United Nations ECE/TRANS/WP.29/GRSG/2015/16

Economic and Social Council

Distr.: General
20 February 2015

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Working Party on General Safety Provisions

108th session
Geneva, 4–8 May 2015
Item 3 of the provisional agenda
Regulation No. 39 (Speedometer)

Proposal for draft 01 series of amendments to Regulation No. 39 (Speedometer)

Submitted by the expert from the Fédération Internationale de l'Automobile *

The text reproduced below was prepared by the expert from the Fédération Internationale de l'Automobile (FIA) proposing further amendments to the proposal submitted by Belgium on performance requirements for the installation of odometers on vehicles (ECE/TRANS/WP.29/GRSG/2015/15). The modifications to document ECE/TRANS/WP.29/GRSG/2015/15 are marked in bold characters.

* In accordance with the programme of work of the Inland Transport Committee for 2012–2016 (ECE/TRANS/224, para. 94 and ECE/TRANS/2012/12, programme activity 02.4), the World Forum will develop, harmonize and update Regulations in order to enhance the performance of vehicles. The present document is submitted in conformity with that mandate.

I. Proposal

The title of the Regulation, amend to read:

"UNIFORM PROVISIONS CONCERNING THE APPROVAL OF VEHICLES WITH REGARD TO THE SPEEDOMETER AND ODOMETER EQUIPMENT INCLUDING ITS INSTALLATION"

Table of contents, Annexes, amend to read:

"ANNEXES

……

Annex 3 - Test of speedometer **and odometer** accuracy for conformity of production

Annex 4 - Test of odometer manipulation protection for conformity of production

Annex 5 - Approach of a Protection Profile against Mileage Fraud according to Common Criteria"

Paragraph 1., amend to read (including footnote [1]):

"1. SCOPE

This Regulation applies to the approval of vehicles of categories L, M and N.[1]

---

[1] As defined in the Consolidated Resolution on the Construction of Vehicles (R.E.3.), document ECE/TRANS/WP.29/78/Rev.3, para. 2. - www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29resolutions.html"

Paragraphs 2.1. to 2.6., amend to read:

"2.1. "*Approval of a vehicle*" means the approval of a vehicle type with regard to the speedometer and odometer equipment including its installation.

2.2. "*Type of vehicle in respect of its speedometer and odometer*" means vehicles which do not among themselves display any essential differences, where those differences can apply, in particular, to the following:

2.2.1. the size designation of the tyres chosen from the range of tyres normally fitted;

2.2.2. the overall transmission ratio, including any reduction drives, to the speedometer;

2.2.3. the type of speedometer as characterised by:

2.2.3.1. the tolerances of the speedometer's measuring mechanism;

2.2.3.2. the technical constant of the speedometer;

2.2.3.3. the range of speeds displayed.

2.2.4. the type of odometer as characterised by:

2.2.4.1. the technical constant of odometer;

2.2.4.2. the number of numerals.

2.3. "*Tyres normally fitted*" means the type or types of tyre provided by the manufacturer on the vehicle type in question; snow tyres shall not be regarded as tyres normally fitted;

2.4. "*Normal running pressure*" means the cold inflation pressure specified by the vehicle manufacturer increased by 0.2 bar;

2.5. "*Speedometer*" means that part of the speedometer equipment which indicates to the driver the speed of the vehicle at any given moment; [2]

2.5.1. "*Tolerances of the speedometer's measuring mechanism*" shall mean the accuracy of the speedometer instrument itself, expressed as the upper and the lower speed indication limits for a range of speed inputs;

2.5.2. "*Technical constant of the speedometer*" shall mean the relationship between the input revolutions or pulses per minute and a specified displayed speed;

2.6. "*Odometer*" means that part of the information equipment which indicates to the driver the actual mileage of the vehicle resulting from any driving operation and include the (physical) measurement parts, the computation, the storage and alternative display options.

2.6.1. "*Technical constant of the odometer*" means the relationship between the input revolutions or pulses and the distance travelled by the vehicle.

2.7. "*Unladen vehicle*" means the vehicle in running order, complete with fuel, coolant, lubricant, tools and a spare wheel (if provided as standard equipment by the vehicle manufacturer), carrying a driver weighing 75 kg, but no driver's mate, optional accessories or load."

Paragraphs 3.1. to 3.2.1., amend to read:

"3.1. The application for approval of a vehicle type with regard to the speedometer and odometer equipment including its installation shall be submitted by the vehicle manufacturer or by their duly accredited representative.

…

3.2.1. a description of the vehicle type with regard to the items mentioned in paragraphs 2.2., 2.3., 2.4., 2.5. and 2.6. above; the vehicle type shall be specified."

Paragraph 4., amend to read:

"4.1. If the vehicle type submitted for approval pursuant to this Regulation meets the requirements of the Regulation in respect of the speedometer and odometer equipment including its installation, approval of that vehicle type shall be granted."

Insert a new paragraph 5.1., to read:

"5.1. An onboard speedometer and odometer complying with the requirements of this Regulation shall be fitted to the vehicle to be approved."

Paragraphs 5.1. to 5.3. (former), renumber as paragraphs 5.2. to 5.4.

Insert new paragraphs 5.5. and ***5.5.3.,*** to read:

"5.5. The display of the odometer shall be visible or accessible to the driver. The odometer shall contain at least an integer number composed of a minimum of 6 numerals for the vehicles of categories M and N, and at least an integer

[2] This does not include the speed- and distance-indicating part of a tachograph if this complies with type approval specifications which do not permit an absolute difference between true and indicated speed which is higher than the values resulting from the requirements in paragraph 5.3. below.

number composed of a minimum of 5 numerals for the vehicles of category L. Nevertheless, the Type Approval Authorities may also accept an integer number composed of at least 5 numerals for the vehicles of categories M and N if the intended use of the vehicle justifies it. **If the odometer reaches its maximum value of display (e.g. 999,999 km), the display shall stop at the maximum value (e.g. 999,999 km).**

5.5.1. In the case of vehicles manufactured for sale in any country where imperial units are used, the odometer may be marked in miles. **The total mileage displayed by the odometer shall not vary from the actual mileage covered by more than ± 4 per cent.**

5.5.2. Odometer data on the complete processing chain (measurement, computation, storage, display) shall be protected against manipulation. The correct mileage date shall be securely – based on the security and assurance requirements expressed in Protection Profile (described in Annex 5) - stored inside the vehicle and successfully evaluated according Common Criteria V3.1 of September 2012. The Common Criteria Methodology and its testing Methods (CEM) is internationally accepted, publicly available (www.commoncriteriaportal.org) and released as ISO/IEC 15408 and ISO/IEC 18045. Manipulations shall be so time and cost intensive that they are no longer cost-efficient compared to the sales price, risk of mortal danger or environmental perils that can be achieved during the complete lifetime of the vehicle. The mileage data of this electronic control module shall be readable via the 16 PIN on-board diagnostic (OBD) port inside the vehicle but protected against (over) writing and changing the values. The date shall be accessible for all interested stakeholders, e.g. workshops, second hand vehicle dealers, automobile clubs, authorities, etc. Any inconsistency between the mileage in the display and the mileage in the secured place in an electronic control unit should be visible for drivers in the dashboard, e.g. as a fault message or via a malfunction indication lamp.

5.5.3. In the case of reparation or replacement of the odometer or replacement of the related components, it shall result in a display of the same number or after a course of limited distance as before the reparation or replacement. For these methods of replacement or reparation, verified countermeasures need to be in place to eliminate paths of manipulations or misuses of the values as well. The technical constant of the odometer cannot be changed after reparation, the accurate mileage is securely and manipulation protected stored inside the vehicle. This value shall be readable with OBD devices in a trustable way to be able to compare this secure value with the actual displayed value."

Insert new paragraphs 10. to 10.4., to read:

"10. TRANSITIONAL PROVISIONS

10.1. As from the official date of entry into force of the 01 series of amendments, no Contracting Party applying this Regulation shall refuse to grant or refuse to accept type approvals under this Regulation as amended by the 01 series of amendments.

10.2. As from 1 September 2017, Contracting Parties applying this Regulation shall grant new type approvals only if the vehicle type to be approved meets the requirements of this Regulation as amended by the 01 series of amendments.

10.3. Contracting Parties applying this Regulation shall not refuse to grant extensions of type approvals for existing types which have been granted according to the preceding series of amendments to this Regulation.

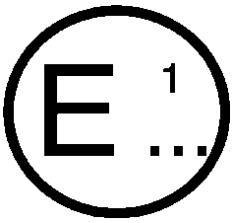
10.4. After the date of entry into force of the 01 series of amendments to this Regulation, Contracting Parties applying this Regulation shall continue to accept type approvals granted according to the preceding series of amendments to the Regulation."

Annexes 1 and 2, amend to read:

"**Annex 1**

COMMUNICATION

(Maximum format: A4 (210 x 297 mm))



issued by : Name of administration:
.....
.....
.....

concerning: [2] APPROVAL GRANTED
APPROVAL EXTENDED
APPROVAL REFUSED
APPROVAL WITHDRAWN
PRODUCTION DEFINITELY DISCONTINUED

of a vehicle type with regard to the speedometer and odometer equipment including its installation pursuant to Regulation No. 39.

Approval No.: ..... Extension No.: .....

1. Trade name or mark of the vehicle: .....

2. Vehicle type: .....

3. Manufacturer's name and address: .....

.....

4. If applicable, name and address of the manufacturer's representative: .....

.....

5. Description of the speedometer equipment: .....

.....

5.1. Details of tyres normally fitted: .....

5.2. Details of tyres fitted during the test: .....

5.3. Ratio of speedometer equipment: .....

6. Description of the odometer equipment **including evaluation evidence**: .....

.....

7. Mass of vehicle as tested and its distribution between the axles:

.....

8. Variants: .....

9. Vehicle submitted for approval on: .....

10. Technical service responsible for conducting approval tests: .....

.....

11. Date of report issued by that service: .....

12. Number of report issued by that service: .....

13. Approval granted/refused/extended/withdrawn [2]

14. Position of approval mark on the vehicle: .....

15. Place: .....

16. Date: .....

17. Signature: .....

_____

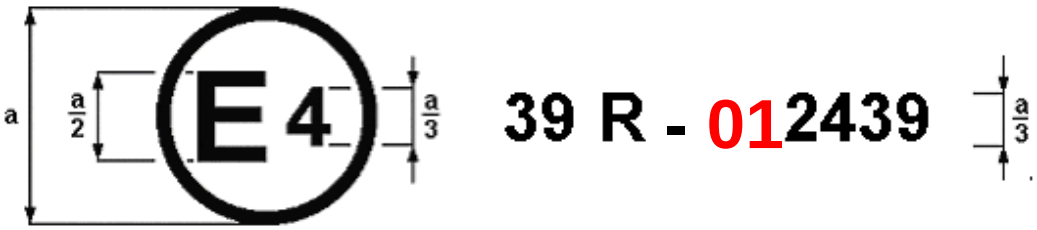
[1] Distinguishing number of the country which has granted/extended/refused/ withdrawn approval (see approval provisions in the Regulation).

[2] Strike out what does not apply."

Annex 2

ARRANGEMENTS OF APPROVAL MARKS

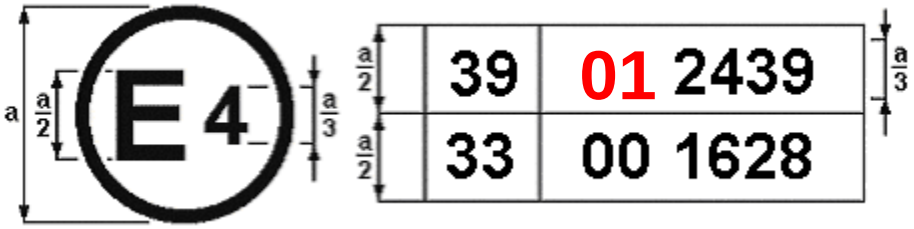
Model A
(see paragraph 4.4. of this Regulation)



a = 8 mm min.

The above approval mark affixed to a vehicle shows that the vehicle type concerned has been approved in the Netherlands (E 4), pursuant to Regulation No. 39. The approval number indicates that the approval was granted in accordance with the requirements of Regulation No. 39 **incorporating the 01 series of amendments**.

Model B
(see paragraph 4.5. of this Regulation)



a = 8 mm min.

The above approval mark affixed to a vehicle shows that the vehicle type concerned has been approved in the Netherlands (E 4) pursuant to Regulations Nos. 39 and 33.[1] The approval numbers indicate that, at the dates when the respective approvals were granted, **Regulation No. 39 incorporated the 01 series of amendments and Regulation No. 33 was** still in its original form.

---

[1] The second number is given merely as an example"

Insert new Annexes 4 and 5, to read:

"**Annex 4**

TEST OF ODOMETER MANIPULATION PROTECTION FOR CONFORMITY OF PRODUCTION

(to be developed)

Annex 5

APPROACH OF PROTECTION PROFILE AGAINST MILEAGE FRAUD ACCORDING TO COMMON CRITERIA

1. Objective

1.1. The security concept on mileage fraud is based on a Protection Profile to be developed by the stakeholders in accordance with the common criteria version 3.1 of September 2012 as published in standard ISO/IEC 15408.[3]

1.2. The aim of this Protection Profile is to ensure that the mileage of a vehicle displayed to a driver, buyer, seller, repairer or an authority reflects the actual mileage of the vehicle that results from any driving operation.

1.3. To achieve an economical balance between the protection against the mileage fraud and the benefit a fraud can achieve, the vehicle manufacturer can choose the appropriate protection for their vehicles by defining the Security Target based on the Protection Profile. Latest every twenty-four months a group of all stakeholders shall decide if the Protection Profile shall be upgraded according to the technical developments.

2. Target of Evaluation (TOE): Overview

The Protection Profile covers the entire odometer system related to mileage fraud and any relevant use cases encountered during the vehicle's lifecycle. The TOE is thus comprised of subsystems with respective to the Protection Profile. In terms of subsystems and system boundaries from a mileage fraud viewpoint, four subsystems can be identified:

2.1. Mileage computation subsystem:

This subsystem is comprised of all Electronic Control Units (ECUs) and sensors that are involved in the computation of the vehicle's mileage. A special threat that has to be countered by the measures imposed by this Protection Profile are attempts to stop the recording of added mileage during driving, e.g. by faking wheel movement sensor signals to the computation units.

2.2. Mileage storage subsystem:

This subsystem is comprised of ECUs or modules of ECUs within which the value of the actual mileage is stored. As long as the security functional requirements and security assurance requirements of this Protection Profile are met, the vehicle manufacturers are free to select their implementation. They could opt to store the mileage in a dedicated ECU or choose a strategy of distributed and/or multiple storage across several ECUs to be able to detect attacks against a single ECU easier.

2.3. Mileage display device subsystem:

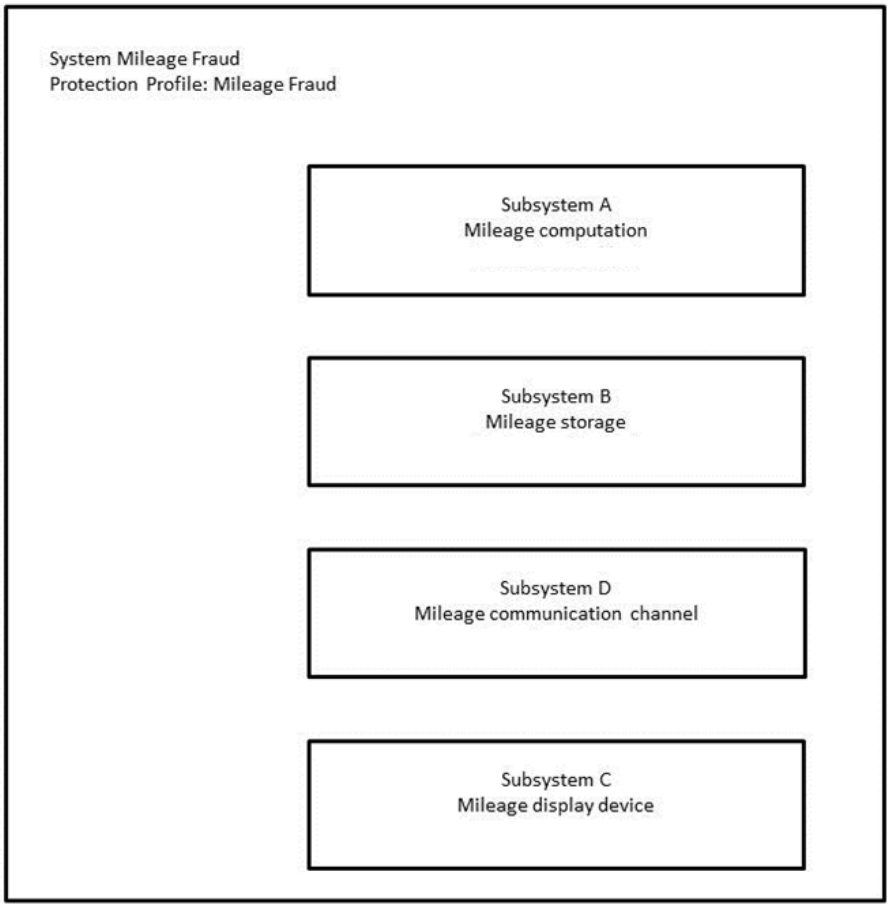
This subsystem is comprised of the display device which is used by a stakeholder to retrieve and display the actual mileage of the vehicle. This could be an external certified device that is used within a workshop or/and this could be an in-vehicle display. As long as the Protection Profile for this subsystem is met, every alternative is valid. Although from a security perspective it is much easier for a potential attacker to try to corrupt a built-in display to which there is direct access as opposed to the effort it takes to corrupt the values that go out from the vehicle to an external device which cannot be corrupted before.

[3] See also: http://www.commoncriteriaportal.org/

2.4. Mileage communication channel subsystem:

This subsystem is comprised of the communication channel and communication process used to transmit the value of the actual mileage to the display device. This channel as the fourth relevant subsystem of the overall mileage fraud solution has also to be protected by the Protection Profile to prevent "Man in the Middle" attacks. If, for example, the mileage is perfectly accurate and safely stored in the vehicle but the communication between the display device is a form of unencrypted messages over the OBD-port, then an attacker could easily implement a small hardware solution inside the vehicle that accesses the bus, intercepts the request for mileage retrieval and corrupts the answer to the display device. State of the art encryption technology for the communication channel between stored value (Subsystem B) and display device (Subsystem C) will thus be enforced by the Protection Profile.

Figure 1
Target of Evaluation (System Overview)



3. Operational Use

3.1. Once installed and tested during the assembly of the vehicle, every "driving movement" of the vehicle, may it be on the road or on test stands (e.g. during periodical technical inspections) will always increase the mileage value stored in the subsystem "Mileage storage". The value in "Mileage storage" cannot ever decrease or be reset to zero over time.

3.2. Even a complete exchange of the "Mileage storage" subsystem (Depending on the vendor's implementation of this Protection Profile this could imply the exchange of one or more ECUs) shall not lead to a mileage value that is corrupted.

3.3. Because the overall mileage fraud Protection Profile's goal is fulfilled when the effort for the attacker exceeds the financial benefits that can be achieved with intervention, this could be potentially realized via a distributed protected storage of the mileage in so many ECUs that the costly exchange of all storage ECUs is economically unattractive for an attacker, even for premium class vehicles.

3.4. Any time a certified display device (Subsystem C) issues a mileage retrieval command via the certified communication channel (Subsystem D), the mileage storage (Subsystem B) will send out the actual mileage, computed and updated constantly by the mileage computation subsystem (Subsystem A) to be presented to any stakeholder.

4. Conformance Claims

4.1. Conformance Claim (CC)

This Protection profile claims conformance to Common Criteria for Information Technology Security Evaluation, (Part 1-3), Version 3.1, Revision 4, 2012

4.2. Conformance Statement

This Protection Profile requires strict conformance of any Security Target or Protection Profile claiming conformance to this Protection Profile.

Annotation: This ensures that no Security Target document that a Vehicle Manufacturer uses to have their implementation tested against imposes lesser rigid security or assurance requirements on the solution than the ones set out in this Protection Profile.

5. Security Problem Definition

5.1. Primary Information asset: Actual Mileage

Annotation: By design - see the structure of an overall system comprised of four interacting subsystems this overall asset protection requires a set of assets to be protected by the Protection Profiles of the respective subsystems.

As an example, the subsystem "Mileage storage" will have to protect at least the following two assets:

(a) the actual mileage (an asset protection task it takes over for the overall system), and

(b) the cryptographic key it uses to communicate in a secure and trustworthy manner with the subsystem "Mileage Display Device".

5.2. Subjects and external Entities

A list of all subjects that can either rightfully interact with the system like regular users that use the display device within a workshop to retrieve and display the actual mileage, but also attackers that try to harm the system's integrity. In this Protection Profile's design, the Mileage computation subsystem encapsulates the wheel sensors so no external entity is depicted here.

6. Threats

Threats to the assets are named in the Protection Profile with "T." followed by a unique name identifying the threat. The author of a Protection Profile or Security Target document is free to assign any name of their choice as long as it is unique. For the overall Protection Profile "Mileage Fraud" the following main threat should be countered:

6.1. T.Mileage_Corrupted

Threat that the value displayed in the subsystem "Mileage display device" does not reflect the actual mileage of the vehicle.

Annotation: When broken down in the Protection Profiles to the subsystems, this threat disseminates in a variety of threats for the subsystems.

6.2. T.Fake_Mileage_Computing

Threat that an attacker tries to emulate and/or corrupt the sequence of mileage increments delivered for storage to the subsystem "Mileage storage" by the subsystem "Mileage computation".

6.3. T.Hardware_Memory_Loss

In the past, attack hackers have successfully brought Electrically Erasable Programmable Read-Only Memory (EEProms) in a state where they lost their memory, thus lost the actual mileage and could be reprogrammed with a corrupted value.

6.4. T.Intercepted_Communication

The subsystem "Mileage display device" needs to be part of the threat.

7. Organization Security Policies

Organization Security Policies (OSP) are security rules, procedures, practices, or guidelines imposed by an organization upon its operations to support security objectives and can be imposed on the TOE or it's environment. They are named with "OSP." followed by a unique name.

7.1. OSP.Audit

The subsystem "Mileage storage" monitors and reports attempts of failed authentification of the subsystem "Mileage Display device".

7.2. OSP.Crypto:

The authorities responsible for the key generation for the communication (Trust centers) shall ensure that keys for mileage display devices are only issued to legitimate stakeholders.

8. Assumptions about the environment of the TOE

A list of assumptions about the environment of the TOE is also a mandatory part of the Protection Profile.

8.1. A.System_Activation

The vehicle manufacturers will always activate the system of mileage computation and storage after the assembly of the vehicle.

Assumptions like this narrow down the possible attack scenarios the TOE has to be aware of, e.g. without activation it is obviously too easy to drive around in the vehicle without recording mileage.

9. Security Objectives

The list of security objectives for the TOE shall be complete so that all threats are dealt with by at least one security objective, thus no threat remains. Furthermore, there should be no unnecessary security objective defined to spare development effort and cost. A matrix view highlighting the n:m-relationship between threats and security objectives will be used in the Protection Profile to ensure both aspects. The subsystem "Mileage storage" will, among others, contain the following objectives:

9.1. O.Access:

The TOE shall control user access to functions (activate mileage storage) and data (actual mileage).

9.2. O.Audit

The TOE shall audit attempts to undermine system security

9.3. O.Authentication

The TOE should authenticate connected entities respectively subsystems "mileage computation" and subsystem "mileage display device"

9.4. O.Integrity

The TOE shall maintain stored mileage data integrity

9.5. O.Output

The TOE shall ensure that data output to subsystem "mileage display device" reflects accurately data stored.

Only if all security objectives are met by a TOE, the TOE is protected against all listed threats.

10. Security Requirements

10.1. Security requirements are detailed "best practises" in the field of secure system development. The Common Criteria Group has developed sets of requirements and grouped them into a hierarchical system of:

(a) Functional classes;

(b) Functional Families;

(c) Functional Components;

(d) Functional elements.

10.2. Functional classes address aspects like:

(a) FAU-Class Security Audit;

(b) FDP- Class Data Protection;

(c) FCO- Class Communication.

10.3. The author of a Protection Profile can thus easily pick security requirements from the catalogue described in CC Part 2, tailor them to their needs and apply them. In the same way it is demonstrated that all threats are tackled by security objectives it is then necessary to demonstrate in a matrix, that each security objective is at least addressed by one security functional requirement from the list.

As an example, the objective "O.Output" could be addressed by using FCO_NRO.1 from the catalogue in part 2 of the Common Criteria.

While FCO_NRO.1 can be translated to:

(a) FCO (Name of functional class) Functional Class Communication;

(b) NRO(Name of Functional family): Non Repudiation of Origin;

(c) 1 (Number of functional component within family): "Selective proof of origin".

By selecting this component, the Protection Profile would require any developer to code for all three functional three elements from the catalogue. One example would be for the subsystem "Mileage storage":

FCO_NRO.1.1: The TOE shall be able to generate evidence of origin for transmitted actual mileage at the request of the subsystem mileage display device.

This feature, together with requirements from the functional class FCS (Functional Class cryptographic support) will ensure that the mileage display device can trust the value reported by the mileage storage subsystem and thus a correct value can be presented to the user.

10.4. Security requirements are generally divided into two classes:

(a) Security functional requirements (the best practices) in Common Criteria (ISO/IEC 15408), part 2 offer security functionality like the ability to audit access attempts or the ability to authenticate a user.

(b) Security assurance requirements on the other hand specify the way these functionalities are developed and implemented in the system to ensure that there are no vulnerabilities left.

The common criteria have the assurance requirements grouped in seven Evaluation Assurance Levels (EAL) 1-7, prescribing the development and testing effort and rigor required.

For the mileage fraud Protection Profile a level of 4 should be used, implying a methodical development approach, and white box as well as black box functional testing but without the burden of semiformal or formal development and tests that are required by the higher EAL-Levels.

The protection and resistance of the odometer equipment against manipulation shall be tested in accordance with the defined evaluation procedure for Common Criteria (ISO/IEC 15408) and described in the detailed specification for testing and evaluation procedure, stated in the "Common Methodology For Information Technology Security Evaluation" (CEM, released in ISO/IEC 18045). It defines the test activities and the vulnerability assessment activities among all other details. The evaluation should verify that manipulations are so time effort and cost intensive that they are no longer cost-efficient compared to the higher sales price, risk of mortal danger or environmental perils that can be achieved during the complete lifetime of the vehicle. These test and evaluation methods are internationally accepted and therefore standardized in the ISO document."

II. Justification

1. This proposal aims at supplementing ECE/TRANS/WP.29/GRSG/2015/15 tabled by the expert from Belgium.

2. Mileage fraud causes unexpected faults and may lead to safety risks, e.g. in breakdowns.

3. Mileage fraud undermines the legal requirements for the durability of environmental relevant components[1] and may worsen the environmental performance of vehicles.

4. Mileage fraud causes an annual loss for European consumers of about € 5.6 to € 9.6 billion.[2] The losses for consumers are not only in too high purchase prices for second hand vehicles, but also in higher costs for repair and maintenance. The overall aim of the protection against manipulation is to make odometer fraud economically unattractive during the complete lifetime of the vehicle. Manipulations shall be so time and cost intensive that they are no longer cost-efficient compared to the sales price that can be achieved during the complete lifetime of the vehicle.

5. Mileage Fraud is a cross border issue. Mileage Fraud affects 5 to 12 per cent of used car sales, rising to 30 to 50 per cent for cross border transactions.[2]

6. The approach is to protect the mileage against manipulation by the methodology of common criteria as described in Annex 5 is standardized in ISO 15408. It allows the type approval authorities to check the different manufacturer specific security targets against a single common protection profile. The protection profile for the odometer system has to be defined among stakeholders first. Annex 5 describes the major milestones in the development of the protection profile and should be used as guidance for the experts who develop the protection profile.

---

[1] Regulations (EU) No. 698/2008, Annex 1, paragraph 2.2. and No. 692/2008, Annex VII, paragraphs 1.2. and 1.3.

[2] In twenty-five of the European Union member States, Statistics from the European Commission, "Roadworthiness Package, Impact Assessment", page 17, Brussels, 13 July 2012.