreement.	

		I	
4.1.1.5,	Security data (securityData),	Security data (securityData),	
DSC_17	comprising the data required	comprising the data required	
	by the REDCR to complete its	by the REDCR to complete its	
	ability to decrypt the Data	ability to decrypt the Data	
	shall be supplied as defined in	shall be supplied as defined in	
	Appendix 11 Common Security	Sub-appendix 11 Common	
	Mechanisms and presented as	Security Mechanisms and	
	a data concept value, for	presented as a data concept	
	temporary storage in the	value, for temporary storage	
	DSRC-VU as the current	in the DSRC-VU as the current	
	version of securityData, in the	version of securityData, in the	
	form defined in this Appendix	form defined in this Sub-	
	section 5.4.4.	appendix section 5.4.4.	
4.1.1.6,	This profile covers the use	This profile covers the use	
DSC_18	case where an agent of the	case where an agent of the	
D3C_18	competent control authorities,	competent control authorities,	
	· · · · · · · · · · · · · · · · · · ·		
	uses a short range remote	uses a short range remote	
	communication Remote Early	communication Remote Early	
	Detection Communication	Detection Communication	
	Reader (5.8 GHz DSRC	Reader (5.8 GHz DSRC	
	interfaces operating within	interfaces operating within	
	ERC 70-03, and tested against	ERC 70-03, and tested against	
	the appropriate parameters of	the appropriate parameters of	
	EN 300 674-1 as described in	EN 300 674-1 as described in	
	section 5) (the REDCR) to	section 5) (the REDCR) to	
	remotely identify a vehicle	remotely identify a vehicle	
	which is potentially in	which is potentially in	
	which is potentially in violation of Regulation (EU)	which is potentially in violation of Regulation (EU)	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified,	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified,	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation	
4.2	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle	
4.2	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity	
4.2	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through	
4.2	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication,	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication,	
4.2	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified	
4.2	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication,	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication,	
4.2	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified	
4.2	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Sub-appendix 11 Common Security	
4.2	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Appendix 11 Common Security Mechanisms.	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Sub-appendix 11	
4.2 5.1, DSC_19	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Appendix 11 Common Security Mechanisms.	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Sub-appendix 11 Common Security Mechanisms. 2nd bullet point	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Appendix 11 Common Security Mechanisms.	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Sub-appendix 11 Common Security Mechanisms.	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Appendix 11 Common Security Mechanisms.	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Sub-appendix 11 Common Security Mechanisms. 2nd bullet point	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Sub-appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is stored in the VUSM memory.	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Sub-appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is stored in the VUSM memory.	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is stored in the VUSM memory. At intervals determined in	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Sub-appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is stored in the VUSM memory. At intervals determined in	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is stored in the VUSM memory. At intervals determined in 4.1.1.1 (DSC_12), the VU	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Sub-appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is stored in the VUSM memory. At intervals determined in 4.1.1.1 (DSC_12), the VU	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is stored in the VUSM memory. At intervals determined in 4.1.1.1 (DSC_12), the VU encrypts and replenishes the	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Sub-appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is stored in the VUSM memory. At intervals determined in 4.1.1.1 (DSC_12), the VU encrypts and replenishes the	
	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is stored in the VUSM memory. At intervals determined in 4.1.1.1 (DSC_12), the VU encrypts and replenishes the RTMdata concept (which	which is potentially in violation of Regulation (EU) No. 165/2014. Once identified, the agent of the competent control authorities who is controlling the interrogation decides whether the vehicle should be stopped. To give the possibility to verify the authenticity and integrity of downloaded data through the remote communication, the secured Data is verified and decrypted in accordance with Sub-appendix 11 Common Security Mechanisms. 2nd bullet point The secured data is stored in the VUSM memory. At intervals determined in 4.1.1.1 (DSC_12), the VU encrypts and replenishes the RTMdata concept (which	

	determined below in this Appendix) held in the memory of the DSRC-VU. The operation of the security module is	determined below in this Sub- appendix) held in the memory of the DSRC-VU. The operation of the security module is	
	defined in Appendix 11	defined in Sub-appendix 11	
	Common Security Mechanisms and outwith the scope of this	Common Security Mechanisms and outwith the scope of this	
	Appendix, save that it shall be	Sub-appendix, save that it	
	required to provide updates to the VU Communication facility	shall be required to provide updates to the VU	
	each time the VUSM data	Communication facility each	
5.1, DSC_19	changes. 9 th bullet point	time the VUSM data changes. 9 th bullet point	
3.1, D3C_13	DSRC-VU. This is the	DSRC-VU. This is the	
	function, within or connected	function, within or connected	
	to the antenna and in	to the antenna and in	
	communication with the VU through a wired or wireless	communication with the VU through a wired or wireless	
	(BLE) connection, which holds	(BLE) connection, which holds	
	the current data (VUPM-data)	the current data (VUPM-data)	
	and manages the response to	and manages the response to	
	an interrogation across the 5.8	an interrogation across the 5.8	
	GHz DSRC medium. Disconnection of the DSRC	GHz DSRC medium. Disconnection of the DSRC	
	facility or interference during	facility or interference during	
	normal vehicle operation with	normal vehicle operation with	
	the functioning of the DSRC	the functioning of the DSRC	
	facility shall be construed as a	facility shall be construed as a	
	violation of Regulation (EU) No. 165/2014.	violation of this Agreement.	
5.1, DSC_19	9 th bullet point	9 th bullet point	
	Security module	Security module	
	(REDCR) (SM-REDCR) is the	(REDCR) (SM-REDCR) is the	
	function used to decrypt and check integrity of the data	function used to decrypt and check integrity of the data	
	originating from the VU. The	originating from the VU. The	
	means by which this is	means by which this is	
	achieved is determined in	achieved is determined in	
	Appendix 11 Common	Sub-appendix 11 Common	
	Security Mechanisms, and is not defined in this Appendix.	Security Mechanisms, and is not defined in this Sub-	
	not defined in this Appendix.	appendix.	
5.1, DSC_19	10th bullet point	10th bullet point	
	The DSRC facility	The DSRC facility	
	(REDCR) (DSRC-REDCR)	(REDCR) (DSRC-REDCR)	
	function comprises a 5.8 GHz transceiver and associated	function comprises a 5.8 GHz transceiver and associated	
	firmware and software which	firmware and software which	
	manages the Communication	manages the Communication	
	with the DSRC-VU according to	with the DSRC-VU according to	
	this Appendix.	this Sub-appendix.	

	T	T	
5.1, DSC_19	The DSRC antenna shall be	The DSRC antenna shall be	
	connected to the DSRC-VU	connected to the DSRC-VU	
	facility either directly within	facility either directly within	
	the module mounted to or	the module mounted to or	
	close to the windshield, or	close to the windshield, or	
	through a dedicated cable	through a dedicated cable	
	constructed in a manner to	constructed in a manner to	
	make illegal disconnection	make illegal disconnection	
	difficult. Disconnection of or	difficult. Disconnection of or	
	interference with the	interference with the	
	functioning of Antenna shall	functioning of Antenna shall	
	be a violation of Regulation	be a violation of Regulation	
	(EU) No. 165/2014. Deliberate	(EU) No. 165/2014. Deliberate	
	masking or otherwise	masking or otherwise	
	detrimentally affecting the	detrimentally affecting the	
	operational performance of	operational performance of	
	the Antenna shall be	the Antenna shall be	
	construed as a violation of	construed as a violation of this	
	Regulation (EU) No. 165/2014.	Agreeement.	
5.1, DSC_22	Last paragraph	Last paragraph	
	A display and/or notification	A display and/or notification	
	function is used to present the	function is used to present the	
	results of the remote	results of the remote	
	communication function to	communication function to	
	the agent of the competent	the agent of the competent	
	control authorities. A display	control authorities. A display	
	may be provided on a screen,	may be provided on a screen,	
	as a printed output, an audio	as a printed output, an audio	
	signal, or a combination of	signal, or a combination of	
	such notifications. The form of	such notifications. The form of	
	such display and/or	such display and/or	
	notification is a matter of the	notification is a matter of the	
	requirements of the agents of	requirements of the agents of	
	the competent control	the competent control	
	authorities and equipment	authorities and equipment	
	design and is not specified	design and is not specified	
	within this Appendix.	within this Sub-appendix.	
5.1, DSC_23	The design and form factor of	The design and form factor of	
_	the REDCR shall be a function	the REDCR shall be a function	
	of commercial design,	of commercial design,	
	operating within ERC 70-03,	operating within ERC 70-03,	
	and the design and	and the design and	
	performance specifications	performance specifications	
	defined in this Appendix,	defined in this Sub-appendix,	
	(section 5.3.2), thus providing	(section 5.3.2), thus providing	
	the marketplace maximum	the marketplace maximum	
	flexibility to design and	flexibility to design and	
	provide equipment to cover	provide equipment to cover	
	the specific interrogation	the specific interrogation	
	scenarios of any particular	scenarios of any particular	
	competent control authority.	competent control authority.	

_ ,			
5.1, DSC_24	The design and form factor of	The design and form factor of	
	the DSRC-VU and its	the DSRC-VU and its	
	positioning inside or outside	positioning inside or outside	
	the VU shall be a function of	the VU shall be a function of	
	commercial design, operating	commercial design, operating	
	within ERC 70-03 and the	within ERC 70-03 and the	
	design and performance	design and performance	
	specifications defined in this	specifications defined in this	
	Appendix (section 5.3.2) and	Sub-appendix (section 5.3.2)	
	within this Clause (5.1).	and within this Clause (5.1).	
5.2.2,	Data received across the 5.8	Data received across the 5.8	
DSC_26	GHz interface shall carry the	GHz interface shall carry the	
	meaning and import defined	meaning and import defined	
	in 5.4.4 and 5.4.5 below and	in 5.4.4 and 5.4.5 below and	
	only that meaning and import,	only that meaning and import,	
	and shall be understood	and shall be understood	
	within the objectives defined	within the objectives defined	
	therein. In accordance with	therein. In accordance with	
	the provisions of Regulation	the provisions of Regulation	
	(EU) No. 165/2014, the Data	(EU) No. 165/2014, the Data	
	shall be used only to provide	shall be used only to provide	
	relevant information to a		
		relevant information to a	
	competent control authority	competent control authority	
	to assist them to determine	to assist them to determine	
	which vehicle should be	which vehicle should be	
	stopped for physical	stopped for physical	
	inspection, and shall be	inspection, and shall be	
	subsequently destroyed in	subsequently destroyed in	
	accordance with Article 9 of	accordance with the	
	Regulation (EU) No. 165/2014.	legislation applicable at	
		national level.	
5.2.1	Step c)	Step c)	
	c. The VUSM function	c. The VUSM function	
	secures the data in	secures the data in	
	accordance with the	accordance with the	
	procedures determined in	procedures determined in	
	Appendix 11.	Sub-appendix 11.	
5.3.2, Table	Item D2, 3 rd column	Item D2, 3 rd column	
14.1	No other specific requirement	No other specific requirement	
	within this Annex	within this Appendix	
5.3.2, Table	Item D11b, 4 th column	Item D11b, 4 th column	
14.1	Extended requirement for	Extended requirement for	
	horizontal angles up to ±45°,	horizontal angles up to ±45°,	
	due to the use cases defined	due to the use cases defined	
	in this annex.	in this Appendix.	
5.3.2, Table	Item U12a, 4 th column	Item U12a, 4 th column	
14.2	Greater that the specified	Greater that the specified	
	value range for horizontal	value range for horizontal	
	angles up to ±45°, due to the	angles up to ±45°, due to the	
	1 6 1 1 1 1 1		
1	use cases defined in this	use cases defined in this	

E 2 2 2	DCC 22 In the test	DCC 22 In the test	
5.3.3.2,	DSC_33 In the test	DSC_33 In the test	
DSC_33	environment in a workshop	environment in a workshop	
	(see section 6.3), a DSRC-VU	(see section 6.3), a DSRC-VU	
	antenna, affixed according to	antenna, affixed according to	
	5.1 above, shall successfully	5.1 above, shall successfully	
	connect with a standard test	connect with a standard test	
	communication and	communication and	
	successfully provide an RTM	successfully provide an RTM	
	transaction as defined within	transaction as defined within	
	this Appendix, at a distance	this Sub-appendix, at a	
	between 2 and 10 meters,	distance between 2 and 10	
	better than 99% of the time,	meters, better than 99% of	
	averaged over 1000 read	the time, averaged over 1000	
	interrogations.	read interrogations.	
5.4.4,	DSC 37 The semantic	DSC 37 The semantic	
DSC_37	structure of the Data when	structure of the Data when	
D3C_37	passed across the 5.8 GHz	passed across the 5.8 GHz	
	DSRC interface shall be	DSRC interface shall be	
	consistent with what	consistent with what	
	described in this Appendix.	described in this Sub-	
	The way these data are	appendix. The way these data	
	structured is specified in this	are structured is specified in	
	clause.	this clause.	
5.4.4,	DSC_38 The payload	DSC_38 The payload	
DSC_38	(RTM data) consists of the	(RTM data) consists of the	
	concatenation of	concatenation of	
	1.	1.	
	EncryptedTachographP	EncryptedTachographP	
	ayload data, which is the	ayload data, which is the	
	encryption of the	encryption of the	
	TachographPayload defined in	TachographPayload defined in	
	ASN.1 in section 5.4.5. The	ASN.1 in section 5.4.5. The	
	method of encryption is	method of encryption is	
	described in Appendix 11	described in Sub-appendix 11	
	dSRCSecurityData,	dSRCSecurityData,	
	specified in Appendix 11.	specified in Sub-appendix 11.	
5.4.4,	See current tachograph	See new proposed tachograph	
DSC_40	payload definition at the end	payload definition at the end	
	of this document	of this document	
5.4.4,	RtmData definition	RtmData definition	
DSC_40	RtmData ::= SEQUENCE {	RtmData ::= SEQUENCE {	
	encryptedTachographP	encryptedTachographP	
	ayload OCTET STRING	ayload OCTET STRING	
	(SIZE(67)) (CONSTRAINED BY {	(SIZE(67)) (CONSTRAINED BY {	
	calculated encrypting	calculated encrypting	
	TachographPayload as per	TachographPayload as per	
	Appendix 11}),	Sub-appendix 11}),	
	DSRCSecurityData	DSRCSecurityData	
	OCTET STRING	OCTET STRING	
	}	}	
5.4.5, Table	See current table at the end of	See new proposed table at the	
14.3	this document	end of this document	
		and a supplemental to the	İ

F 4.0	E II	E 0	
5.4.8,	Full tests that include	Full tests that include	
DSC_53	securing the data, need to	securing the data, need to	
	be carried out as defined in	be carried out as defined in	
	Appendix 11 Common	Sub-appendix 11 Common	
	Security Mechanisms, by	Security Mechanisms, by	
	authorised persons with	authorised persons with	
	access to security procedures,	access to security procedures,	
	using the normal GET	using the normal GET	
	command as defined above.	command as defined above.	
5.4.8,	Commissioning and periodic	Commissioning and periodic	
DSC_54	inspection tests that require	inspection tests that require	
	decrypting and	decrypting and	
	comprehension of the	comprehension of the	
	decrypted data content shall	decrypted data content shall	
	be undertaken as specified in	be undertaken as specified in	
	Appendix 11 Common Security	Sub-appendix 11 Common	
	Mechanisms and Appendix 9,	Security Mechanisms and	
	Type Approval List of	Appendix 9, Type Approval List	
	Minimum required tests.	of Minimum required tests.	
	However, the basic DSRC	However, the basic DSRC	
	communication can be tested	communication can be tested	
	by the command ECHO. Such	by the command ECHO. Such	
	tests may be required on		
	commissioning, at periodic	tests may be required on commissioning, at periodic	
	inspection, or otherwise to the	inspection, or otherwise to the	
	requirement of the competent	requirement of the competent	
	control authority or	control authority or	
	Regulation (EU) No. 165/2014	Regulation (EU) No. 165/2014	
	(See 6 below)	(See 6 below)	
5.5.4,	DSC_62 The payload (OWS	DSC_62 The payload (OWS	
DSC_62	data) consists of the	data) consists of the	
550_02	concatenation of	concatenation of	
	EncryptedOwsPayload	EncryptedOwsPayload	
	data, which is the encryption	data, which is the encryption	
	of the OwsPayload defined in	of the OwsPayload defined in	
	ASN.1 in section 5.5.5. The	ASN.1 in section 5.5.5. The	
	method of encryption shall be	method of encryption shall be	
	the same adopted for the	the same adopted for the	
	RtmData, which is specified in	RtmData, which is specified in	
	Appendix 11	Sub-appendix 11	
	2. dSRCSecurityData,	2. dSRCSecurityData,	
	calculated with the same	calculated with the same	
	algorithms adopted for the	algorithms adopted for the	
	RtmData, which is specified in	RtmData, which is specified in	
	Appendix 11.	Sub-appendix 11.	
5.5.5,	OwsData definition	OwsData definition	
		OwsData :: = SEQUENCE {	
DSC 63	OwsData :: = SEQUENCE {	OWSData SEQUENCE 1	
DSC_63	OwsData :: = SEQUENCE { encryptedOwsPayload		
DSC_63	encryptedOwsPayload	encryptedOwsPayload	
DSC_63	encryptedOwsPayload OCTET STRING (SIZE(51))	encryptedOwsPayload OCTET STRING (SIZE(51))	
DSC_63	encryptedOwsPayload	encryptedOwsPayload	

	OwsPayload as per Appendix 11}),	OwsPayload as per Sub- appendix 11}), DSRCSecurityData OCTET STRING }	
5.7.2.1, DSC_81	DSC_81 Encryption and signature errors shall be handled as defined in Appendix 11 Common Security Mechanisms and are not present in any error messages associated with the DSRC transfer of data.	DSC_81 Encryption and signature errors shall be handled as defined in Subappendix 11 Common Security Mechanisms and are not present in any error messages associated with the DSRC transfer of data.	

Current TachographPayload definition

```
TachographPayload ::= SEQUENCE {
           tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 155091
           tp15638SpeedingEvent
                                  BOOLEAN, -- 1= Irregularities in speed (see Annex 1C)
                                                   -- 1= Invalid card usage (see Annex 1C)
           tp15638DrivingWithoutValidCard BOOLEAN,
           tp15638DriverCard
                                         BOOLEAN, -- 0= Indicates a valid driver card (see Annex
1C)
           tp15638CardInsertion
                                         BOOLEAN, -- 1= Card insertion while driving (see Annex
1C)
           tp15638MotionDataError
                                        BOOLEAN, -- 1= Motion data error (see Annex 1C)
           tp15638VehicleMotionConflict BOOLEAN, -- 1= Motion conflict (see Annex 1C)
           tp156382ndDriverCard
                                         BOOLEAN, -- 1= Second driver card inserted (see Annex
1C)
           tp15638CurrentActivityDriving BOOLEAN, -- 1= other activity selected;
                                                    -- 0= driving selected
           tp15638LastSessionClosed BOOLEAN, -- 1= improperly, 0= properly, closed
           tp15638PowerSupplyInterruption INTEGER (0..127), -- Supply interrupts in the last 10
days
                                          INTEGER (0..255),-- eventFaultType as per data dictionary
           tp15638SensorFault
-- All subsequent time related types as defined in Annex 1C.
           tp15638TimeAdjustment
                                        INTEGER(0..4294967295), -- Time of the last time
adjustment
           tp15638LatestBreachAttempt INTEGER(0..4294967295), -- Time of last breach attempt
           tp15638LastCalibrationData INTEGER(0..4294967295), -- Time of last calibration data
                                        INTEGER(0..4294967295), -- Time of previous calibration
           tp15638PrevCalibrationData
data
```

New proposed TachographPayload definition

```
TachographPayload ::= SEQUENCE {
            {\tt tp15638VehicleRegistrationPlate\ LPN\ --\ Vehicle\ Registration\ Plate\ as\ per\ EN\ 15509^{\tt l}}
            tp15638SpeedingEvent
                                             BOOLEAN, -- 1= Irregularities in speed (see Appendix
1C)
            tp15638DrivingWithoutValidCard BOOLEAN,
                                                         -- 1= Invalid card usage (see Appendix 1C)
            tp15638DriverCard
                                   BOOLEAN, -- 0= Indicates a valid driver card (see
Appendix 1C)
                                            BOOLEAN, -- 1= Card insertion while driving (see
            tp15638CardInsertion
Appendix 1C)
            tp15638MotionDataError
                                             BOOLEAN, -- 1= Motion data error (see Appendix 1C)
            tp15638VehicleMotionConflict BOOLEAN, -- 1= Motion conflict (see Appendix 1C)
            tp156382ndDriverCard
                                            BOOLEAN, -- 1= Second driver card inserted (see
Appendix 1C)
            tp15638CurrentActivityDriving BOOLEAN, -- 1= other activity selected;
                                                        -- 0= driving selected
            tp15638LastSessionClosed BOOLEAN, -- 1= improperly, 0= properly, closed
            {\tt tp15638PowerSupplyInterruption\quad INTEGER\ (0..127),\ --\ Supply\ interrupts\ in\ the\ last\ 10}
days
            tp15638SensorFault
                                             INTEGER (0..255), -- eventFaultType as per data dictionary
-- All subsequent time related types as defined in Appendix 1C.
            tp15638TimeAdjustment
                                            INTEGER(0..4294967295), -- Time of the last time
adjustment
                                         INTEGER(0..4294967295), -- Time of last breach attempt

INTEGER(0..4294967295) -- Time of last calibration data
            tp15638LatestBreachAttempt
            tp15638LastCalibrationData
            tp15638PrevCalibrationData
data
```

Current Table 14.3

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
RTM1 Vehicle Registration Plate	The VU shall set the value of the tp15638VehicleRegistrationPlate data element RTM1 from the recorded value of the data type VehicleRegistrationIdentification as defined in Appendix 1 VehicleRegistrationIdentification	Vehicle Registration Plate expressed as a string of characters	tp15638VehicleRegstrationPlate LPN,Vehicle RegistrationPlate imported from ISO 14906 with the limitation specified in EN 15509 which is a SEQUENCE comprising Country Code followed by an alphabet indicator followed by the plate number itself, which is always 14 octets (padded with zero's) so the EN 15509 LPN type length is always 17 octets, of which 14 are the "real" plate
RTM2 Speeding Event	The VU shall generate a boolean value for data element RTM2 tp15638SpeedingEvent. The tp15638SpeedingEvent value shall be calculated by the VU from the number of Over Speeding Events recorded in the VU in the last 10 days of occurrence, as defined in Annex 1C. If there is at least one tp15638SpeedingEvent in the last 10 days of occurrence, the tp15638SpeedingEvent value shall be set to TRUE.	1 (TRUE) - Indicates irregularities in speed within last 10 days of occurrence	tp15638speedingEvent BOOLEAN,

DTM	The Miller of the control of the colors	A (TDLIE) La diserca i avalida	. 156000
RTM3	The VU shall generate a boolean	1 (TRUE) = Indicates invalid	tp15638DrivingWithoutVa
Driving Without	value for data element RTM3	card usage	lidCard
Valid Card	tp15638DrivingWithoutValidCard.		BOOLEAN,
	The VU shall assign a value of True to		
	the tp15638DrivingWithoutValidCard		
	variable if the VU data has recorded		
	at least one event in the last 10 days		
	of occurrence of type "Driving without		
	an appropriate card" event as defined		
	in Annex 1C.		
	ELSE if there are no events in the last		
	10 days of occurrence, the		
	tp15638DrivingWithoutValidCard		
RTM4	The VU shall generate a boolean	0 (FALSE) = Indicates a	tp15638DriverCard
Valid Driver Card	value for data element RTM4	valid driver card	BOOLEAN,
Tana Brivoi Gara	tp15638DriverCard on the basis of the	valia dirvoi cara	,
	data stored in the VU and defined in		
	Appendix 1.		
	Appendix 1.		
	If no valid driver cord is present the		
	If no valid driver card is present the		
	VU shall set the variable to TRUE		
	FLOE 'S a scalled debugge and in processes		
	ELSE if a valid driver card is present	. (75.15)	
RTM5	The VU shall generate a boolean	1 (TRUE) = Indicates card	tp15638CardInsertion
Card Insertion while	value for data element RTM5.	insertion while driving within	BOOLEAN,
Driving		last 10 days of occurrence	
	The VU shall assign a value of TRUE		
	to the tp15638CardInsertion variable if		
	the VU data has recorded in the last		
	10 days of occurrence at least one		
	event of type "Card insertion while		
	driving." as defined in Annex 1C.		
	ELSE if there are no such events in		
	the last 10 days of occurrence, the		
	tp15638CardInsertion variable shall		
RTM6	The VU shall generate a boolean	1 (TRUE) = Indicates motion	tp15638motionDataError
Motion Data Error	value for data element RTM6.	data error within last 10 days	BOOLEAN,
		of occurrence	
	The VU shall assign a value of TRUE		
	to the tp15638MotionDataError		
	variable if the VU data has in the last		
	10 days of occurrence recorded at		
	least one event of type "Motion data		
	error" as defined in Annex 1C.		
	FLOE Williams and the state of		
	ELSE if there are no such events in		
İ	the last 10 days of occurrence, the		

RTM7 Vehicle Motion Conflict	The VU shall generate a boolean value for data element RTM7. The VU shall assign a value of TRUE to the tp15638vehicleMotionConflict variable if the VU data has in the last 10 days recorded at least one event of type Vehicle Motion Conflict (value '0A'H). ELSE if there are no events in the last	1 (TRUE) = Indicates motion conflict within last 10 days of occurrence	tp15638vehicleMotionCon flict BOOLEAN,
RTM8 2nd Driver Card	The VU shall generate a boolean value for data element RTM8 on the basis of Annex 1C ("Driver Activity Data" CREW and CO-DRIVER). If a 2nd valid driver card is present the VU shall set the variable to TRUE ELSE if a 2nd valid driver card is not present the VU shall set the variable	1 (TRUE) = Indicates a second driver card inserted	tp156382ndDriverCard BOOLEAN,
RTM9 Current Activity	The VU shall generate a boolean value for data element RTM9. If the current activity is recorded in the VU as any activity other than "DRIVING" as defined in Annex 1C the VU shall set the variable to TRUE ELSE if the current activity is	1 (TRUE) = other activity selected; 0 (FALSE) = driving selected	tp15638currentActivityD riving BOOLEAN
RTM10 Last Session Closed	The VU shall generate a boolean value for data element RTM10. If the last card session was not properly closed as defined in Annex 1C the VU shall set the variable to TRUE. ELSE if the last card session was	1 (TRUE) = improperly closed 0 (FALSE) = properly closed	tp15638lastSessionClose d BOOLEAN

RTM11	The VU shall generate an integer	Number of power supply	tp15638powerSupplyInter
Power Supply	value for data element RTM11.	interruptions in last 10 days	ruption
Interruption	value for data element (CTWTT).	of occurrence	INTEGER (0127),
шин	The VU shall assign a value for the	or occurrence	11126211 (0.11217)
	tp15638PowerSupplyInterruption		
	variable equal to the longest power		
	supply interruption" according to		
	Article 9, Reg (EU) 165/2014 of type		
	"Power supply interruption" as defined		
	in Annex 1C.		
	ELSE if in the last 10 days of		
RTM12	The VU shall generate an integer	sensor fault one octet as	tp15638SensorFault
Sensor Fault	value for data element RTM12.	per data dictionary	INTEGER (0255),
	The VU shall assign to the variable		
	sensorFault a value of:		
	4 16 4 61 (05)11 0		
	- 1 if an event of type '35'H Sensor		
	fault has been recorded in the last		
	10 days,		
	- 2 if an event of type GNSS receiver		
	fault (either internal or external with		
	enum values '36'H or		
	'37'H) has been recorded in the last		
	10 days.		
	0. %		
	- 3 if an event of type '0E'H Communication error with the external		
	GNSS facility event has been		
	recorded in the last 10 days.		
	recorded in the last 10 days.		
	-4 If both Sensor Fault and GNSS		
	receiver faults have been recorded in		
	the last 10 days.		
	·		
	-5 If both Sensor Fault and		
	Communication error with the external		
	GNSS facility event have been		
	recorded in the last 10 days.		
	-6 If both GNSS receiver fault and		
	Communication error with the external		
	GNSS facility event have been		
	recorded in the last 10 days.		

DTM40	The Million of the second of the	The state of the state of	15620ml 3.11
RTM13 Time Adjustment	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM13 on the basis of the presence of Time Adjustment data as defined in Annex 1C. The VU shall assign the value of time at which the last time adjustment data event has occurred.	Time of the last time adjustment	tp15638TimeAdjustment INTEGER(04294967295),
	ELSE if no "Time Adjustment" event.		
RTM14 Security Breach Attempt	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM14 on the basis of the presence of a Security breach attempt event as defined in Annex 1C. The VU shall set the value of the time	Time of last breach attempt Default value =0x00FF	<pre>tp15638LatestBreachAtte mpt INTEGER(04294967295),</pre>
RTM15	of the latest security breach attempt event recorded by the VU. ELSE if no "security breach attempt" event as defined in Annex 1C is The VU shall generate an integer	Time of last calibration data	tp15638LastCalibrationD
Last Calibration	value (timeReal from Appendix 1) for data element RTM15 on the basis of the presence of Last Calibration data as defined in Annex 1C.	Time of last campration data	ata INTEGER(04294967295),
	The VU shall set the value of time of the latest two calibrations (RTM15 and RTM16), which are set in VuCalibrationData defined in Appendix 1.		
RTM16 Previous Calibration	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM16 of the calibration record preceding that of the last calibration	Time of previous calibration data	tp15638PrevCalibrationD ata INTEGER(04294967295),
	ELSE if there has been no previous calibration the VU shall set the value of RTM16 to 0.		

RTM17 Date Tachograph Connected RTM18 Current Speed	For data element RTM17 the VU shall generate an integer value (timeReal from Appendix 1). The VU shall set the value of the time of the initial installation of the VU. The VU shall extract this data from the VuCalibrationData (Appendix 1) from the vuCalibrationRecords with The VU shall generate an integer value for data element RTM18. The VU shall set the value for RTM16 to the last current recorded speed at the time of the latest undate of the	Date tachograph connected Last current recorded speed	tp15638DateTachoConnect ed INTEGER(04294967295), tp15638CurrentSpeed INTEGER (0255),
RTM19 Timestamp	to the last current recorded speed at the time of the latest update of the RtmData. For data element RTM19 the VU shall generate an integer value (timeReal from Appendix 1). The VU shall set the value for RTM19 to the time of the latest update of the RtmData.	Timestamp of current TachographPayload record	tp15638Timestamp INTEGER(04294967295),

New proposed Table 14.3

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
KTW Data Liement	Action performed by the vo		ASN.1 definition of data
RTM1 Vehicle Registration Plate	The VU shall set the value of the tp15638VehicleRegistrationPlate data element RTM1 from the recorded value of the data type VehicleRegistrationIdentification as defined in Sub-appendix 1 VehicleRegistrationIdentification	Vehicle Registration Plate expressed as a string of characters	tp15638VehicleRegstrati onPlate LPN,Vehicle Registration Plate imported from ISO 14906 with the limitation specified in EN 15509 which is a SEQUENCE comprising Country Code followed by an alphabet indicator followed by the plate number itself, which is always 14 octets (padded with zero's) so the EN 15509 LPN type length is always 17 octets, of which 14

RTM2	The VIII shall generate a healesn	1 (TRUE) Indicates	+n1E629anoodingErron+
Speeding Event	The VU shall generate a boolean value for data element RTM2	1 (TRUE) - Indicates	tp15638speedingEvent BOOLEAN,
Speeding Event		irregularities in speed within	BOOLEAN,
	tp15638SpeedingEvent.	last 10 days of occurrence	
	The thits Cooking Cyant value		
	The tp15638SpeedingEvent value		
	shall be calculated by the VU from the		
	number of Over Speeding Events		
	recorded in the VU in the last 10 days		
	of occurrence, as defined in Appendix		
	1C.		
	If there is at least one		
	tp15638SpeedingEvent in the last 10		
	days of occurrence, the		
	•		
	tp15638SpeedingEvent value shall be		
	set to TRUE.		
	ELSE if there are no events in the last		
RTM3	The VU shall generate a boolean	1 (TRUE) = Indicates invalid	tp15638DrivingWithoutVa
Driving Without	value for data element RTM3	card usage	lidCard
Valid Card	tp15638DrivingWithoutValidCard.	•	BOOLEAN,
	The VU shall assign a value of True to		
	the tp15638DrivingWithoutValidCard		
	variable if the VU data has recorded		
	at least one event in the last 10 days		
	of occurrence of type "Driving without		
	an appropriate card" event as defined		
	in Appendix 1C.		
	iii Appelluix 10.		
	ELSE if there are no events in the last		
	10 days of occurrence, the		
	tn15638DrivingWithoutValidCard		
RTM4	The VU shall generate a boolean	0 (FALSE) = Indicates a	tp15638DriverCard
Valid Driver Card	value for data element RTM4	valid driver card	BOOLEAN,
	tp15638DriverCard on the basis of the		,
	data stored in the VU and defined in		
	Sub-appendix 1.		
	Cab appoint i.		
	If no valid driver card is present the		
	VU shall set the variable to TRUE		
	ELSE if a valid driver card is present		

	1		
RTM5	The VU shall generate a boolean	1 (TRUE) = Indicates card	tp15638CardInsertion
Card Insertion while	value for data element RTM5.	insertion while driving within	BOOLEAN,
Driving	The VIII shall engine a value of TDIII	last 10 days of occurrence	
	The VU shall assign a value of TRUE to the tp15638CardInsertion variable if		
	the VU data has recorded in the last		
	10 days of occurrence at least one		
	event of type "Card insertion while		
	driving." as defined in Appendix 1C.		
	arring. as asimed in 7 pportain 10.		
	ELSE if there are no such events in		
	the last 10 days of occurrence, the		
	tp15638CardInsertion variable shall		
	be set to FALSE.		
RTM6	The VU shall generate a boolean	1 (TRUE) = Indicates motion	tp15638motionDataError
Motion Data Error	value for data element RTM6.	data error within last 10 days	BOOLEAN,
		of occurrence	
	The VU shall assign a value of TRUE		
	to the tp15638MotionDataError		
	variable if the VU data has in the last		
	10 days of occurrence recorded at least one event of type "Motion data		
	error" as defined in Appendix 1C.		
	error as defined in Appendix 1C.		
	ELSE if there are no such events in		
	the last 10 days of occurrence, the		
RTM7	•	1 /TDUE) Indicates motion	tp15638vehicleMotionCon
Vehicle Motion	The VU shall generate a Boolean value for data element RTM7.	1 (TRUE) = Indicates motion conflict within last 10 days of	flict
Conflict	value for data element KTIVIT.	occurrence	BOOLEAN,
Commet	The VU shall assign a value of TRUE	occurrence	BOOLEAN,
	to the tp15638vehicleMotionConflict		
	variable if the VU data has in the last		
	10 days recorded at least one event		
	of type Vehicle Motion Conflict		
	(value '0A'H).		
	ELSE if there are no events in the last		
	10 days of occurrence, the		
RTM8	The VU shall generate a boolean	1 (TRUE) = Indicates a	tp156382ndDriverCard
2nd Driver Card	value for data element RTM8 on the	second driver card inserted	BOOLEAN,
	basis of Appendix 1C ("Driver Activity		
	Data" CREW and CO-DRIVER).		
	If a 2nd valid driver and in present the		
	If a 2nd valid driver card is present the		
	VU shall set the variable to TRUE		
	ELSE if a 2nd valid driver card is not		
	present the VU shall set the variable		
	hieselit tile AO stigli zet tile Agligbie		

RTM9	The VU shall generate a Boolean	1 (TRUE) = other activity	tp15638currentActivityD
Current Activity	value for data element RTM9.	selected:	riving
- Currone Activity	value for data element (Time.	0 (FALSE) = driving selected	BOOLEAN
	If the current activity is recorded in	o (171202) = anting colocica	20022111
	the VU as any activity other than		
	"DRIVING" as defined in Appendix 1C		
	the VU shall set the variable to TRUE		
	the vo shall set the variable to TNOL		
	ELSE if the current activity is		
	recorded in the VU as "DRIVING" the		
RTM10		1 (TDLIE) improperly closed	+-15C201+C
	The VU shall generate a Boolean	1 (TRUE) = improperly closed	=
Last Session Closed	value for data element RTM10.	0 (FALSE) = properly closed	d
			BOOLEAN
	If the last card session was not		
	properly closed as defined in		
	Appendix 1C the VU shall set the		
	variable to TRUE.		
	ELSE if the last card session was		
RTM11	The VU shall generate an integer	Number of power supply	tp15638powerSupplyInter
Power Supply	value for data element RTM11.	interruptions in last 10 days	ruption
Interruption		of occurrence	INTEGER (0127),
•	The VU shall assign a value for the		
	tp15638PowerSupplyInterruption		
	variable equal to the longest power		
	supply interruption" according to		
	Article 9, Reg (EU) 165/2014 of type		
	"Power supply interruption" as defined		
	in Appendix 1C.		
	ELSE if in the last 10 days of		

RTM12	The VU shall generate an integer	sensor fault one octet as	tp15638SensorFault
Sensor Fault	value for data element RTM12.	per data dictionary	INTEGER (0255),
		, , , , , , , , , , , , , , , , , , , ,	, , , , ,
	The VU shall assign to the variable		
	sensorFault a value of:		
	- 1 if an event of type '35'H Sensor		
	fault has been recorded in the last		
	10 days,		
	- 2 if an event of type GNSS receiver		
	fault (either internal or external with		
	enum values '36'H or		
	'37'H) has been recorded in the last		
	10 days.		
	- 3 if an event of type '0E'H		
	Communication error with the external		
	GNSS facility event has been		
	recorded in the last 10 days.		
	-4 If both Sensor Fault and GNSS		
	receiver faults have been recorded in		
	the last 10 days.		
	-5 If both Sensor Fault and		
	Communication error with the external		
	GNSS facility event have been		
	recorded in the last 10 days.		
	-6 If both GNSS receiver fault and		
	Communication error with the external		
	GNSS facility event have been		
	recorded in the last 10 days.		
RTM13	The VU shall generate an integer	Time of the last time	tp15638TimeAdjustment
Time Adjustment	value (timeReal from Sub-appendix 1)	adjustment	INTEGER(04294967295),
	for data element RTM13 on the basis	,	
	of the presence of Time Adjustment		
	data as defined in Appendix 1C.		
	The VU shall assign the value of time		
	at which the last time adjustment data		
	event has occurred.		
	ELSE if no "Time Adjustment" event.		
	ELSE if no "Time Adjustment" event.		

RTM14	The VIII shall generate an integer	Time of lost breech offers	+n156201 a+ aa+D
Security Breach	The VU shall generate an integer value (timeReal from Sub-appendix 1)	Time of last breach attempt Default value =0x00FF	tp15638LatestBreachAtte
Attempt	for data element RTM14 on the basis	Delault value =0x001 l	INTEGER (04294967295),
Attempt	of the presence of a Security breach		INTEGER (04254507255),
	attempt event as defined in Appendix		
	1C.		
	The VU shall set the value of the time		
	of the latest security breach attempt		
	event recorded by the VU.		
	ELSE if no "security breach attempt"		
	event as defined in Appendix 1C is		
RTM15	The VU shall generate an integer	Time of last calibration data	tp15638LastCalibrationD
Last Calibration	value (timeReal from Sub-appendix 1)		ata
	for data element RTM15 on the basis		INTEGER(04294967295),
	of the presence of Last Calibration		
	data as defined in Appendix 1C.		
	The VU shall set the value of time of		
	the latest two calibrations (RTM15		
	and RTM16), which are set in		
	VuCalibrationData defined in Sub-		
	appendix 1.		
	The VU shall set the value for RTM15 to the timeReal of the latest		
RTM16	R TWT5 to the timeReal of the latest	Time of previous calibration	tp15638PrevCalibrationD
Previous Calibration	The VU shall generate an integer value	data	ata
	(timeReal from Sub-appendix 1) for		INTEGER(04294967295),
	data element RTM16 of the calibration		
	record preceding that of the last		
	calibration		
	ELSE if there has been no previous		
	calibration the VU shall set the value		
	of RTM16 to 0.		
RTM17	For data element RTM17 the VU shall	Date tachograph	tp15638DateTachoConnect
Date Tachograph	generate an integer value (timeReal	connected	ed
Connected	from Sub-appendix 1).		INTEGER(04294967295),
	The VU shall set the value of the time		
	of the initial installation of the VU.		
	The VU shall extract this data from		
	the VuCalibrationData (Sub-appendix		
	1) from the vuCalibrationRecords with		
	CalibrationPurpose equal to: '03'H		

RTM18 Current Speed	The VU shall generate an integer value for data element RTM18. The VU shall set the value for RTM16 to the last current recorded speed at the time of the latest update of the RtmData.	Last current recorded speed	tp15638CurrentSpeed INTEGER (0255),
RTM19 Timestamp	For data element RTM19 the VU shall generate an integer value (timeReal from Sub-appendix 1). The VU shall set the value for RTM19 to the time of the latest update of the RtmData.	Timestamp of current TachographPayload record	tp15638Timestamp INTEGER(04294967295),

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 15 FOR AETR V0.2 20190113

Point or article	Text Appendix 15	Proposed text for AETR	Comments
TITLE/TABLE OF	(Title) APPENDIX 15. MIGRATION:	SUB-APPENDIX 15.	
CONTENTS	MANAGING THE CO- EXISTENCE OF EQUIPMENT GENERATIONS	MIGRATION: MANAGING THE CO-EXISTENCE OF EQUIPMENT GENERATIONS	
1	For the purposes of this Appendix, the following	For the purposes of this Subappendix, the following	
1	definitions are used. smart tachograph system	definitions are used. smart tachograph system	
	definition smart tachograph system: as defined by this Annex (chapter	definition smart tachograph system: as defined by this Appendix	
1	1: definition bbb); first generation tachograph system definition first generation tachograph system: as defined by this	(chapter 1: definition bbb); first generation tachograph system definition first generation tachograph system: as defined in the	
	Regulation (article 2: definition 1);	introduction of this Appendix;	
1	second generation tachograph system definition second generation tachograph system: as defined by this Regulation (article 2: definition 7);	second generation tachograph system definition second generation tachograph system: as defined in the introduction of this Appendix;	
1	introduction date definition introduction date: as defined by this Annex (chapter 1: definition ccc);	introduction date definition introduction date: as defined by this Appendix (chapter 1: definition ccc);	
1	Intelligent Dedicated Equipment definition Intelligent Dedicated Equipment (IDE): equipment used to perform data downloading, as defined in Appendix 7 of this Annex.	Intelligent Dedicated Equipment definition Intelligent Dedicated Equipment (IDE): equipment used to perform data downloading, as defined in Sub-appendix 7 of this Appendix.	
2.1	The preamble of this Annex provides an overview of the transition between the first and the second generation tachograph systems.	The preamble of this Appendix provides an overview of the transition between the first and the second generation tachograph systems.	
2.2	It is understood that first generation tachograph cards are interoperable with first	It is understood that first generation tachograph cards are interoperable with first	

	generation vehicle units (in compliance with Annex 1B of Regulation (EEC) No 3821/85), while second generation tachograph cards are interoperable with second generation vehicle units (in compliance with Annex 1C of this Regulation). In addition, the requirements below shall apply.	generation vehicle units (in compliance with Appendix 1B, while second generation tachograph cards are interoperable with second generation vehicle units (in compliance with Appendix 1C of this Regulation). In addition, the requirements below shall apply.	
2.4.2, MIG_013	MIG_013 Data shall be downloaded from a first generation card inserted in a second generation vehicle unit using the data download protocol defined in Appendix 7 of this Annex. The vehicle unit shall send commands to the card exactly the same manner as a first generation vehicle unit, and downloaded data shall respect the format defined for first generation cards.	MIG_013 Data shall be downloaded from a first generation card inserted in a second generation vehicle unit using the data download protocol defined in Subappendix 7 of this Appendix. The vehicle unit shall send commands to the card exactly the same manner as a first generation vehicle unit, and downloaded data shall respect the format defined for first generation cards.	
2.4.3, MIG_014	MIG_014 Outside the frame of drivers' control by non EU control authorities, data shall be downloaded from second generation vehicle units using the second generation security mechanisms, and the data download protocol specified in Appendix 7 of this Annex.	MIG_014 Outside the frame of drivers' control by non EU control authorities, data shall be downloaded from second generation vehicle units using the second generation security mechanisms, and the data download protocol specified in Sub-appendix 7 of this Appendix.	
4, MIG_022	MIG_022 After the introduction date, Member States shall only issue second generation tachograph cards.	MIG_022 After the introduction date, Contracting Parties shall only issue second generation tachograph cards.	

LIST OF PROPOSED CHANGES TO ANNEX 1C APPENDIX 16 FOR AETR V0.2 20190113

Point or	Toyt Annondiy 16	Proposed text for	Comments
article	Text Appendix 16	AETR	Comments
TITLE/TABLE	(Title)		
OF	APPENDIX 16. ADAPTOR FOR	SUB-APPENDIX 16. ADAPTOR	
CONTENTS	M 1 AND N1 CATEGORY	FOR M 1 AND N1 CATEGORY	
	VEHICLES	VEHICLES	
		(update table of contents	
		according to the change in the	
2.1,	The adaptor shall provide a	titles) The adaptor shall provide a	
ADA_001	connected VU with secured	connected VU with secured	
71571_001	motion data permanently	motion data permanently	
	representative of vehicle	representative of vehicle	
	speed and distance travelled.	speed and distance travelled.	
	The adaptor is only intended	The adaptor is only intended	
	for those vehicles that are	for those vehicles that are	
	required to be equipped with	required to be equipped with	
	recording equipment in	control device in compliance	
	compliance with this	with this Agreement.	
	Regulation.	It shall be installed and used	
	It shall be installed and used	only in those types of vehicle	
	only in those types of vehicle defined in definition yy)	defined in definition yy) 'adaptor' of Appendix IC	
	'adaptor' of Annex IC where it	where it is not mechanically	
	is not mechanically possible to	possible to install any other	
	install any other type of	type of existing motion sensor	
	existing motion sensor which	which is otherwise compliant	
	is otherwise compliant with	with the provisions of this	
	the provisions of this Annex	Appendix and its Sub-	
	and its Appendixes 1 to 16.	Appendixes 1 to 16.	
	The adaptor shall not be	The adaptor shall not be	
	mechanically interfaced to a	mechanically interfaced to a	
	moving part of the vehicle, but	moving part of the vehicle, but	
	connected to the speed/distance impulses	connected to the speed/distance impulses	
	which are generated by	which are generated by	
	integrated sensors or	integrated sensors or	
	alternative interfaces.	alternative interfaces.	
2.1,	ADA_002 A type approved	ADA_002 A type approved	
ADA_002	motion sensor (according to	motion sensor (according to	
	the provisions of this Annex IC,	the provisions of this	
	section 8, Type approval of	Appendix IC, section 8, Type	
	recording equipment and	approval of control device and	
	tachograph cards) shall be fitted into the adaptor	tachograph cards) shall be fitted into the adaptor	
	housing, which shall also	housing, which shall also	
	include a pulse converter	include a pulse converter	

device inducing the incoming pulses to the embedded motion sensor. The embedded motion sensor itself shall be connected to the VU, so that the interface between the VU and the adaptor shall be compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in device inducing the incoming pulses to the embedded motion sensor. The embedded motion sensor itself shall be connected to the VU, so that the interface between the VU and the adaptor shall be compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Appendix. Security related requirements specified in
motion sensor. The embedded motion sensor itself shall be connected to the VU, so that the interface between the VU and the adaptor shall be compliant with the requirements set out in ISO16844-3. 3.3, ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in motion sensor. The embedded motion sensor itself shall be connected to the VU, so that the interface between the VU and the adaptor shall be compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Appendix. Security related requirements specified in
motion sensor itself shall be connected to the VU, so that the interface between the VU and the adaptor shall be compliant with the requirements set out in ISO16844-3. 3.3, ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in motion sensor itself shall be connected to the VU, so that the interface between the VU and the adaptor shall the interface between the VU and the adaptor shall be compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Appendix. Security related requirements specified in
connected to the VU, so that the interface between the VU and the adaptor shall be compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in Connected to the VU, so that the interface between the VU and the VU and the AU, so that the interface between the VU and the adaptor shall be compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Appendix. Security related requirements specified in
the interface between the VU and the adaptor shall be compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in the motion sensor generic security related requirements specified in the interface between the VU and the interface between the VU and the interface between the VU and the adaptor shall be compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Sub-Appendix 10 of this Appendix. Security related requirements specified in
and the adaptor shall be compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in with the requirements shall be compliant with the requirements specified in and the adaptor shall be compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Appendix. Security related requirements specified in
compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in Compliant with the requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Appendix 10 of this Appendix. Security related requirements specified in
requirements set out in ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in r
ISO16844-3. ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in Sub-Appendix. Security related requirements specified in Sub-Appendix 10 of this Appendix. Security related requirements specified in Sub-Appendix 10 of this Appendix. Security related requirements specified in Sub-Appendix 10 of this Appendix. Security related requirements specified in Sub-Appendix 10 of this Appendix. Security related requirements specified in Sub-Appendix 10 of this Appendix. Security related requirements specified in Sub-Appendix 10 of this Appendix.
ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in ADA_004 The adaptor shall not be security certified according to the motion sensor generic security target defined in Sub-Appendix 10 of this Appendix. Security related requirements specified in
not be security certified according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in not be security certified according to the motion sensor generic security target defined in Sub-Appendix 10 of this Appendix. Security related requirements specified in
according to the motion sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in according to the motion sensor generic security target defined in Sub-Appendix 10 of this Appendix. Security related requirements specified in
sensor generic security target defined in Appendix 10 of this Annex. Security related requirements specified in sensor generic security target defined in Sub-Appendix 10 of this Appendix. Security related requirements specified in
defined in Appendix 10 of this Annex. Security related requirements specified in defined in Sub-Appendix 10 of this Appendix. Security related requirements specified in
Annex. Security related requirements specified in this Appendix. Security related requirements specified in
requirements specified in requirements specified in
section 4.4 of this Appendix section 4.4 of this Sub-
shall apply instead. Appendix shall apply instead.
title 3. Requirements for the 3. Requirements for the
recording equipment when an control device when an
adaptor is installed adaptor is installed
The requirements in the The requirements in the
following Chapters indicate following Chapters indicate
how the requirements of this how the requirements of this
Annex shall be understood Appendix shall be understood
when an adaptor is used. The when an adaptor is used. The
related requirement numbers related requirement numbers
of Annex IC are provided of Appendix IC are provided
between brackets. between brackets.
, ADA_005 ADA_005 The recording ADA_005 The control device
equipment of any vehicle of any vehicle fitted with an
fitted with an adaptor must adaptor must comply with all
comply with all the provisions the provisions of this
of this Annex, except Appendix, except otherwise
otherwise specified in this specified in this Sub-Appendix.
Appendix.
, ADA_006 ADA_006 When an adaptor ADA_006 When an adaptor
is installed, the recording is installed, the control
equipment includes cables, device includes cables, the
the adaptor (including a adaptor (including a motion
motion sensor), and a VU sensor), and a VU [01].
[01].
ADA_007 The detection of ADA_007 The detection of
function of the recording function of the control
equipment is modified as device is modified as
follows: follows:
- the "power supply - the "power supply
interruption" event shall be interruption" event shall be

	triggered by the VU, while	triggered by the VU, while	
	not in calibration mode, in	not in calibration mode, in	
	case of any interruption	case of any interruption	
	exceeding 200 milliseconds	exceeding 200 milliseconds	
	of the power supply of the	of the power supply of the	
	embedded motion sensor	embedded motion sensor	
	[79]	[79]	
	- the "motion data	- the "motion data	
	error" event shall be	error" event shall be	
	triggered by the VU in case	triggered by the VU in case	
	of interruption of the	of interruption of the	
	normal data flow between	normal data flow between	
	the embedded motion	the embedded motion	
	sensor and the VU and/or	sensor and the VU and/or	
	in case of data integrity or	in case of data integrity or	
	data authentication error	data authentication error	
	during data exchange	during data exchange	
	between the embedded	between the embedded	
	motion sensor and the VU	motion sensor and the VU	
	[83]	[83]	
	- the "security breach	- the "security breach	
	attempt" event shall be	attempt" event shall be	
	triggered by the VU for any	triggered by the VU for any	
	other event affecting the	other event affecting the	
	security of the embedded	security of the embedded	
	motion sensor, while not in	motion sensor, while not in	
	calibration mode [85]	calibration mode [85]	
	- the "recording	- the "recording	
	equipment" fault shall be	equipment" fault (fault of	
	triggered by the VU, while	the control device) shall be	
	not in calibration mode, for	triggered by the VU, while	
	any fault of the embedded	not in calibration mode, for	
	motion sensor [88]	any fault of the embedded	
		motion sensor [88]	
3, ADA_008	ADA_008 The adaptor	ADA_008 The adaptor	
	faults detectable by the	faults detectable by the	
	recording equipment shall	control device shall be	
	be those related with the	those related with the	
	embedded motion sensor	embedded motion sensor	
	[88].	[88].	
4.1,	ADA_012 The adaptor input	ADA_012 The adaptor input	
ADA_012	interface shall be able, if	interface shall be able, if	
	applicable, to multiply or	applicable, to multiply or	
	divide the frequency pulses	divide the frequency pulses	
	of the incoming speed	of the incoming speed	
	pulses by a fixed factor, to	pulses by a fixed factor, to	
	adapt the signal to the k	adapt the signal to the k	

	f		
	factor range defined by this	factor range defined by this	
	Annex (4000 to 25000	Appendix (4000 to 25000	
	pulses/km). This fixed	pulses/km). This fixed	
	factor may only be	factor may only be	
	programmed by the	programmed by the	
	adaptor manufacturer, and	adaptor manufacturer, and	
	the approved workshop	the approved workshop	
	performing the adaptor	performing the adaptor	
	installation.	installation.	
4.7,	ADA_027 A descriptive	ADA 027 A descriptive	
ADA_027	plaque shall be affixed to	plaque shall be affixed to	
11011_021		1 -	
	the adaptor and shall show	the adaptor and shall show	
	the following details:	the following details:	
	- name and address of	- name and address of	
	the manufacturer of the	the manufacturer of the	
	adaptor,	adaptor,	
	- manufacturer's part	 manufacturer's part 	
	number and year of	number and year of	
	manufacture of the	manufacture of the	
	adaptor,	adaptor,	
	- approval mark of the	- approval mark of the	
	adaptor type or of the	adaptor type or of the	
	recording equipment type	control device type	
	including the adaptor,	including the adaptor,	
	- the date on which	- the date on which	
	the adaptor has been	the adaptor has been	
		I	
	installed,	installed, - the vehicle	
	- the vehicle	identification number of the	
	identification number of	vehicle on which it has been	
	the vehicle on which it has	installed.	
	been installed.		
5,title	5. Installation of the	5. Installation of the control	
	recording equipment when	device when an adaptor is	
	an adaptor is used	used	
6.1,	ADA_035 When an adaptor is	ADA_035 When an adaptor is	
ADA_035	used, each periodic inspection	used, each periodic inspection	
	(periodic inspections means in	(periodic inspections means in	
	compliance with Requirement	compliance with Requirement	
	[409] through to Requirement	[409] through to Requirement	
	[413] of Annex 1C) of the	[413] of Appendix 1C) of the	
	recording equipment shall	control device shall include	
	include the following checks:	the following checks:	
	- that the adaptor carries the	- that the adaptor carries the	
	appropriate type approval	appropriate type approval	
	markings,	markings,	
	- that the seals on the adaptor	- that the seals on the adaptor	
	and its connections are intact,	and its connections are intact,	

	 - that the adaptor is installed as indicated on the installation plaque, - that the adaptor is installed as specified by the adapter and/or vehicle manufacturer, - that mounting an adaptor is authorised for the inspected vehicle. 	 that the adaptor is installed as indicated on the installation plaque, that the adaptor is installed as specified by the adapter and/or vehicle manufacturer, that mounting an adaptor is authorised for the inspected vehicle. 	
7, title	7. Type approval of recording equipment when an adaptor is used	7. Type approval of control device when an adaptor is used	
7.1, ADA_037	ADA_037 Recording equipment shall be submitted for type approval complete, with the adaptor [425].	ADA_037 Control device shall be submitted for type approval complete, with the adaptor [425].	
7.1, ADA_038	ADA_038 Any adaptor may be submitted for its own type approval, or for type approval as a component of a recording equipment.	ADA_038 Any adaptor may be submitted for its own type approval, or for type approval as a component of a control device.	
7.2, ADA_040	ADA_040 A functional certificate of an adaptor or of recording equipment including an adaptor shall be delivered to the adaptor manufacturer only after all the following minimum functional tests have been successfully passed.	ADA_040 A functional certificate of an adaptor or of control device including an adaptor shall be delivered to the adaptor manufacturer only after all the following minimum functional tests have been successfully passed.	
		1	1