Informal document No. 2

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 defined as synonyms and use both of them as it corresponds. Continue to use recording equipment in Appendix 1C.	To be discussed
INTRODUCTION	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 vehicles registered for the first time, and second	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 generation recording equipment and tachograph cards requirements.	Starting date of deployment of the first generation digital tachograph on the territory of the AETR Contracting Parties to be discussed.

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

	the data, stored in the tachograph, which have been locked by that transport undertaking;	the data, stored in the tachograph, which have been locked by that transport undertaking;	
1, n)	n) "continuous driving time" is computed within the recording equipment as[1]: the continuous driving time is computed as the current accumulated driving times of a particular driver, since the end of his last AVAILABILITY or BREAK/REST or UNKNOWN[2] period of 45 minutes or more (this period may have been split according to Regulation (EC) N°. 561/2006). The computations involved take into account, as needed, past activities stored on the driver card. When the driver has not inserted his card, the computations involved are based on the data memory recordings related to the current period where no card was inserted and related to the relevant slot;	n) "continuous driving time" is computed within the recording equipment as[3]: the continuous driving time is computed as the current accumulated driving times of a particular driver, since the end of his last AVAILABILITY or BREAK/REST or UNKNOWN[4] period of 45 minutes or more (this period may have been split according to this Agreement). The computations involved take into account, as needed, past activities stored on the driver card. When the driver has not inserted his card, the computations involved are based on the data memory recordings related to the current period where no card was inserted and related to the relevant slot;	The AETR defines splits in driving periods of four and a half hours (in Article 7).
1, o)	o) "control card" means: a tachograph card issued by the authorities of a Member State to a national competent control authority which identifies the control body and, optionally, the control officer, and which allows access to the data stored in the data memory or in the driver cards	o) "control card" means: a tachograph card issued by the authorities of a Contracting Party to a national competent control authority which identifies the control body and, optionally, the control officer, and which allows access to the data stored in the data 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 workshop cards for reading, printing and/or downloading; It shall also give access to the roadside calibration checking function and to data on the remote early detection communication reader.	and, optionally, in the workshop cards for reading, printing and/or downloading; It shall also give access to the roadside calibration checking function and to data on the remote early detection communication reader.	
1, p)	p) "cumulative break time" is computed within the recording equipment as1: the cumulative break from driving time is computed as the current accumulated AVAILABILITY or BREAK/REST or UNKNOWN2 times of 15 minutes or more of a particular driver, since the end of his last AVAILABILITY or BREAK/REST or UNKNOWN2 period of 45 minutes or more (this period may have been split according to Regulation (EC) N°. 561/2006). The computations involved take into account, as needed, past activities stored on the driver card. Unknown periods of negative duration (start of unknown period > end of unknown period) due to time overlaps between two different recording equipments, are not taken into account for the computation. When the driver has not inserted his card, the computations involved are based on the data memory recordings related to the current period where no card was inserted and related to the relevant slot	p) "cumulative break time" is computed within the recording equipment as1: the cumulative break from driving time is computed as the current accumulated AVAILABILITY or BREAK/REST or UNKNOWN2 times of 15 minutes or more of a particular driver, since the end of his last AVAILABILITY or BREAK/REST or UNKNOWN2 period of 45 minutes or more (this period may have been split according to according to this Agreement. The computations involved take into account, as needed, past activities stored on the driver card. Unknown periods of negative duration (start of unknown period > end of unknown period) due to time overlaps between two different recording equipments, are not taken into account for the computation. When the driver has not inserted his card, the computations involved are based on the data memory recordings related to the current period where no card was inserted and related to the relevant slot	The AETR defines splits in driving periods of four and a half hours (in Article 7).
1, s)	s) "downloading" means: the copying, together with the digital signature, of a part, or of a complete set, of data files recorded in the data memory of the vehicle	s) "downloading" means: the copying, together with the digital signature, of a part, or of a complete set, of data files recorded in the data memory of the vehicle	The AETR defines what rules must be complied with, instead of Regulation (EC) N°. 561/2006).

	unit or in the memory of a tachograph card, provided that this process does not alter or delete any stored data; Manufacturers of smart tachograph vehicle units and manufacturers of equipment designed and intended to download data files shall take all reasonable steps to ensure that the downloading of such data can be performed with the minimum delay by transport undertakings or drivers. The downloading of the detailed speed file may not be necessary to establish compliance with Regulation (EC) N°. 561/2006, but may be used for other purposes such as accident investigation.	unit or in the memory of a tachograph card, provided that this process does not alter or delete any stored data; Manufacturers of smart tachograph vehicle units and manufacturers of equipment designed and intended to download data files shall take all reasonable steps to ensure that the downloading of such data can be performed with the minimum delay by transport undertakings or drivers. The downloading of the detailed speed file may not be necessary to establish compliance with this Agreement but may be used for other purposes such as accident investigation.	
1, t)	t) “driver card” means: a tachograph card, issued by the authorities of a Member State to a particular driver, which identifies the driver and allows for the storage of driver activity data;	t) “driver card” means: a tachograph card, issued by the authorities of a Contracting Party to a particular driver, which identifies the driver and allows for the storage of driver activity data;	
1, u)	u) “effective circumference of the wheels” means: the average of the distances travelled by each of the wheels moving the vehicle (driving wheels) in the course of one complete rotation. The measurement of these distances shall be made under standard test conditions as defined under requirement 414 and is expressed in the form “l = … mm”. Vehicle manufacturers may replace the measurement of these distances by a theoretical	u) “effective circumference of the wheels” means: the average of the distances travelled by each of the wheels moving the vehicle (driving wheels) in the course of one complete rotation. The measurement of these distances shall be made under standard test conditions as defined under requirement 414 and is expressed in the form “l = … mm”. Vehicle manufacturers may replace the measurement of these 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)	Footnote 3 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, 30/01/1976, p. 0001 - 0005.	~~Footnote 6~~ ~~Directive 76/114/EEC, 18/12/1975; OJ No L 024, 30/01/1976, p. 0001 - 0005.~~	Replaced with VIN definition in vv)
1, xx)	xx) “workshop card” means: a tachograph card issued by the authorities of a Member State to designated staff of a tachograph manufacturer, a	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	

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

	of interfering with, the proper and secure operation of the recording equipment and the provisions of this Regulation.	of interfering with, the proper and secure operation of the recording equipment and the provisions of this Agreement.	
2.1, 7)	07) The recording equipment provides selective access rights to data and functions according to user's type and/or identity. The recording equipment records and stores data in its data memory, in the remote communication facility and in tachograph cards. This is done 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 , 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.	07) The recording equipment provides selective access rights to data and functions according to user's type and/or identity. The recording equipment records and stores data in its data memory, in the remote communication facility and in tachograph cards. ~~This is done 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 , 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.~~	
2.4, 14)	14) In order to achieve the system security, the following components shall meet the security requirements specified in their Protection Profiles, as required in Appendix 10: - vehicle unit, - tachograph card, - motion sensor, - external GNSS facility (this Profile is only needed and applicable for the external GNSS variant).	14) In order to achieve the system security, the following components shall meet the security requirements specified in their Protection Profiles, as required in Sub-appendix 10: - vehicle unit, - tachograph card, - motion sensor, - external GNSS facility (this Profile is only needed and applicable for the external GNSS variant).	
3.1, 17)	17) First generation tachograph cards shall be considered as non-valid by the recording equipment, after the possibility of using first generation tachograph cards has been suppressed by a	17) First generation tachograph cards shall be considered as non-valid by the recording equipment, after the possibility of using first generation tachograph cards has been suppressed by a	

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

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

	supply cut-off of less than 28 days.	power-supply cut-off of less than 28 days.	
3.12.2, 101)	101) The recording equipment shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A and part B.	101) The recording equipment shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part A and 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 driving time), - the related GNSS accuracy, date and time if applicable; - the vehicle odometer value.	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), - the related GNSS accuracy, date and time if applicable; - the vehicle odometer value.	
3.12.8 117)	See Annex 1	See Annex 1	
3.12.9 118)	See Annex 2	See Annex 2	
3.12.10 120)	120) The following data shall be recorded for each of these calibrations: - purpose of calibration (activation, first installation, 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	120) The following data shall be recorded for each of these calibrations: - 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	

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

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

	communication, as specified in Appendix 14.	communication, as specified in 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. 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 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 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:	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. 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. 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 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	Change reference to Regulation (EU) 2016/679 ("General Data Protection Regulation") as appropriate.

	- 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 (Sub-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.	

	Other data may also be output in addition to the set of selected existing data, considered as the minimum list, provided they cannot be considered as personal data. The recording equipment shall have the capacity to communicate the driver consent status to other platforms in the vehicle network. When the ignition of the vehicle is ON, these data shall be permanently broadcasted.	Other data may also be output in addition to the set of selected existing data, considered as the minimum list, provided they cannot be considered as personal data. The recording equipment shall have the capacity to communicate the driver consent status to other platforms in the vehicle network. When the ignition of the vehicle is ON, these data shall be permanently broadcasted.	
3.20, 201)	The serial link interface as specified in Annex 1B to Regulation (EEC) N°. 3821/85, as last amended, can continue to equip tachographs for back compatibility. Anyhow, the driver consent is still required in case personal data are transmitted.	The serial link interface as specified in Appendix 1B of this Agreement can continue to equip tachographs for back compatibility. Anyhow, the driver consent is still required in case personal data are transmitted.	
3.21, 203)	203) In addition, the calibration function shall allow to supress the use of first generation tachograph cards in the recording equipment, provided the conditions specified in Appendix 15 are met.	203) In addition, the calibration function shall allow to supress the use of first generation tachograph cards in the recording equipment, provided the conditions specified in Sub-appendix 15 are met.	
3.21, 206)	206) The calibration function shall be able to input necessary data through the calibration/downloading connector in accordance with the calibration protocol defined in Appendix 8. The calibration function may also input necessary data through other means.	206) The calibration function shall be able to input necessary data through the calibration/downloading connector in accordance with the calibration protocol defined in Sub-appendix 8. The calibration function may also input necessary data through other means.	
3.22, 209)	209) The roadside calibration checking function shall also allow controlling the selection of the I/O mode of the calibration I/O signal line specified in Appendix 6, via	209) The roadside calibration checking function shall also allow controlling the selection of the I/O mode of the calibration I/O signal line specified in Sub-appendix 6,	

	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.	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.	
4.1, 227)	227) the words “Driver card” or “Control card” or “Workshop 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 the card.	227) the words “Driver card” or “Control card” or “Workshop 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 the card.	
4.1, 228)	228) the name of the Member State issuing the card (optional);	228) the name of the Contracting Party issuing the card (optional);	
4.1, 229)	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:	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 (2nd paragraph) The tachograph cards functions, commands and logical structures, fulfilling data storage requirements are specified in Appendix 2.	4.5 (2nd 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.	
4.5.2.2, 250)	250) Tachograph cards shall be able to store the application identification data objects specified in Appendix 2.	250) Tachograph cards shall be able to store the application identification data objects specified in Sub-appendix 2.	
4.5.2.3, 251)	251) Tachograph cards shall be able to store the following extended length information data object: - in the case the tachograph card supports extended length fields, the extended length information data object specified in Appendix 2.	251) Tachograph cards shall be able to store the following extended length information data object: - in the case the tachograph card supports extended length fields, the extended length information data object specified in Sub-appendix 2.	
4.5.2.4, 252)	252) Tachograph cards shall be able to store the following extended length information data objects: - in the case the tachograph card supports extended length fields, the extended length information data objects specified in Appendix 2.	252) Tachograph cards shall be able to store the following extended length information data objects: - in the case the tachograph card supports extended length fields, the extended length information data objects specified in Sub-appendix 2.	
4.5.3.1.2, 254)	254) The driver card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A.	254) The driver card shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part A.	
4.5.3.1.3, 255)	255) The driver 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.	255) The driver 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.	
4.5.3.1.6, 259)	259) The driver card shall be able to store the following driving licence data: – issuing Member State, issuing authority name, driving licence number (at the date of the issue of the card).	259) The driver card shall be able to store the following driving licence data: – issuing Contracting Party, issuing authority name, driving licence number (at the date of the issue of the card).	
4.5.3.1.7 261)	261) The driver card shall be able to store the following data for these events:	261) 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.	– 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.	
4.5.3.1.8, 264)	264) The driver card shall be able to store the following data for these faults: – Fault code, – Date and time of beginning of the fault (or of card insertion if the fault was on-going at that time), – Date and time of end of the fault (or of card withdrawal if the fault was on-going at that time), VRN and registering Member State of vehicle in which the fault happened.	264) The driver card shall be able to store the following data for these faults: – Fault code, – Date and time of beginning of the fault (or of card insertion if the fault was on-going at that time), – Date and time of end of the fault (or of card withdrawal if the fault was on-going at that time), VRN and registering Contracting Party of vehicle in which the fault happened.	
4.5.3.1.10, 269)	269) The driver card shall be able to store, for each calendar day where the card has been used, and for each period of use of a given vehicle that day (a period of use includes all consecutive insertion / withdrawal cycle of the card in the vehicle, as seen from the card point of view), the following data: – date and time of first use of the vehicle (i.e. first card insertion for this period of use of the vehicle, or 00h00 if the period of use is on-going at that time),	269) The driver card shall be able to store, for each calendar day where the card has been used, and for each period of use of a given vehicle that day (a period of use includes all consecutive insertion / withdrawal cycle of the card in the vehicle, as seen from the card point of view), the following data: – date and time of first use of the vehicle (i.e. first card insertion for this period of use of the vehicle, or 00h00 if the period of use is on-going at that time),	

	– vehicle odometer value at that time, – 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.	– vehicle odometer value at that time, – 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 Contracting Party of the vehicle.	
4.5.3.1.12, 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.	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 Contracting Party.	
4.5.3.1.13, 274)	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.	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 of the vehicle in which the control happened. Note: card downloading will only be recorded if performed through a recording equipment.	

4.5.3.2.2, 279)	279) The driver card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part B.	279) The driver card shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part B.	
4.5.3.2.3, 280)	280) The driver 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.	280) The driver 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.	
4.5.3.2.6, 284)	284) The driver card shall be able to store the following driving licence data: – issuing Member State, issuing authority name, – driving licence number (at the date of the issue of the card).	284) The driver card shall be able to store the following driving licence data: – issuing Contracting Party, issuing authority name, driving licence number (at the date of the issue of the card).	
4.5.3.2.7, 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.	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 Contracting Party of vehicle in which the event happened.	
4.5.3.2.8, 289)	289) The driver card shall be able to store the following data for these faults: – Fault code, – Date and time of beginning of the fault	289) The driver card shall be able to store the following data for these faults: – Fault code, – Date and time of beginning of the fault	

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

4.5.4.2.3, 333)	333) 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.	333) 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.	
4.5.5.1.2, 358)	358) The control card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A.	358) The control card shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part A.	
4.5.5.1.3, 359)	359) The control 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).	359) The control 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).	
4.5.5.1.5, 361)	361) The control card shall be able to store the following 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 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.	361) The control card shall be able to store the following 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 roadside calibration checking), - period downloaded (if any), - VRN and Contracting Party registering authority of the controlled vehicle, card number and card issuing Contracting Party of the driver card controlled.	
4.5.5.2.2, 364)	364) The control card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part B.	364) The control card shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part B.	
4.5.5.2.3, 365)	365) The control card shall be able to store the following card identification data: - card number,	365) The control 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).	- issuing Contracting Party, issuing authority name, issue date, card beginning of validity date, card expiry date (if any).	
4.5.5.2.5, 367)	367) The control card shall be able to store the following 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 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.	367) The control card shall be able to store the following 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 roadside calibration checking) - period downloaded (if any), - VRN and Contracting Party registering authority of the controlled vehicle, card number and card issuing Contracting Party of the driver card controlled.	
4.5.6.1.2, 370)	370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part A.	370) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part A.	
4.5.6.1.3, 371)	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).	371) 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)	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 vehicle,	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 vehicle,	

	card number and card issuing Member State (in case of card downloading).	card number and card issuing Contracting Party (in case of card downloading).	
4.5.6.2.2, 376)	376) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Appendix 11 part B.	376) The company card shall be able to store a number of cryptographic keys and certificates, as specified in Sub-appendix 11 part B.	
4.5.6.2.3, 377)	377) 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).	377) 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).	
4.5.6.2.5, 379)	379) 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 vehicle, - card number and card issuing Member State (in case of card downloading).	379) 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 vehicle, - card number and card issuing Contracting Party (in case of card downloading).	
5.1, 385)	385) Vehicle manufacturers or fitters shall activate the installed recording equipment at the latest before the vehicle is used in scope of Regulation (EC) N°. 561/2006.	385) Vehicle manufacturers or fitters shall activate the installed recording equipment at the latest before the vehicle is used in scope of this Agreement.	The AETR defines what rules must be complied with, instead of Regulation (EC) N°. 561/2006).
5.1, 392)	392) Installation shall be followed by a calibration. The first calibration may not necessarily include entry of the vehicle registration number (VRN), when it is not known by the approved workshop having to undertake this calibration. In these	392) Installation shall be followed by a calibration. The first calibration may not necessarily include entry of the vehicle registration number (VRN), when it is not known by the approved workshop having to undertake this calibration. In these	The AETR defines what rules must be complied with, instead of Regulation (EC) N°. 561/2006).

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

	Regulation (EU) N° 165/2014 and shall be prepared to produce them to competent national authorities whenever need be.	Agreement and shall be prepared to produce them to competent national authorities whenever need be.	
6	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 in Chapter 5.3 of this annex.	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 in Chapter 5.3 of this Appendix.	Reference to Regulation (EU) N°165/2014 can be removed (not needed)
6.1	The Member States 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: – 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.	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 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 Sub-appendix 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	

	with workshop or control body name or with the fitter or control officer's name would Member States so decide.	with workshop or control body name or with the fitter or control officer's name would Contracting Parties so decide.	
7, 424)	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.	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 Appendix), – a functional certificate, – and an interoperability certificate (if	

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

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

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 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 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

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

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

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

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

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

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

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

	card holder (Annex 1C requirement 306 and 352).	card holder (Appendix 1C requirement 306 and 352).	
2.41	Generation 1: 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). Generation 2: Certificate ::= OCTET STRING (SIZE(204..341)) **Value assignment**: See Appendix 11	Generation 1: Certificate ::= OCTET STRING (SIZE(194)) **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(204..341)) **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. **vehicleRegistrationInformation** 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	

	Annex 1C requirements 266, 299, 320, and 343.	Appendix 1C requirements 266, 299, 320, and 343.	
2.61	Information, stored in a driver card related to the identification of the application of the card (Annex 1C requirement 253 and 278).	Information, stored in a driver card related to the identification of the application of the card (Appendix 1C requirement 253 and 278).	
2.62	Information, stored in a driver card, related to the identification of the cardholder (Annex 1C requirement 256 and 281).	Information, stored in a driver card, related to the identification of the cardholder (Appendix 1C requirement 256 and 281).	
2.63	The plain text information and the MAC to be transmitted via DSRC from the tachograph to the Remote Interrogator (RI), see Appendix 11 Part B chapter 13 for details.	The plain text information and the MAC to be transmitted via DSRC from the tachograph to the Remote Interrogator (RI), see Sub-appendix 11 Part B chapter 13 for details.	
2.63	(definitions) **tagLength** is part of the DER-TLV encoding and shall be set to ’81 10’ (see Appendix 11 Part B chapter 13). **currentDateTime** is the current date and time of the vehicle unit. **counter** enumerates the RTM messages. vuSerialNumber is the serial number of the vehicle unit. **dSRCMKVersionNumber** is the version number of the DSRC Master Key from which the VU specific DSRC keys were derived. **tagLengthMac** is the tag and length of the MAC data object as part of the DER-TLV encoding. The tag shall be set to ‘8E’, the length shall encode the length of the MAC in octets (see Appendix 11 Part B chapter 13). **mac** is the MAC calculated over the RTM message (see	**tagLength** is part of the DER-TLV encoding and shall be set to ’81 10’ (see Sub-appendix 11 Part B chapter 13). **currentDateTime** is the current date and time of the vehicle unit. **counter** enumerates the RTM messages. vuSerialNumber is the serial number of the vehicle unit. **dSRCMKVersionNumber** is the version number of the DSRC Master Key from which the VU specific DSRC keys were derived. **tagLengthMac** is the tag and length of the MAC data object as part of the DER-TLV encoding. The tag shall be set to ‘8E’, the length shall encode the length of the MAC in octets (see Sub-appendix 11 Part B chapter 13). **mac** is the MAC calculated over the RTM message (see	

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

2.80	Information related to the GNSS position of the vehicle (Annex 1C requirements 108, 109, 110, 296, 305, 347, and 353).	Information related to the GNSS position of the vehicle (Appendix 1C requirements 108, 109, 110, 296, 305, 347, and 353).	
2.85	Constant of the recording equipment (definition m)).	Constant of the control device (definition m)).	
2.86	(last paragraph) The third choice is suitable to reference the public key of a Member State.	The third choice is suitable to reference the public key of a Contracting Party.	
2.87	AES key and its associated key version used for VU – Motion Sensor pairing. For details see Appendix 11.	AES key and its associated key version used for VU – Motion Sensor pairing. For details see Sub-appendix 11.	
2.89	Date and time, stored on a driver card, of last card download (for other purposes than control) Annex 1C requirement 257 and 282. This date is updateable by a VU or any card reader.	Date and time, stored on a driver card, of last card download (for other purposes than control) Appendix 1C requirement 257 and 282. This date is updateable by a VU or any card reader.	
2.90	The link certificate between European Root CA key pairs.	The link certificate between ~~European~~ Root CA key pairs.	
2.92	A cryptographic checksum of 8, 12 or 16 bytes length corresponding to the cipher suites specified in Appendix 11.	A cryptographic checksum of 8, 12 or 16 bytes length corresponding to the cipher suites specified in Sub-appendix 11.	
2.93	Code identifying whether a cardholder has manually entered driver activities at card insertion or not (Annex 1B requirement 081 and Annex 1C requirement 102).	Code identifying whether a cardholder has manually entered driver activities at card insertion or not (Appendix 1B requirement 081 and Appendix 1C requirement 102).	
2.94	Code identifying a manufacturer of type approved equipment. ManufacturerCode ::= INTEGER(0..255) The laboratory competent for interoperability tests maintains and publishes the list of manufacturer codes on its web site (Annex 1C requirement 454). ManufacturerCodes are provisionally assigned to developers of tachograph equipment on application to	Code identifying a manufacturer of type approved equipment. ManufacturerCode ::= INTEGER(0..255) The laboratory competent for interoperability tests maintains and publishes the list of manufacturer codes on its web site (Appendix 1C requirement 454). ManufacturerCodes are provisionally assigned to developers of tachograph equipment on application to	

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

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

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

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

	and/or changes of driving status and/or changes of card status for a given calendar day (Annex 1B requirement 084 and Annex 1C requirement 105, 106, 107) and to slots status at 00:00 that day.	and/or changes of driving status and/or changes of card status for a given calendar day (Appendix 1B requirement 084 and Appendix 1C requirement 105, 106, 107) and to slots status at 00:00 that day.	
2.171	Information, stored in a VU, related to changes of activity and/or changes of driving status and/or changes of card status for a given calendar day (Annex 1C requirement 105, 106, 107) and to slots status at 00:00 that day.	Information, stored in a VU, related to changes of activity and/or changes of driving status and/or changes of card status for a given calendar day (Appendix 1C requirement 105, 106, 107) and to slots status at 00:00 that day.	
2.172	(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.	
2.173	Information, stored in a vehicle unit, related to the calibrations of the recording equipment (Annex 1B requirement 098).	Information, stored in a vehicle unit, related to the calibrations of the recording equipment (Appendix 1B requirement 098).	
2.174	Information, stored in a vehicle unit, related a calibration of the recording equipment (Annex 1B requirement 098 and Annex 1C requirement 119 and 120).	Information, stored in a vehicle unit, related a calibration of the recording equipment (Appendix 1B requirement 098 and Appendix 1C requirement 119 and 120).	
2.174	(vehicleRegistrationIdentification definition) **vehicleRegistrationIdentification** contains the VRN and registering Member State.	**vehicleRegistrationIdentification** contains the VRN and registering Contracting Party.	
2.175	Information, stored in a vehicle unit, related to the calibrations of the recording equipment (Annex 1C requirement 119 and 120).	Information, stored in a vehicle unit, related to the calibrations of the recording equipment (Appendix 1C requirement 119 and 120).	
2.176	Information, stored in a vehicle unit, related to insertion and withdrawal cycles of driver cards or of workshop cards in the vehicle unit (Annex 1B requirement	Information, stored in a vehicle unit, related to insertion and withdrawal cycles of driver cards or of workshop cards in the vehicle unit (Appendix 1B	

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

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

	event (Annex 1B requirement 094 and Annex 1C requirement 117 except over speeding event).	event (Appendix 1B requirement 094 and Appendix 1C requirement 117 except over speeding event).	
2.199	Information, stored in a vehicle unit, related to events (Annex 1C requirement 117 except over speeding event).	Information, stored in a vehicle unit, related to events (Appendix 1C requirement 117 except over speeding event).	
2.200	Information, stored in a vehicle unit, related to faults (Annex 1B requirement 096).	Information, stored in a vehicle unit, related to faults (Appendix 1B requirement 096).	
2.201	Information, stored in a vehicle unit, related to a fault (Annex 1B requirement 096 and Annex 1C requirement 118).	Information, stored in a vehicle unit, related to a fault (Appendix 1B requirement 096 and Appendix 1C requirement 118).	
2.202	Information, stored in a vehicle unit, related to faults (Annex 1C requirement 118).	Information, stored in a vehicle unit, related to faults (Appendix 1C requirement 118).	
2.203	Information, stored in a vehicle unit, related to the GNSS position of the vehicle if the accumulated driving time of the driver reaches a multiple of three hours (Annex 1C requirement 108, 110).	Information, stored in a vehicle unit, related to the GNSS position of the vehicle if the accumulated driving time of the driver reaches a multiple of three hours (Appendix 1C requirement 108, 110).	
2.204	Information, stored in a vehicle unit, related to the GNSS position of the vehicle if the accumulated driving time reaches a multiple of three hours (Annex 1C requirement 108 and 110).	Information, stored in a vehicle unit, related to the GNSS position of the vehicle if the accumulated driving time reaches a multiple of three hours (Appendix 1C requirement 108 and 110).	
2.205	Information, stored in a vehicle unit, related to the identification of the vehicle unit (Annex 1B requirement 075 and Annex 1C requirement 93 and 121).	Information, stored in a vehicle unit, related to the identification of the vehicle unit (Appendix 1B requirement 075 and Appendix 1C requirement 93 and 121).	
2.208	Information, stored in a vehicle unit, related to drivers' consent on the usage of Intelligent Transport Systems (Annex 1C requirement 200).	Information, stored in a vehicle unit, related to drivers' consent on the usage of Intelligent Transport Systems (Appendix 1C requirement 200).	
2.212	Information, stored in a vehicle unit, related to over speeding events since the last	Information, stored in a vehicle unit, related to over 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	

	requirement 087 and Annex 1C requirement 108 and 110).	1B requirement 087 and Appendix 1C requirement 108 and 110).	
2.219	(Generation 2, fullCardNumberAndGeneration definition) **fullCardNumberAndGeneration** is the type of card, its issuing Member State, its card number and generation as stored in the card.	**fullCardNumberAndGeneration** is the type of card, its issuing Contracting Party, 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).	Information, stored in a vehicle unit, related to places where drivers begin or end a daily work period (Appendix 1C requirement 108 and 110).	
2.223	Serial number of the vehicle unit (Annex 1B requirement 075 and Annex 1C requirement 93).	Serial number of the vehicle unit (Appendix 1B requirement 075 and Appendix 1C requirement 93).	
2.228	Information, stored in a vehicle unit, related to specific conditions (Annex 1C requirement 130).	Information, stored in a vehicle unit, related to specific conditions (Appendix 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).	Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (Appendix 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).	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).	
2.233	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 (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).	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 workshop card, related to	Information, stored in a workshop card, related to	

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

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

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

3.5	(2nd paragraph) Additional relevant details, related to cryptographic operations involved, are given in Appendix 11 Common security mechanisms for Tachograph Generation 1 and Generation 2.	(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.	
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)	

3.5.2.1.1, TCS_46	(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)	
3.5.2.3.1, TCS_54	(14th row in the table) LCC : Length of following cryptographic checksum ‘08h’, ‘0Ch’ or ‘10h’ depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B)	(14th row in the table) LCC : Length of following cryptographic checksum ‘08h’, ‘0Ch’ or ‘10h’ depending on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B)	
3.5.2.3.1, TCS_55	(9th row in the table) LCC : Length of following cryptographic checksum ‘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 ‘08h’, ‘0Ch’ or ‘10h’ depending on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B)	
3.5.3.1.1, TCS_58	(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)	
3.5.3.1.1, TCS_59	(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)	(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 Sub-appendix 11 Part B)	
3.5.3.3.1, TCS_67	(11th row in the table)	(11th row in the table)	

	LCC : Length of following cryptographic checksum ‘08h’, ‘0Ch’ or ‘10h’ depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B)	LCC : Length of following cryptographic checksum ‘08h’, ‘0Ch’ or ‘10h’ depending on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B)	
3.5.3.3.1, TCS_68	(6th row in the table) Lcc : Length of following cryptographic checksum ‘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 ‘08h’, ‘0Ch’ or ‘10h’ depending on AES key length for Generation 2 secure messaging (see Sub-appendix 11 Part B)	
3.5.5, TCS_72	TCS_72 The PIN entered by the user must be ASCII encoded and right padded with ‘FFh’ bytes up to a length of 8 bytes by the IFD, see also the data type WorkshopCardPIN in Appendix 1.	TCS_72 The PIN entered by the user must be ASCII encoded and right padded with ‘FFh’ bytes up to a length of 8 bytes by the IFD, see also the data type WorkshopCardPIN in Sub-appendix 1.	
3.5.7.1, TCS_84	(7th row in the table) Certificate : concatenation of data elements (as described in Appendix 11)	(7th row in the table) Certificate : concatenation of data elements (as described in Sub-appendix 11)	
3.5.7.1, TCS_85	(2nd indent after the table) • If the certificate verification fails, the processing state returned is ‘6688’. The verification and unwrapping process of the certificate is described in Appendix 11 for G1 and G2.	(2nd indent after the table) • If the certificate verification fails, the processing state returned is ‘6688’. The verification and unwrapping process of the certificate is described in Sub-appendix 11 for G1 and G2.	
3.5.7.2	(2nd paragraph) The certificate structure and the domain parameters are defined in Appendix 11.	(2nd paragraph) The certificate structure and the domain parameters are defined in Sub-appendix 11.	
3.5.7.2, TCS_89	Note: According to Appendix 11 the card stores the certificate or the relevant contents of the certificate and updates its currentAuthenticatedTime.	Note: According to Sub-appendix 11 the card stores the certificate or the relevant contents of the certificate and updates its currentAuthenticatedTime.	
3.5.7.2, TCS_90	(2nd indent) • If the selected public key (used to unwrap the certificate) has a CHA.LSB (CertificateHolderAuthorisation.equipmentType) that is not suitable for the certificate verification according to Appendix 11, the processing state returned is **‘6985’**.	(2nd indent) • If the selected public key (used to unwrap the certificate) has a CHA.LSB (CertificateHolderAuthorisation.equipmentType) that is not suitable for the certificate verification according to Sub-appendix 11, the processing state returned is **‘6985’**.	

3.5.7.2, TCS_91	(2nd paragraph) Using the INTERNAL AUTHENTICATE command, the IFD can authenticate the card. The authentication process is described in Appendix 11. It includes the following statements:	(2nd paragraph) Using the INTERNAL AUTHENTICATE command, the IFD can authenticate the card. The authentication process is described in Sub-appendix 11. It includes the following statements:	
3.5.7.2, TCS_92	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).	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 Sub-appendix 11).	
3.5.7.2, TCS_93	(7th row in the table) VU.CHR (see Appendix 11)	(7th row in the table) VU.CHR (see Sub-appendix 11)	
3.5.7.2, TCS_94	(2nd row in the table) Card authentication token (see Appendix 11)	(2nd row in the table) Card authentication token (see Sub-appendix 11)	
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.	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).	(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).	
3.5.9, TCS_97	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	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 EXTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys.	plain EXTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys.	
3.5.9, TCS_98	(7th row in the table) Generation 1 authentication: Cryptogram (see Appendix 11 Part A) Generation 2 authentication: Signature generated by the IFD (see Appendix 11 Part B)	(7th row in the table) Generation 1 authentication: Cryptogram (see Sub-appendix 11 Part A) Generation 2 authentication: Signature generated by the IFD (see Sub-appendix 11 Part B)	
3.5.10	This command is used for the generation 2 chip authentication protocol specified in Appendix 11 Part B and is compliant with ISO/IEC 7816-4.	This command is used for the generation 2 chip authentication protocol specified in Sub-appendix 11 Part B and is compliant with ISO/IEC 7816-4.	
3.5.10, TCS_101	(7th row in the table) DER-TLV encoded ephemeral public key value (see Appendix 11) The VU shall send the data objects in this order.	(7th row in the table) DER-TLV encoded ephemeral public key value (see Sub-appendix 11) The VU shall send the data objects in this order.	
3.5.10, TCS_102	(2nd row in the table) DER-TLV encoded Dynamic Authentication Data: nonce and authentication token (see Appendix 11)	(2nd row in the table) DER-TLV encoded Dynamic Authentication Data: nonce and authentication token (see Sub-appendix 11)	
3.5.11.1, TCS_106	(9th row in the table) Key identifier as specified in Appendix 11	(9th row in the table) Key identifier as specified in Sub-appendix 11	
3.5.11.2.1, TCS_109	(7th row in the table) DER-TLV encoded cryptographic mechanism reference: Object Identifier of Chip Authentication (value only, Tag ‘06h’ is omitted). See Appendix 1 for the values of object identifiers; the byte notation shall be used. See Appendix 11 for guidance on how to select one of these object identifiers.	(7th row in the table) DER-TLV encoded cryptographic mechanism reference: Object Identifier of Chip Authentication (value only, Tag ‘06h’ is omitted). See Sub-appendix 1 for the values of object identifiers; the byte notation shall be used. See Sub-appendix 11 for guidance on how to select one of these object identifiers.	
3.5.11.2.2, TCS_111	(6th row in the table) DER-TLV encoded cryptographic mechanism reference: Object Identifier of VU Authentication (value only, Tag ‘06h’ is omitted).	(6th row in the table) DER-TLV encoded cryptographic mechanism reference: Object Identifier of VU Authentication (value only, Tag ‘06h’ is omitted).	

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

	the relevant EQT_Sign public key. In some cases, the control card may have stored the corresponding EQT_MA public key. The control card shall always set the EQT_Sign public key for use when it receives an MSE: SET DST command.	control card will always have stored the relevant EQT_Sign public key. In some cases, the control card may have stored the corresponding EQT_MA public key. The control card shall always set the EQT_Sign public key for use when it receives an MSE: SET DST command.	
3.5.12, TCS_116	(8th row in the table) Length L of the hash code: ‘14h’ in Generation 1 application (see Appendix 11 Part A) ‘20h’, ‘30h’ or ‘40h’ in Generation 2 application (see Appendix 11 Part B)	(8th row in the table) Length L of the hash code: ‘14h’ in Generation 1 application (see Sub-appendix 11 Part A) ‘20h’, ‘30h’ or ‘40h’ in Generation 2 application (see Sub-appendix 11 Part B)	
3.5.13, TCS_123	TCS_123 The Tachograph Generation 2 application shall support the SHA-2 algorithm (SHA-256, SHA-384 or SHA-512, specified by the cipher suite in Appendix 11 Part B for the card signature key Card_Sign.	TCS_123 The Tachograph Generation 2 application shall support the SHA-2 algorithm (SHA-256, SHA-384 or SHA-512, specified by the cipher suite in Sub-appendix 11 Part B for the card signature key Card_Sign.	
3.5.13, TCS_124	(5th row in the table, 3rd paragraph) For the Tachograph Generation 2 application: SHA-2 algorithm (SHA-256, SHA-384 or SHA-512) defined by the cipher suite in Appendix 11 Part B for the card signature key Card_Sign	(5th row in the table, 3rd paragraph) For the Tachograph Generation 2 application: SHA-2 algorithm (SHA-256, SHA-384 or SHA-512) defined by the cipher suite in Sub-appendix 11 Part B for the card signature key Card_Sign	
3.5.14, TCS_128	TCS_128 The Generation 1 tachograph application performs a digital signature using a padding method compliant with PKCS1 (see Appendix 11 for details).	TCS_128 The Generation 1 tachograph application performs a digital signature using a padding method compliant with PKCS1 (see Sub-appendix 11 for details).	
3.5.14, TCS_129	TCS_129 The Generation 2 tachograph application computes an elliptic curve based digital signature (see Appendix 11 for details).	TCS_129 The Generation 2 tachograph application computes an elliptic curve based digital signature (see Sub-appendix 11 for details).	
3.5.15, TCS_133	(8th row in the table, 2nd and 3rd paragraph) 128 bytes coded in accordance with Appendix 11 Part A for Tachograph Generation 1 application.	(8th row in the table, 2nd and 3rd paragraph) 128 bytes coded in accordance with Sub-appendix 11 Part A for Tachograph Generation 1 application.	

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

	Confidentiality nesting the concatenation of the following data elements (see Appendix 1 dSRCSecurityData and Appendix 11 Part B chapter 13):	Confidentiality nesting the concatenation of the following data elements (see Sub-appendix 1 dSRCSecurityData and Sub-appendix 11 Part B chapter 13):	
3.5.16, TCS_138	(9th row in the table, 1st paragraph) DER-TLV encoded MAC over the DSRC message. For the MAC algorithm and calculation see Appendix 11, Part B chapter 13.	(9th row in the table, 1st paragraph) DER-TLV encoded MAC over the DSRC message. For the MAC algorithm and calculation see Sub-appendix 11, Part B 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 OF CONTENTS	*(Title)* *APPENDIX 3. PICTOGRAMS*	*SUB-APPENDIX 3. PICTOGRAMS*	
1	*Note: Additional pictogram combinations to form printout blocks or record identifiers are defined in Appendix 4.*	*Note: Additional pictogram combinations to form printout blocks or record identifiers are 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	

	VIN Registering Member State and VRN	VIN Registering Contracting Party and VRN	
2, PRT_007	Block 8.2 Card insertion in slot S Record identifier; S = Slot pictogram Vehicle registering Member State and VRN Vehicle odometer at card insertion	Block 8.2 Card insertion in slot S Record identifier; S = Slot pictogram Vehicle registering Contracting Party and VRN Vehicle odometer at card insertion	
2, PRT_007	Block 12.4 Event and/or Fault record Record identifier Event/fault pictogram, record purpose, date time of start, Additional event/fault code (if any), duration Registering Member State & VRN of vehicle in which the event or fault occurred	Block 12.4 Event and/or Fault record Record identifier Event/fault pictogram, record purpose, date time of start, Additional event/fault code (if any), duration Registering Contracting Party & VRN of vehicle in which the event or fault occurred	
2, PRT_007	Block 17.1 Calibration record Record identifier Workshop having performed the calibration Workshop address Workshop card identification Workshop card expiry date Blank line Calibration date + calibration purpose VIN Registering Member State & VRN Characteristic coefficient of vehicle Constant of the recording equipment Effective circumference of wheel tyres Size of tyres mounted Speed limiting device setting Old and new odometer values	Block 17.1 Calibration record Record identifier Workshop having performed the calibration Workshop address Workshop card identification Workshop card expiry date Blank line Calibration date + calibration purpose VIN Registering Contracting Party & VRN Characteristic coefficient of vehicle Constant of the control device Effective circumference of wheel tyres Size of tyres mounted Speed limiting device setting 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 OF CONTENTS	*(Title)* *APPENDIX* 5. DISPLAY	*SUB-APPENDIX* 5. DISPLAY	

	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 OF CONTENTS	*(Title)* *APPENDIX* 6. FRONT CONNECTOR FOR CALIBRATION AND DOWNLOAD	*SUB-APPENDIX* 6. FRONT CONNECTOR FOR CALIBRATION AND DOWNLOAD	

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

Point or article	Text Appendix 7	Proposed text for AETR	Comments
TITLE/TABLE OF CONTENTS	*(Title)* *APPENDIX 7. DATA DOWNLOADING PROTOCOLS*	*SUB-APPENDIX 7. DATA DOWNLOADING PROTOCOLS*	
1	This appendix specifies the procedures to follow in order to perform the different types of data download to an External Storage Medium, together with the protocols that must be implemented to assure the correct data transfer and the full compatibility of the downloaded data format to allow any controller to inspect these data and be able to control their authenticity and their integrity before analysing them.	This Sub-appendix specifies the procedures to follow in order to perform the different types of data download to an External Storage Medium, together with the protocols that must be implemented to assure the correct data transfer and the full compatibility of the downloaded data format to allow any controller to inspect these data and be able to control their authenticity and their integrity before analysing them.	
1.1	Data may be downloaded to an ESM: - from a Vehicle Unit by an Intelligent Dedicated Equipment (IDE) connected to the VU, - from a tachograph card by an IDE fitted with a card interface device (IFD), - from a tachograph card via a vehicle unit by an IDE connected to the VU. To give the possibility to verify the authenticity and integrity of downloaded data stored on an ESM, data is downloaded with a signature appended in accordance with Appendix 11 Common Security Mechanisms. The source equipment (VU or card) identification and its security certificates (Member state and equipment) are also downloaded. The verifier of the data must possess	Data may be downloaded to an ESM: - from a Vehicle Unit by an Intelligent Dedicated Equipment (IDE) connected to the VU, - from a tachograph card by an IDE fitted with a card interface device (IFD), - from a tachograph card via a vehicle unit by an IDE connected to the VU. To give the possibility to verify the authenticity and integrity of downloaded data stored on an ESM, data is downloaded with a signature appended in accordance with Sub-appendix 11 Common Security Mechanisms. The source equipment (VU or card) identification and its security certificates (Contracting Party and equipment) are also downloaded. The verifier of 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 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 A. Similarly, there are two types of data downloads from second generation driver cards inserted in a VU, as specified in paragraphs 3 and 4 of this Appendix.	independently a trusted root public key. Data downloaded from a VU are 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 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 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 Part A. Similarly, there are two types of data downloads from second generation driver cards inserted in a VU, as specified in paragraphs 3 and 4 of this Sub-appendix.	
1.2	The following acronyms are used in this appendix:	The following acronyms are used in this Sub-appendix:	
2.2.6	This paragraph specifies the content of the data fields of the various positive response messages. Data elements are defined in Appendix 1 data dictionary.	This paragraph specifies the content of the data fields of the various positive response messages. Data elements are defined in 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, 4th 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, 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 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	(3rd 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.	(3rd 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 OF CONTENTS	*(Title)* *APPENDIX 8. CALIBRATION PROTOCOL*	*SUB-APPENDIX 8.* *CALIBRATION PROTOCOL*	
1	This appendix describes how data is exchanged between a vehicle unit and a tester via the K-line which forms part of the calibration interface described in Appendix 6. It also describes control of the input / output signal line on the calibration connector. Establishing K-line communications is described in Section 4 "Communication Services". This appendix uses the idea of diagnostic "sessions" to determine the scope of K-line control under different conditions. The default session is the "StandardDiagnosticSession" where all data can be read from a vehicle unit but no data can be written to a vehicle unit. Selection of the diagnostic session is described in Section 5 "Management Services". This appendix has to be considered as relevant for both generations of VUs and of workshop cards, in compliance with the interoperability requirements laid down in this Regulation.	This Sub-appendix describes how data is exchanged between a vehicle unit and a tester via the K-line which forms part of the calibration interface described in Sub-appendix 6. It also describes control of the input / output signal line on the calibration connector. Establishing K-line communications is described in Section 4 "Communication Services". This Sub-appendix uses the idea of diagnostic "sessions" to determine the scope of K-line control under different conditions. The default session is the "StandardDiagnosticSession" where all data can be read from a vehicle unit but no data can be written to a vehicle unit. Selection of the diagnostic session is described in Section 5 "Management Services". This Sub-appendix has to be considered as relevant for both generations of VUs and of workshop cards, in compliance with the interoperability requirements laid down in this Agreement.	
3.1, CPR_004	(CPR_004 2nd indent) - The **2nd column** includes the section number in this appendix where of service is further defined.	- The **2nd column** includes the section number in this Sub-appendix where of service is further defined.	
6.1.3, CPR_053	(CPR_053 2nd indent)		

	- 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, 2nd column) Code Page (as defined in Appendix 1) Vehicle Registration Number (as defined in Appendix 1)	Code Page (as defined in Sub-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 certification** performed by the competent body 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 certification** performed by 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	

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

	Tachograph cards shall be printed with the following background predominant colours: - driver card: white, - workshop card: red, - control card: blue, - company card: yellow.	Tachograph cards shall be printed with the following background predominant colours: - driver card: white, - workshop card: red, - control card: blue, - company card: yellow.	
4, 2.1	[Security] 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: - a security design background with fine guilloche patterns and rainbow printing, - at least one two-coloured microprint line.	[Security] 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: - a security design background with fine guilloche patterns and rainbow printing, - at least one two-coloured microprint line.	
4, 2.1	[Markings] Annex 1C, chapter 4.1 'Visible data', 236) Member States may add colours or markings, such as national symbols and security features.	[Markings] Appendix 1C, chapter 4.1 'Visible data', 236) Contracting Parties may add colours or markings, such as national symbols and security features.	
4, 2.2	[Durability] 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.	[Durability] Appendix 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.	
4, 4.1	[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 and not over 100 times during the life time of the card.	[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 100 times during the life time of the card.	

	The Tachograph cards are exposed in consecutive steps to the following temperatures and humidities for the given time. After each step the Tachograph cards are tested for electrical functionality. 1. Temperature of – 20 °C for 2 h. 2. Temperature of +/- 0 °C for 2 h. 3. Temperature of + 20 °C, 50 % RH, for 2 h. 4. Temperature of + 50 °C, 50 % RH, for 2 h. 5. Temperature of + 70 °C, 50 % RH, for 2 h. The temperature is increased intermittently to + 85 °C, 50 % RH, for 60 min. 6. Temperature of + 70 °C, 85 % RH, for 2 h. The temperature is increased intermittently to + 85 °C, 85 % RH, for 30 min.	The Tachograph cards are exposed in consecutive steps to the following temperatures and humidities for the given time. After each step the Tachograph cards are tested for electrical functionality. 1. Temperature of – 20 °C for 2 h. 2. Temperature of +/- 0 °C for 2 h. 3. Temperature of + 20 °C, 50 % RH, for 2 h. 4. Temperature of + 50 °C, 50 % RH, for 2 h. 5. Temperature of + 70 °C, 50 % RH, for 2 h. The temperature is increased intermittently to + 85 °C, 50 % RH, for 60 min. 6. Temperature of + 70 °C, 85 % RH, for 2 h. The temperature is increased intermittently to + 85 °C, 85 % RH, for 30 min.	
4, 4.1	[Humidity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 242) Tachograph cards shall be capable of operating correctly in the humidity range 10% to 90%.	[Humidity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 242) Tachograph cards shall be capable of operating correctly in the humidity range 10% to 90%.	
4, 4.1	[Electromagnetic compatibility - EMC] Annex 1C, chapter 4.4 'Environmental and electrical specifications' 244) During operation, Tachograph cards shall conform to ECE R10 related to electromagnetic compatibility.	[Electromagnetic compatibility - EMC] Appendix 1C, chapter 4.4 'Environmental and electrical specifications' 244) During operation, Tachograph cards shall conform to ECE R10 related to electromagnetic compatibility.	
4, 4.1	[Static electricity] Annex 1C, chapter 4.4 'Environmental and electrical specifications', 244) During operation, Tachograph cards shall be protected against electrostatic discharges. Tachograph cards must conform to standard	[Static electricity] Appendix 1C, chapter 4.4 'Environmental and electrical specifications', 244) During operation, Tachograph cards shall be protected against electrostatic discharges. Tachograph cards must 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 Sub-appendix 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 Sub-appendix 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 OF CONTENTS	*(Title)* *APPENDIX 10. SECURITY REQUIREMENTS*	*SUB-APPENDIX 10. SECURITY REQUIREMENTS*	
1st paragraph	This appendix specifies the IT security requirements for the smart tachograph system components (second-generation tachograph).	This Sub-appendix specifies the IT security requirements for the smart tachograph system components (second-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 OF CONTENTS	*(Title)* *APPENDIX 11. COMMON SECURITY MECHANISMS*	*SUB-APPENDIX 11. COMMON SECURITY MECHANISMS*	
Table of contents	…	*(to be updated after having applied all the changes)*	
Preamble	This Appendix specifies the security mechanisms ensuring - mutual authentication between different components of the tachograph system. - confidentiality, integrity, authenticity and/or non-repudiation of data transferred between different components of the tachograph system or downloaded to external storage media. This Appendix consists of two parts. Part A defines the security mechanisms for the first-generation tachograph system (digital tachograph). Part B defines the security mechanisms for the second-generation tachograph system (smart tachograph). The mechanisms specified in Part A of this Appendix shall apply if at least one of the components of the tachograph system involved in a mutual authentication and/or data transfer process is of the first generation. The mechanisms specified in Part B of this Appendix shall apply if both components of the tachograph system involved in the mutual authentication and/or data	This Sub-appendix specifies the security mechanisms ensuring - mutual authentication between different components of the tachograph system. - confidentiality, integrity, authenticity and/or non-repudiation of data transferred between different components of the tachograph system or downloaded to external storage media. This Sub-appendix consists of two parts. Part A defines the security mechanisms for the first-generation tachograph system (digital tachograph). Part B defines the security mechanisms for the second-generation tachograph system (smart tachograph). The mechanisms specified in Part A of this Sub-appendix shall apply if at least one of the components of the tachograph system involved in a mutual authentication and/or data transfer process is of the first generation. The mechanisms specified in Part B of this Sub-appendix shall apply if both components of the tachograph system involved in the mutual	

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

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

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

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

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

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

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

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

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

	shall use an ephemeral key pair exclusively to perform session key agreement with a tachograph card or external GNSS facility, as specified in sections 10.4 and 11.4 of this Appendix.	shall use an ephemeral key pair exclusively to perform session key agreement with a tachograph card or external GNSS facility, as specified in sections 10.4 and 11.4 of this Sub-appendix.	
9.1.4, CSM_77	CSM_77 A vehicle unit shall use the private key VU_Sign.SK of its VU_Sign key pair exclusively to sign downloaded data files, as specified in chapter 14 of this Appendix. The corresponding public key VU_Sign.PK shall be used exclusively to verify signatures created by the vehicle unit.	CSM_77 A vehicle unit shall use the private key VU_Sign.SK of its VU_Sign key pair exclusively to sign downloaded data files, as specified in chapter 14 of this Sub-appendix. The corresponding public key VU_Sign.PK shall be used exclusively to verify signatures created by the vehicle unit.	
9.1.4, CSM_78	Notes: - The extended validity period of a VU_Sign certificate allows a Vehicle Unit to create valid signatures over downloaded data during the first three months after it has expired, as required in Regulation (EU) N°. 581/2010.	Notes: - The extended validity period of a VU_Sign certificate allows a Vehicle Unit to create valid signatures over downloaded data during the first three months after it has expired. ~~as required in Regulation (EU) N°. 581/2010.~~	
9.1.4, CSM_82	CSM_82 In addition to the cryptographic keys and certificates listed in CSM_81, vehicle units shall also contain the keys and certificates specified in Part A of this Appendix, allowing a vehicle unit to interact with first-generation tachograph cards.	CSM_82 In addition to the cryptographic keys and certificates listed in CSM_81, vehicle units shall also contain the keys and certificates specified in Part A of this Sub-appendix, allowing a vehicle unit to interact with first-generation tachograph cards.	
9.1.5, CSM_86	CSM_86 A tachograph card shall use its Card_MA key pair, consisting of private key Card_MA.SK and public key Card_MA.PK, exclusively to perform mutual authentication and session key agreement towards vehicle units, as specified in sections 10.3 and 10.4 of this Appendix.	CSM_86 A tachograph card shall use its Card_MA key pair, consisting of private key Card_MA.SK and public key Card_MA.PK, exclusively to perform mutual authentication and session key agreement towards vehicle units, as specified in sections 10.3 and 10.4 of this Sub-appendix.	
9.1.5, CSM_87	CSM_87 A driver card or workshop card shall use the private key Card_Sign.SK of its Card_Sign key pair exclusively to sign downloaded data files,	CSM_87 A driver card or workshop card shall use the private key Card_Sign.SK of its Card_Sign key pair exclusively to sign downloaded data files,	

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

	exclusively to perform mutual authentication and session key agreement towards vehicle units, as specified in section 11.4 of this Appendix.	exclusively to perform mutual authentication and session key agreement towards vehicle units, as specified in section 11.4 of this Sub-appendix.	
9.2.1.1	Note: readers of this section are supposed to be familiar with the contents of [ISO 16844-3] describing the interface between a vehicle unit and a motion sensor. The pairing process between a VU and a motion sensor is described in detail in chapter 12 of this Appendix.	Note: readers of this section are supposed to be familiar with the contents of [ISO 16844-3] describing the interface between a vehicle unit and a motion sensor. The pairing process between a VU and a motion sensor is described in detail in chapter 12 of this Sub-appendix.	
9.2.1.1, CSM_100	CSM_100 A number of symmetric keys is needed for pairing vehicle units and motion sensors, for mutual authentication between vehicle units and motion sensors and for encrypting communication between vehicle units and motion sensors, as shown in Table 3. All of these keys shall be AES keys, with a key length equal to the length of the motion sensor master key, which shall be linked to the length of the (foreseen) European root key pair as described in CSM_50.	CSM_100 A number of symmetric keys is needed for pairing vehicle units and motion sensors, for mutual authentication between vehicle units and motion sensors and for encrypting communication between vehicle units and motion sensors, as shown in Table 3. All of these keys shall be AES keys, with a key length equal to the length of the motion sensor master key, which shall be linked to the length of the (foreseen) root key pair as described in CSM_50.	
9.2.1.1, CSM_101	CSM_101 The European Root Certificate Authority shall generate KM-VU and KM-WC, two random and unique AES keys from which the motion sensor master key KM can be calculated as KM-VU XOR KM-WC. The ERCA shall communicate KM, KM-VU and KM-WC to Member State Certificate Authorities upon their request.	CSM_101 The European Root Certificate Authority shall generate KM-VU and KM-WC, two random and unique AES keys from which the motion sensor master key KM can be calculated as KM-VU XOR KM-WC. The ERCA shall communicate KM, KM-VU and KM-WC to Contracting Party Certificate Authorities upon their request.	
9.2.1.1, CSM_103	CSM_103 A Member State Certificate Authority shall forward KM-VU, together with its version number, to vehicle unit manufacturers upon their request. The VU manufacturers shall insert	CSM_103 A Contracting Party Certificate Authority shall forward KM-VU, together with its version number, to vehicle unit manufacturers upon their request. The VU 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 key to the motion sensor manufacturer. For each encrypted key, the MSCA shall notify the motion sensor manufacturer of the version number of the associated KM.	and shall return the encrypted key to the motion sensor manufacturer. For each encrypted key, the MSCA shall notify the motion sensor manufacturer of the version number of the associated KM.	
9.2.1.1, CSM_108	CSM_108 Each motion sensor manufacturer shall generate a unique serial number for every motion sensor, and shall send all serial numbers to its Member State Certificate Authority. The MSCA shall encrypt each serial number separately with the identification key KID and shall return the encrypted serial number to the motion sensor manufacturer. For each encrypted serial number, the MSCA shall notify the motion sensor manufacturer of the version number of the associated KID.	CSM_108 Each motion sensor manufacturer shall generate a unique serial number for every motion sensor, and shall send all serial numbers to its Contracting Party Certificate Authority. The MSCA shall encrypt each serial number separately with the identification key KID and shall return the encrypted serial number to the motion sensor manufacturer. For each encrypted serial number, the MSCA shall notify the motion sensor manufacturer of the version number of the associated KID.	
9.2.1.1, CSM_111	CSM_111 In addition to the AES-based cryptographic material specified in CSM_110, a motion sensor manufacturer may also store in each motion sensor the TDES-based cryptographic material specified in requirement CSM_037 in Part A of this Appendix.	CSM_111 In addition to the AES-based cryptographic material specified in CSM_110, a motion sensor manufacturer may also store in each motion sensor the TDES-based cryptographic material specified in requirement CSM_037 in Part A of this Sub-appendix.	
9.2.1.2, CSM_114	CSM_114 At least one year before generating a new European root key pair, as described in CSM_56, the ERCA shall generate a new motion sensor master key KM by generating a new KM-VU and KM-WC. The length of the motion sensor master key shall be linked to the foreseen strength of the new European root key pair, according to CSM_50. The ERCA shall communicate the new KM, KM-VU and KM-WC to the MSCAs upon their request,	CSM_114 At least one year before generating a new root key pair, as described in CSM_56, the ERCA shall generate a new motion sensor master key KM by generating a new KM-VU and KM-WC. The length of the motion sensor master key shall be linked to the foreseen strength of the new European root key pair, according to CSM_50. The ERCA shall communicate the new KM, KM-VU and KM-WC to the MSCAs upon their request,	

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

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

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

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

	- 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 Sub-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	
10.2.1, CSM_157	Notes to **Error! Reference source not found.**: - The Card certificates and public keys mentioned in the figure are those for mutual authentication. Section **Error! Reference source not found.** denotes these as Card_MA. - The Card.CA certificates and public keys mentioned in the figure are those for signing card certificates and it is indicated in the CAR of the Card certificate. Section **Error! Reference source not found.** denotes these as MSCA_Card. - The Card.CA.EUR certificate mentioned in the figure is the European root certificate that is indicated in the CAR of the Card.CA certificate.	Notes to **Error! Reference source not found.**: - The Card certificates and public keys mentioned in the figure are those for mutual authentication. Section **Error! Reference source not found.** denotes these as Card_MA. - The Card.CA certificates and public keys mentioned in the figure are those for signing card certificates and it is indicated in the CAR of the Card certificate. Section **Error! Reference source not found.** denotes these as MSCA_Card. - The Card.CA.EUR certificate mentioned in the figure is the root certificate that is indicated in the CAR	

	- 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 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).	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 Sub-appendix 1, data type EquipmentType).	

10.2.2, CSM_161	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.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.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.EUR certificate is the European root certificate that is indicated in the CAR of the VU.Link certificate.	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.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 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 root key pair created by the ERCA and signed by the previous root private key. - The VU.Link.EUR 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 combination with the hashing algorithm linked to the key	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 ECDSA algorithm, in combination with the hashing	

	size of the VU's VU_MA key pair, as specified in CSM_50'.	algorithm linked to the key size of the VU's VU_MA key pair, as specified in CSM_50'.	
10.5.1, CSM_182	CSM_182 Except when reading from a file with access condition SM-R-ENC-MAC-G2 (see Appendix 2, section 4), Secure Messaging shall be used in authentication-only mode. In this mode, a cryptographic checksum (a.k.a. MAC) is added to all commands and responses to ensure message authenticity and integrity.	CSM_182 Except when reading from a file with access condition SM-R-ENC-MAC-G2 (see Sub-appendix 2, section 4), Secure Messaging shall be used in authentication-only mode. In this mode, a cryptographic checksum (a.k.a. MAC) is added to all commands and responses to ensure message authenticity and integrity.	
10.5.2, CSM_188	Note: As specified in Appendix 2, tachograph cards may support the READ BINARY and UPDATE BINARY command with an odd INS byte ('B1' resp. 'D7'). These command variants are required to read and update files with more than 32768 bytes or more. In case such a variant is used, a data object with tag 'B3' shall be used instead of an object with tag '81'. See Appendix 2 for more information.	Note: As specified in Appendix 2, tachograph cards may support the READ BINARY and UPDATE BINARY command with an odd INS byte ('B1' resp. 'D7'). These command variants are required to read and update files with more than 32768 bytes or more. In case such a variant is used, a data object with tag 'B3' shall be used instead of an object with tag '81'. See Sub-appendix 2 for more information.	
10.5.2, CSM_190	CSM_190 APDUs protected by Secure Messaging shall be created as follows: - The command header shall be included in the MAC calculation, therefore value '0C'shall be used for the class byte CLA. - As specified in Appendix 2, all INS bytes shall be even, with the possible exception of odd INS bytes for the READ BINARY and UPDATE BINARY commands. - The actual value of Lc will be modified to Lc' after	CSM_190 APDUs protected by Secure Messaging shall be created as follows: - The command header shall be included in the MAC calculation, therefore value '0C'shall be used for the class byte CLA. - As specified in Sub-appendix 2, all INS bytes shall be even, with the possible exception of odd INS bytes for the READ BINARY and UPDATE BINARY commands. - The actual value of Lc will be modified to Lc' after	

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

	- The Card.Link certificate mentioned in the figure shall be interpreted as the EGF'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 Card.Link.EUR certificate is the European root certificate that is indicated in the CAR of the Card.Link certificate. - Instead of the cardExtendedSerialNumber, the VU shall read the sensorGNSSserialNumber from EF ICC. - Instead of selecting the Tachograph AID, the VU shall select the EGF AID. - 'Ignore Card' shall be interpreted as 'Ignore EGF'.	- The Card.Link certificate mentioned in the figure shall be interpreted as the EGF'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 European private key. - The Card.Link.EUR certificate is the root certificate that is indicated in the CAR of the Card.Link certificate. - Instead of the cardExtendedSerialNumber, the VU shall read the sensorGNSSserialNumber from EF ICC. - Instead of selecting the Tachograph AID, the VU shall select the EGF AID. - 'Ignore Card' shall be interpreted as 'Ignore EGF'.	
11.3.2, CSM_208	Notes to Figure 5 within this context: - The VU shall generate a fresh ephemeral key pair using the domain parameters in the EGF certificate. - 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.EUR certificate mentioned in the figure is the European 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,	Notes to Figure 5 within this context: - The VU shall generate a fresh ephemeral key pair using the domain parameters in the EGF certificate. - 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.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.EUR certificate is the European root certificate that is indicated in the CAR of the VU.Link certificate.	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 certificate is the root certificate that is indicated in the CAR of the VU.Link certificate.	
11.3.3, CSM_211	Note that Figure 11 in essence consists of the first steps shown in Figure 4 and Figure 5. Again, note that since an EGF is not a smart card, the VU will probably not send a Reset to initiate the communication and will not receive an ATR. In any case this is out of the scope of this Appendix.	Note that Figure 11 in essence consists of the first steps shown in Figure 4 and Figure 5. Again, note that since an EGF is not a smart card, the VU will probably not send a Reset to initiate the communication and will not receive an ATR. In any case this is out of the scope of this Sub-appendix.	
12.3, CSM_220	Note: in [ISO 16844-3], the number of plaintext data bytes is always a multiple of 8, such that padding is not necessary when using TDES. The definition of data and messages in [ISO 16844-3] is not changed by this part of this Appendix, thus necessitating the application of padding.	Note: in [ISO 16844-3], the number of plaintext data bytes is always a multiple of 8, such that padding is not necessary when using TDES. The definition of data and messages in [ISO 16844-3] is not changed by this part of this Sub-appendix, thus necessitating the application of padding.	
12.4, CSM_222	CSM_222 As explained in section 9.2.1, a second-generation motion sensor may contain the TDES-based encryption of the pairing data (as defined in Part A of this Appendix), which allows the motion sensor to be paired to a first-generation VU. If this is the case, a first-generation VU and a second-generation motion sensor shall be paired as described in Part A of this Appendix and in [ISO 16844-3]. For the pairing process either a first-generation or a second-generation workshop card may be used.	CSM_222 As explained in section 9.2.1, a second-generation motion sensor may contain the TDES-based encryption of the pairing data (as defined in Part A of this Sub-appendix), which allows the motion sensor to be paired to a first-generation VU. If this is the case, a first-generation VU and a second-generation motion sensor shall be paired as described in Part A of this Sub-appendix and in [ISO 16844-3]. For the pairing process either a first-generation or a second-generation workshop card may be used.	
13.1	As specified in Appendix 14, a VU regularly generates	As specified in Appendix 14, a VU regularly generates	

	Remote Tachograph Monitoring (RTM) data and sends this data to the (internal or external) Remote Communication Facility (RCF). The remote communication facility is responsible for sending this data over the DSRC interface described in Appendix 14 to the remote interrogator. Appendix 1 specifies that the RTM data is the concatenation of: • Encrypted tachograph payload the encryption of the plaintext tachograph payload • DSRC security data described below The plaintext tachograph payload data format is specified in Appendix 1 and further described in Appendix 14. This section describes the structure of the DSRC security data; the formal specification is in Appendix 1	Remote Tachograph Monitoring (RTM) data and sends this data to the (internal or external) Remote Communication Facility (RCF). The remote communication facility is responsible for sending this data over the DSRC interface described in Sub-appendix 14 to the remote interrogator. Sub-appendix 1 specifies that the RTM data is the concatenation of: • Encrypted tachograph payload the encryption of the plaintext tachograph payload • DSRC security data described below The plaintext tachograph payload data format is specified in Sub-appendix 1 and further described in Sub-appendix 14. This section describes the structure of the DSRC security data; the formal specification is in Sub-appendix 1	
13.2, CSM_226	CSM_226 Given a plaintext data element with data type TachographPayload as described in Appendix 14, a VU shall encrypt this data as shown in Figure 12: the VU's DSRC key for encryption K_VUDSRC_ENC (see section 9.2.2) shall be used with AES in the Cipher Block Chaining (CBC) mode of operation, as defined in [ISO 10116], with an interleave parameter m = 1. The initialization vector shall be equal to IV = current date time || '00 00 00 00 00 00 00 00' || counter, where current date time and counter are specified in CSM_224. The data to be encrypted shall be padded	CSM_226 Given a plaintext data element with data type TachographPayload as described in Sub-appendix 14, a VU shall encrypt this data as shown in Figure 12: the VU's DSRC key for encryption K_VUDSRC_ENC (see section 9.2.2) shall be used with AES in the Cipher Block Chaining (CBC) mode of operation, as defined in [ISO 10116], with an interleave parameter m = 1. The initialization vector shall be equal to IV = current date time || '00 00 00 00 00 00 00 00' || counter, where current date time and counter are specified in CSM_224. The data to be encrypted shall be padded	

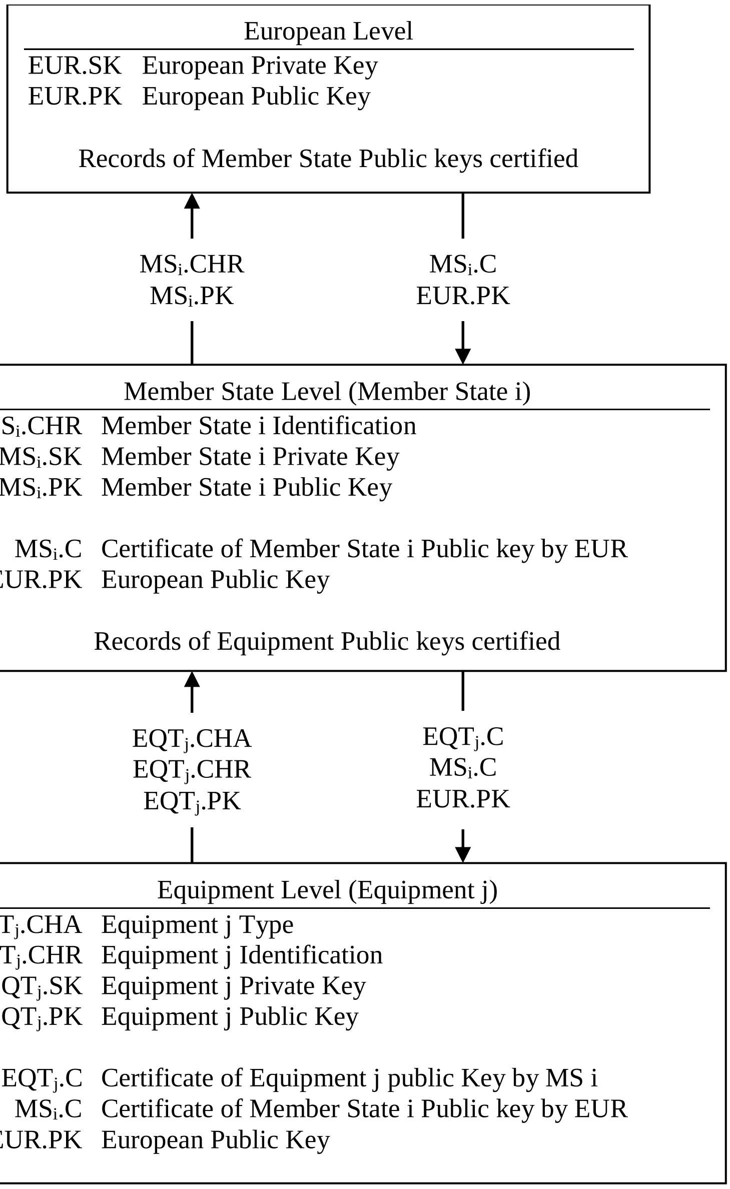
	using method 2 defined in [ISO 9797-1].	using method 2 defined in [ISO 9797-1].	
13.3, CSM_228	*CSM_228* When a remote interrogator receives RTM data from a VU, it shall send the entire RTM data to a control card in the data field of a PROCESS DSRC MESSAGE command, as described in Appendix 2. Then: *1.*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

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

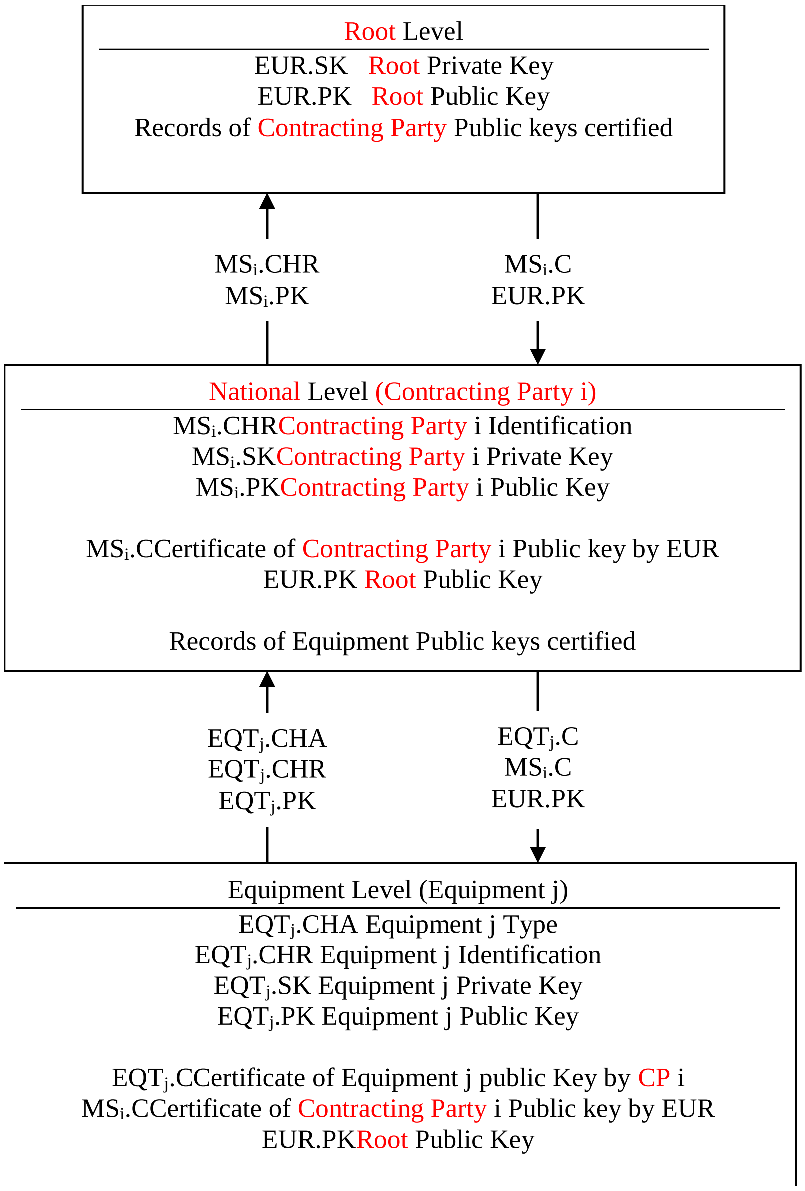
14.1, CSM_232	Note: the method the IDE uses to retrieve these certificates is not specified in this Appendix.	Note: the method the IDE uses to retrieve these certificates is not specified in this Sub-appendix.	
14.3, CSM_234	CSM_234 An IDE may perform verification of a signature over downloaded data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

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

Current image in CSM_010


European Level
EUR.SK European Private Key
EUR.PK European Public Key
Records of Member State Public keys certified
MS_i.CHR
MS_i.PK
MS_i.C
EUR.PK
Member State Level (Member State i)
MS_i.CHR Member State i Identification
MS_i.SK Member State i Private Key
MS_i.PK Member State i Public Key
MS_i.C Certificate of Member State i Public key by EUR
EUR.PK European Public Key
Records of Equipment Public keys certified
EQT_j.CHA
EQT_j.CHR
EQT_j.PK
EQT_j.C
MS_i.C
EUR.PK
Equipment Level (Equipment j)
EQT_j.CHA Equipment j Type
EQT_j.CHR Equipment j Identification
EQT_j.SK Equipment j Private Key
EQT_j.PK Equipment j Public Key
EQT_j.C Certificate of Equipment j public Key by MS i
MS_i.C Certificate of Member State i Public key by EUR
EUR.PK European Public Key

New proposed image


Root Level
EUR.SK Root Private Key
EUR.PK Root Public Key
Records of Contracting Party Public keys certified
MS$_i$.CHR
MS$_i$.PK
MS$_i$.C
EUR.PK
National Level (Contracting Party i)
MS$_i$.CHRContracting Party i Identification
MS$_i$.SKContracting Party i Private Key
MS$_i$.PKContracting Party i Public Key
MS$_i$.CCertificate of Contracting Party i Public key by EUR
EUR.PK Root Public Key
Records of Equipment Public keys certified
EQT$_j$.CHA
EQT$_j$.CHR
EQT$_j$.PK
EQT$_j$.C
MS$_i$.C
EUR.PK
Equipment Level (Equipment j)
EQT$_j$.CHA Equipment j Type
EQT$_j$.CHR Equipment j Identification
EQT$_j$.SK Equipment j Private Key
EQT$_j$.PK Equipment j Public Key
EQT$_j$.CCertificate of Equipment j public Key by CP i
MS$_i$.CCertificate of Contracting Party i Public key by EUR
EUR.PKRoot Public Key

	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.	

	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: 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).	To be deleted	
2, GNS_2	GNS_2 Manufacturers shall ensure that the GNSS receivers in the Smart Tachographs are compatible with the positioning services provided by the Galileo and the EGNOS systems. Manufacturers may also choose, in addition, compatibility with other satellite navigation systems.	GNS_2 Manufacturers shall ensure that the GNSS receivers in the smart tachographs are compatible with the positioning services provided by GPS, GLONASS and Galileo. Manufacturers may also choose, in addition, compatibility with other satellite navigation systems.	
2, GNS_3a (new)		GNS_3a GNSS receivers may be also capable of receiving and processing SBAS signals.	
3, GNS_5	GNS_5 The Vehicle Unit shall store in the VU database the position information for latitude and longitude with a resolution of 1/10 of minute or 1/600 of a degree as described in Appendix 1 for type GeoCoordinates.	GNS_5 The Vehicle Unit shall store in the VU database the position information for latitude and longitude with a resolution of 1/10 of minute or 1/600 of a degree as described in Sub-appendix 1 for type GeoCoordinates.	
4.2.1, GNS_18	GNS_18 Regarding the functions 1) the collection and distribution of GNSS data and	GNS_18 Regarding the functions 1) the collection and distribution of GNSS data and	

	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 SensorExternalGNSSSCIdentifier	EF.EGF 10th line Identifier of the security component of the external GNSS facility defined in Sub-appendix 1 as SensorExternalGNSSSCIdentifier	
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 Sub-appendix 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	

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

	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 • Bluetooth® – Core Version 4.2 • NMEA 0183 V4.1 protocol	~~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	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 achieved is internal to the VU, specified elsewhere in the Regulation, and is not specified in this Appendix.	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 achieved is internal to the VU, specified elsewhere in this Agreement, and is not specified in this Sub-appendix.	
4.1.1	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	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	

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

	See Appendix 12 for more information about the format and content of GNSS data. See Annex IB and IC for more information about event data code and faults.	See Sub-appendix 12 for more information about the format and content of GNSS data. See Appendix IB and IC for more information about event data code and faults.	
4.8	ITS units shall be able to request events data containing the list of all the unexpected events. These data are considered standard or personal, see Annex 3. The content of each event is in accordance with the documentation provided in Annex 1 of this appendix.	ITS units shall be able to request events data containing the list of all the unexpected events. These data are considered standard or personal, see Annex 3. The content of each event is in accordance with the documentation provided in Annex 1 of this Sub-appendix.	
Annex 1, point 2	See Appendix 12 – GNSS	See Sub-appendix 12 – GNSS	
Annex 1, point 3	Event codes table (available without driver consent)	New table, see at the end of thisdocument	
Annex 1, point 4	Event codes table (available with driver consent)	New table, see at the end of thisdocument	
Annex 1, point 5	Fault codes table (available without driver consent)	New table, see at the end of thisdocument	
Annex 3, line 375	--See Appendix 1 for definition of GeoCoordinates--	--See Sub-appendix 1 for definition of GeoCoordinates--	
Annex 3, line 389	IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information about NationAlpha--	IMPORTS NationAlpha FROM Sub-appendix 1; --See Sub-appendix 1 for more information about NationAlpha--	

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 card	- the 10 most recent events.	- date and time of event, - 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 correctly closed	- the 10 most recent events.	- date and time of card insertion, - 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 event.	- date and time of beginning of 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 last days of occurrence, - the 5 longest events over the last 365 days.	- control device (recording equipment) date and time - GNSS date and time, - 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 Member State 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 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 article	Text Appendix 14	Proposed text for AETR	Comments
TITLE/TABLE OF CONTENTS	(Title) APPENDIX 14. REMOTE COMMUNICATION FUNCTION	SUB-APPENDIX 14. REMOTE COMMUNICATION FUNCTION	
1	This Appendix specifies the design and the procedures to follow in order to perform the remote communication function (the Communication) as required in Article 9 of Regulation (EU) No. 165/2014 (the Regulation).	This Sub-appendix specifies the design and the procedures to follow in order to perform the remote communication function (the Communication) ~~as required in Article 9 of Regulation (EU) No. 165/2014 (the Regulation)~~.	Reference suppressed (not needed)
1, DSC_1	Regulation (EU) No. 165/2014 determines that the tachograph shall be equipped with a remote communication functionality that shall enable agents of the competent control authorities to read tachograph information from passing vehicles by using remote interrogation equipment (the Remote early detection communication reader [REDCR]), specifically, interrogation equipment connecting wirelessly using CEN 5.8 GHz Dedicated Short Range Communication (DSRC) interfaces. It is important to comprehend that this functionality is intended to serve only as a pre-filter in order to select vehicles for closer inspection, and it does not replace the formal inspection process as determined in the provisions of Regulation (EU) No. 165/2014. See recital 9 in the preamble of this regulation, stating that remote communication between the tachograph and control authorities for roadside	~~Regulation (EU) No. 165/2014 determines that~~ The tachograph shall be equipped with a remote communication functionality that shall enable agents of the competent control authorities to read tachograph information from passing vehicles by using remote interrogation equipment (the Remote early detection communication reader [REDCR]), specifically, interrogation equipment connecting wirelessly using CEN 5.8 GHz Dedicated Short Range Communication (DSRC) interfaces. It is important to comprehend that this functionality is intended to serve only as a pre-filter in order to select vehicles for closer inspection, and it does not replace the formal inspection process. ~~as determined in the provisions of Regulation (EU) No. 165/2014. See recital 9 in the preamble of this regulation, stating that~~ Remote communication between the tachograph and control authorities for roadside	

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

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

	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 Sub-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	

	- Data security provisions (such as encryption) concerning the content of the Data (which shall be specified within Appendix 11 Common Security Mechanisms). - 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 by an REDCR).	- Data security provisions (such as encryption) concerning the content of the Data (which shall be specified within Sub-appendix 11 Common Security Mechanisms). - 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 by an REDCR).	
3	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:	
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	

	DSC (n) identifier of a requirement for a specific DSRC appendix	DSC (n) identifier of a requirement for a specific DSRC Sub-appendix	
3	DSRC-VU definition DSRC-VU DSRC – Vehicle Unit. This is the “remote early detection facility” defined in Annex 1C.	DSRC-VU definition DSRC-VU DSRC – Vehicle Unit. This is the “remote early detection facility” defined in Appendix 1C.	
3	REDCR definition REDCR Remote early detection communication reader. This is the “remote early detection communication reader equipment” defined in Annex 1C.	REDCR definition REDCR Remote early detection communication reader. This is the “remote early detection communication reader 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 provides specific and controlled scenarios within which the Communication is to be used. The scenarios supported are: *"Communication Profile 1: Roadside inspection using a short range wireless communication Remote Early Detection Communication Reader instigating a physical roadside inspection (master-:-slave)* *Reader Profile 1a: via a hand aimed or temporary roadside mounted and aimed Remote Early Detection Communication* *Reader Profile 1b: via a vehicle mounted and directed Remote Early Detection Communication Reader".*	The supported scenarios within which the Communication is to be used are: *"Communication Profile 1: Roadside inspection using a short range wireless communication Remote Early Detection Communication Reader instigating a physical roadside inspection (master-:-slave)* *Reader Profile 1a: via a hand aimed or temporary roadside mounted and aimed Remote Early Detection Communication* *Reader Profile 1b: via a vehicle mounted and directed Remote Early Detection Communication Reader".*	
4.1.1.1, DSC_12	The VU shall be responsible to keep updated every 60 seconds and maintain the data to be stored in the VU, without any involvement of the DSRC communication	The VU shall be responsible to keep updated every 60 seconds and maintain the data to be stored in the VU, without any involvement of 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 Sub-appendix (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.	

4.1.1.5, DSC_17	Security data (securityData), comprising the data required by the REDCR to complete its ability to decrypt the Data shall be supplied as defined in Appendix 11 Common Security Mechanisms and presented as a data concept value, for temporary storage in the DSRC-VU as the current version of securityData, in the form defined in this Appendix section 5.4.4.	Security data (securityData), comprising the data required by the REDCR to complete its ability to decrypt the Data shall be supplied as defined in Sub-appendix 11 Common Security Mechanisms and presented as a data concept value, for temporary storage in the DSRC-VU as the current version of securityData, in the form defined in this Sub-appendix section 5.4.4.	
4.1.1.6, DSC_18	This profile covers the use case where an agent of the competent control authorities, uses a short range remote communication Remote Early Detection Communication Reader (5.8 GHz DSRC interfaces operating within ERC 70-03, and tested against the appropriate parameters of EN 300 674-1 as described in section 5) (the REDCR) to remotely identify a 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 should be stopped.	This profile covers the use case where an agent of the competent control authorities, uses a short range remote communication Remote Early Detection Communication Reader (5.8 GHz DSRC interfaces operating within ERC 70-03, and tested against the appropriate parameters of EN 300 674-1 as described in section 5) (the REDCR) to remotely identify a 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 should be stopped.	
4.2	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.	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.	
5.1, DSC_19	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 comprises payload data and security data concept values	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 comprises payload data and security data concept values	

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

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

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

5.3.3.2, DSC_33	DSC_33 In the test environment in a workshop (see section 6.3), a DSRC-VU antenna, affixed according to 5.1 above, shall successfully connect with a standard test communication and successfully provide an RTM transaction as defined within this Appendix, at a distance between 2 and10 meters, better than 99% of the time, averaged over 1000 read interrogations.	DSC_33 In the test environment in a workshop (see section 6.3), a DSRC-VU antenna, affixed according to 5.1 above, shall successfully connect with a standard test communication and successfully provide an RTM transaction as defined within this Sub-appendix, at a distance between 2 and10 meters, better than 99% of the time, averaged over 1000 read interrogations.	
5.4.4, DSC_37	DSC_37 The semantic structure of the Data when passed across the 5.8 GHz DSRC interface shall be consistent with what described in this Appendix. The way these data are structured is specified in this clause.	DSC_37 The semantic structure of the Data when passed across the 5.8 GHz DSRC interface shall be consistent with what described in this Sub-appendix. The way these data are structured is specified in this clause.	
5.4.4, DSC_38	DSC_38 The payload (RTM data) consists of the concatenation of 1. EncryptedTachographPayload data, which is the encryption of the TachographPayload defined in ASN.1 in section 5.4.5. The method of encryption is described in Appendix 11 2. dSRCSecurityData, specified in Appendix 11.	DSC_38 The payload (RTM data) consists of the concatenation of 1. EncryptedTachographPayload data, which is the encryption of the TachographPayload defined in ASN.1 in section 5.4.5. The method of encryption is described in Sub-appendix 11 2. dSRCSecurityData, specified in Sub-appendix 11.	
5.4.4, DSC_40	See current tachograph payload definition at the end of this document	See new proposed tachograph payload definition at the end of this document	

5.4.4, DSC_40	RtmData definition
	RtmData ::= SEQUENCE {
	encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting TachographPayload as per Appendix 11 --}),
	DSRCSecurityData OCTET STRING
	}
		RtmData definition
		RtmData ::= SEQUENCE {
		encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting TachographPayload as per Sub-appendix 11 --}),
		DSRCSecurityData OCTET STRING
		}	

5.4.5, Table 14.3	See current table at the end of this document	See new proposed table at the end of this document	

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

	OwsPayload as per Appendix 11 --}), DSRCSecurityData OCTET STRING }	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 Sub-appendix 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 15509[1]
            tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
            tp15638DrivingWithoutValidCard  BOOLEAN,    -- 1= Invalid card usage (see Annex 1C)
            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
            tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
-- 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
            tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration
data
```

New proposed TachographPayload definition

```
TachographPayload ::= SEQUENCE {
            tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509[1]
            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)
            tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see
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
            tp15638PowerSupplyInterruption  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
            tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
            tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
            tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration
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 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 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,`

RTM3 **Driving Without Valid Card**	The VU shall generate a boolean value for data element RTM3 tp15638DrivingWithoutValidCard. 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	1 (TRUE) = Indicates invalid card usage	tp15638DrivingWithoutValidCard BOOLEAN,
RTM4 **Valid Driver Card**	The VU shall generate a boolean value for data element RTM4 tp15638DriverCard on the basis of the data stored in the VU and defined in Appendix 1. If no valid driver card is present the VU shall set the variable to TRUE ELSE if a valid driver card is present	0 (FALSE) = Indicates a valid driver card	tp15638DriverCard BOOLEAN,
RTM5 **Card Insertion while Driving**	The VU shall generate a boolean value for data element RTM5. 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	1 (TRUE) = Indicates card insertion while driving within last 10 days of occurrence	tp15638CardInsertion BOOLEAN,
RTM6 **Motion Data Error**	The VU shall generate a boolean value for data element RTM6. 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. ELSE if there are no such events in the last 10 days of occurrence, the	1 (TRUE) = Indicates motion data error within last 10 days of occurrence	tp15638motionDataError BOOLEAN,

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	`tp15638vehicleMotionConflict 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	`tp15638currentActivityDriving 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	`tp15638lastSessionClosed BOOLEAN`

RTM11
Power Supply Interruption
	The VU shall generate an integer value for data element RTM11.
	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 Annex 1C.
	ELSE if in the last 10 days of
		-- Number of power supply interruptions in last 10 days of occurrence	`tp15638powerSupplyInterruption`
			`INTEGER (0..127),`

RTM12
Sensor Fault
	The VU shall generate an integer value for data element RTM12.
	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.
		--sensor fault one octet as per data dictionary	`tp15638SensorFault`
			`INTEGER (0..255),`

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. ELSE if no "Time Adjustment" event.	Time of the last time adjustment	`tp15638TimeAdjustment INTEGER(0..4294967295),`
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 of the latest security breach attempt event recorded by the VU. ELSE if no "security breach attempt " event as defined in Annex 1C is	Time of last breach attempt -- Default value =0x00FF	`tp15638LatestBreachAttempt INTEGER(0..4294967295),`
RTM15 **Last Calibration**	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM15 on the basis of the presence of Last Calibration data as defined in Annex 1C. 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.	Time of last calibration data	`tp15638LastCalibrationData INTEGER(0..4294967295),`
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 ELSE if there has been no previous calibration the VU shall set the value of RTM16 to 0.	Time of previous calibration data	`tp15638PrevCalibrationData INTEGER(0..4294967295),`

RTM17 **Date Tachograph Connected**	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	Date tachograph connected	`tp15638DateTachoConnected INTEGER(0..4294967295),`
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 (0..255),`
RTM19 **Timestamp**	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(0..4294967295),`

New proposed 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 Sub-appendix 1 *VehicleRegistrationIdentification*	Vehicle Registration Plate expressed as a string of characters	`tp15638VehicleRegstrationPlate 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 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 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	1 (TRUE) - Indicates irregularities in speed within last 10 days of occurrence	`tp15638speedingEvent BOOLEAN,`
RTM3 **Driving Without Valid Card**	The VU shall generate a boolean value for data element RTM3 tp15638DrivingWithoutValidCard. 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. ELSE if there are no events in the last 10 days of occurrence, the tp15638DrivingWithoutValidCard	1 (TRUE) = Indicates invalid card usage	`tp15638DrivingWithoutValidCard BOOLEAN,`
RTM4 **Valid Driver Card**	The VU shall generate a boolean value for data element RTM4 tp15638DriverCard on the basis of the data stored in the VU and defined in Sub-appendix 1. If no valid driver card is present the VU shall set the variable to TRUE ELSE if a valid driver card is present	0 (FALSE) = Indicates a valid driver card	`tp15638DriverCard BOOLEAN,`

RTM5
Card Insertion while Driving
	The VU shall generate a boolean value for data element RTM5.
	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.
	ELSE if there are no such events in the last 10 days of occurrence, the tp15638CardInsertion variable shall be set to FALSE.
		1 (TRUE) = Indicates card insertion while driving within last 10 days of occurrence	`tp15638CardInsertion`
			`BOOLEAN,`

RTM6
Motion Data Error
	The VU shall generate a boolean value for data element RTM6.
	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.
	ELSE if there are no such events in the last 10 days of occurrence, the
		1 (TRUE) = Indicates motion data error within last 10 days of occurrence	`tp15638motionDataError`
			`BOOLEAN,`

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 10 days of occurrence, the
		1 (TRUE) = Indicates motion conflict within last 10 days of occurrence	`tp15638vehicleMotionConflict`
			`BOOLEAN,`

RTM8
2nd Driver Card
	The VU shall generate a boolean value for data element RTM8 on the basis of Appendix 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 Appendix 1C the VU shall set the variable to TRUE ELSE if the current activity is recorded in the VU as “DRIVING” the	1 (TRUE) = other activity selected; 0 (FALSE) = driving selected	`tp15638currentActivityDriving` `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 Appendix 1C the VU shall set the variable to TRUE. ELSE if the last card session was	1 (TRUE) = improperly closed 0 (FALSE) = properly closed	`tp15638lastSessionClosed` `BOOLEAN`

RTM11
Power Supply Interruption
	The VU shall generate an integer value for data element RTM11.
	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
		-- Number of power supply interruptions in last 10 days of occurrence	`tp15638powerSupplyInterruption`
			`INTEGER (0..127),`

RTM12 **Sensor Fault**	The VU shall generate an integer value for data element RTM12. 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.	--sensor fault one octet as per data dictionary	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Time Adjustment**	The VU shall generate an integer value (timeReal from Sub-appendix 1) 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.	Time of the last time adjustment	`tp15638TimeAdjustment INTEGER(0..4294967295),`

RTM14 **Security Breach Attempt**	The VU shall generate an integer value (timeReal from Sub-appendix 1) for data element RTM14 on the basis of the presence of a Security breach 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	Time of last breach attempt -- Default value =0x00FF	`tp15638LatestBreachAttempt INTEGER(0..4294967295),`
RTM15 **Last Calibration**	The VU shall generate an integer value (timeReal from Sub-appendix 1) for data element RTM15 on the basis 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	Time of last calibration data	`tp15638LastCalibrationData INTEGER(0..4294967295),`
RTM16 **Previous Calibration**	The VU shall generate an integer value (timeReal from Sub-appendix 1) for 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.	Time of previous calibration data	`tp15638PrevCalibrationData INTEGER(0..4294967295),`
RTM17 **Date Tachograph Connected**	For data element RTM17 the VU shall generate an integer value (timeReal from Sub-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 (Sub-appendix 1) from the vuCalibrationRecords with CalibrationPurpose equal to: ’03’H	Date tachograph connected	`tp15638DateTachoConnected INTEGER(0..4294967295),`

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 (0..255),`
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(0..4294967295),`

	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 CONTENTS	(Title) APPENDIX 15. MIGRATION: MANAGING THE CO-EXISTENCE OF EQUIPMENT GENERATIONS	SUB-APPENDIX 15. MIGRATION: MANAGING THE CO-EXISTENCE OF EQUIPMENT GENERATIONS	
1	For the purposes of this Appendix, the following definitions are used.	For the purposes of this Sub-appendix, the following definitions are used.	
1	smart tachograph system definition smart tachograph system: as defined by this Annex (chapter 1: definition bbb);	smart tachograph system definition smart tachograph system: as defined by this Appendix (chapter 1: definition bbb);	
1	first generation tachograph system definition first generation tachograph system: as defined by this Regulation (article 2: definition 1);	first generation tachograph system definition first generation tachograph system: as defined in the 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 Sub-appendix 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 article	Text Appendix 16	Proposed text for AETR	Comments
TITLE/TABLE OF CONTENTS	*(Title)* *APPENDIX 16. ADAPTOR FOR M 1 AND N1 CATEGORY VEHICLES*	*SUB-APPENDIX 16. ADAPTOR FOR M 1 AND N1 CATEGORY VEHICLES* *(update table of contents according to the change in the titles)*	
2.1, ADA_001	The adaptor shall provide a connected VU with secured motion data permanently representative of vehicle speed and distance travelled. The adaptor is only intended for those vehicles that are required to be equipped with recording equipment in compliance with this Regulation. It shall be installed and used only in those types of vehicle defined in definition yy) 'adaptor' of Annex IC 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 16. The adaptor shall not be mechanically interfaced to a moving part of the vehicle, but connected to the speed/distance impulses which are generated by integrated sensors or alternative interfaces.	The adaptor shall provide a connected VU with secured motion data permanently representative of vehicle speed and distance travelled. The adaptor is only intended for those vehicles that are required to be equipped with control device in compliance with this Agreement. It shall be installed and used only in those types of vehicle defined in definition yy) 'adaptor' of Appendix IC 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 16. The adaptor shall not be mechanically interfaced to a moving part of the vehicle, but connected to the speed/distance impulses which are generated by integrated sensors or alternative interfaces.	
2.1, ADA_002	ADA_002 A type approved motion sensor (according to the provisions of this Annex IC, section 8, Type approval of recording equipment and tachograph cards) shall be fitted into the adaptor housing, which shall also include a pulse converter	ADA_002 A type approved motion sensor (according to the provisions of this Appendix IC, section 8, Type approval of control device and tachograph cards) shall be fitted into the adaptor housing, which shall also 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.	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.	
2.3, ADA_004	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 section 4.4 of this Appendix shall apply instead.	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 section 4.4 of this Sub-Appendix shall apply instead.	
3, title	3. Requirements for the recording equipment when an adaptor is installed	3. Requirements for the control device when an adaptor is installed	
3	The requirements in the following Chapters indicate how the requirements of this Annex shall be understood when an adaptor is used. The related requirement numbers of Annex IC are provided between brackets.	The requirements in the following Chapters indicate how the requirements of this Appendix shall be understood when an adaptor is used. The related requirement numbers of Appendix IC are provided between brackets.	
3, ADA_005	ADA_005 The recording equipment of any vehicle fitted with an adaptor must comply with all the provisions of this Annex, except otherwise specified in this Appendix.	ADA_005 The control device of any vehicle fitted with an adaptor must comply with all the provisions of this Appendix, except otherwise specified in this Sub-Appendix.	
3, ADA_006	ADA_006 When an adaptor is installed, the recording equipment includes cables, the adaptor (including a motion sensor), and a VU [01].	ADA_006 When an adaptor is installed, the control device includes cables, the adaptor (including a motion sensor), and a VU [01].	
3, ADA_007	ADA_007 The detection of events and/or faults function of the recording equipment is modified as follows: - the “power supply interruption” event shall be	ADA_007 The detection of events and/or faults function of the control device is modified as follows: - the “power supply interruption” event shall be	

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

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