United Nations ECE/TRANS/WP.29/GRSG/2021/11

Economic and Social Council

Distr.: General
29 January 2021

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Working Party on General Safety Provisions

121st session
Geneva, 12-16 April 2021
Item 10 (a) of the provisional agenda
Amendments to Devices against Unauthorized Use, Immobilizers and Vehicle Alarm Systems Regulations
UN Regulation No. 116 (Anti-theft and alarm systems)

Proposal for the 01 series of amendments to UN Regulation No. 116 (Anti-theft and alarm systems)

Submitted by the experts from the GRSG Task Force R116 on Key *

The text reproduced below was prepared by the experts from the GRSG Task Force R116 on Key to replace the OICA proposal GRSG/2020/24. The modifications to the current text of UN Regulation No. 116 are marked in bold characters.

.

* In accordance with the programme of work of the Inland Transport Committee for 2021 as outlined in proposed programme budget for 2021 (A/75/6 (Sect.20), para 20.51), the World Forum will develop, harmonize and update UN Regulations in order to enhance the performance of vehicles. The present document is submitted in conformity with that mandate

I. Proposal

Paragraph 5.1.5., amend to read:

"5.1.5. "*Key*" means any ~~device~~ **mechanical and/or electronic solution** designed and constructed to provide a method of operating a locking system which is designed and constructed to be operated ~~only~~ by that ~~device~~ **mechanical and/or electronic solution**."

Insert new paragraphs 5.1.7. to 5.1.9., to read:

"5.1.7. "*Primary user*" is a user who is able to authorize digital keys. There can be more than one primary users.

5.1.8. "*Digital key*" means a key designed to be transferred to multiple devices by the primary user(s) through dedicated processes.

5.1.9. *"Close proximity"* means a distance of less than [6 m]."

Insert a new paragraph 5.2.16., to read:

"**5.2.16. In addition digital keys shall comply with the provisions of Annex 11.**"

Paragraph 6.1.8., amend to read:

"6.1.8. "*Key*" means any ~~device~~ **mechanical and/or electronic solution** designed and constructed to provide a method of operating a locking system which is designed and constructed to be operated ~~only~~ by that ~~device~~ **mechanical and/or electronic solution**."

Insert new paragraphs 6.1.13. to 6.1.15., to read:

"6.1.13. "*Primary user*" is a user who is able to authorize digital keys. There can be more than one primary users.

6.1.14. "*Digital key*" means a key designed to be transferred to multiple devices by the primary user(s) through dedicated processes.

6.1.15. *"Close proximity"* means a distance of less than [6 m]."

Insert a new paragraph 6.2.10., to read:

"**6.2.10. In addition digital keys shall comply with the provisions of Annex 11.**"

Insert a new paragraph 7.2.7., to read:

"**7.2.7. In addition digital keys shall comply with the provisions of Annex 11.**"

Paragraph 8.1.6., amend to read:

"8.1.6. "*Key*" means any ~~device~~ **mechanical and/or electronic solution** designed and constructed to provide a method of operating a locking system which is designed and constructed to be operated ~~only~~ by that ~~device~~ **mechanical and/or electronic solution**."

Insert new paragraphs 8.1.11. to 8.1.13, to read:

"8.1.11. "*Primary user*" is a user who is able to authorize digital keys. There can be more than one primary users.

8.1.12. "*Digital key*" means a key designed to be transferred to multiple devices by the primary user(s) through dedicated processes.

8.1.13. *"Close proximity"* means a distance of less than [6 m]."

Add a new paragraph 8.2.11., to read:

"**8.2.11. In addition digital keys shall comply with the provisions of Annex 11.**"

Add a new paragraph 13.3. and 13.4., to read:

"13.3. Transitional Provisions applicable to the 01 series of amendments:

13.3.1. **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 UN type approvals under this Regulation as amended by the 01 series of amendments.**

13.3.2. **As from 1 September 2022, Contracting Parties applying this Regulation shall not be obliged to accept UN type approvals to the preceding series (00) of amendments, first issued after 1 September 2022.**

13.3.3. **Until 1 September 2024, Contracting Parties applying this Regulation shall continue to accept UN type approvals to the preceding series (00) of amendments to this Regulation, first issued before 1 September 2022.**

13.3.4. **As from 1 September 2024, Contracting Parties applying this Regulation shall not be obliged to accept type approval issued to the preceding series of amendments to this Regulation.**

13.3.5. **Notwithstanding paragraph and 13.3.4., Contracting Parties applying this Regulation shall continue to accept UN type approvals issued according to a preceding series of amendments to this Regulation, for vehicles which are not affected by the provisions introduced with the 01 series of amendments.**

13.4. **General transitional provisions**

13.4.1. **Contracting Parties applying this UN Regulation may grant type approvals according to any preceding series of amendments to this Regulation.**

13.4.2. **Contracting Parties applying this UN Regulation shall continue to grant extensions of existing approvals to any preceding series of amendments to this Regulation."**

Add a new Annex 11, to read:

"Annex 11

Safety provisions for digital keys

1. **General**

The purpose of this annex is to specify the requirements for documentation and verification for digital keys used to operate the 'device to prevent unauthorized use' and/or the 'alarm system' and/or the 'immobilizer' of the vehicle.

2. **Definitions**

2.1. **"*Authorization process*" means any method to provide the digital key which can operate the 'device to prevent unauthorized use' and/or the 'alarm system' and/or the 'immobilizer' of the vehicle.**

2.2. **"*Revocation process*" means any method to prevent the digital key to operate the 'device to prevent unauthorized use' and/or the 'alarm system' and/or the 'immobilizer' of the vehicle.**

2.3. **"*Boundary of functional operation*" defines the boundaries of the external physical limits (e.g. distance) within which the digital key is able to operate the 'device to prevent unauthorized use' and/or the 'immobilizer' of the vehicle.**

3. **Documentation**

The vehicle manufacturer shall provide the following documentation for type approval:

3.1. **A description of the authorization process.**

3.2. **A description of the revocation process.**

3.3. **A description of the boundary of functional operation.**

3.4. **A description of the safety measures designed within the digital key revocation process to ensure safe operation of the vehicle.**

4. **Requirements for Safe Operation**

4.1. **A digital key shall only be transferred to a device via the authorization process.**

4.2. **There shall be a revocation process.**

4.2.1. **Revocation of a digital key shall not result in an unsafe condition.**

A risk reduction analysis using functional safety standard such as ISO 26262 and safety of the intended functionality standard such as ISO/PAS 21448, which documents the risk to vehicle occupants caused by revocation of a digital key and documents the reduction of risk resulting from implementation of the identified risk mitigation functions or characteristics.

4.2.2. **It shall be possible for the primary user(s) to identify the number of authorized registered digital keys.**

4.3. **Boundary of functional operation for the device to prevent unauthorized use and the immobilizer:**

4.3.1. **Unlocking of the device to prevent unauthorized use shall require that an authorized registered digital key is detected in the interior of the vehicle, or in close proximity of the vehicle.**

4.3.2. **Unsetting of the immobilizer shall require that an authorized registered digital key is detected in the interior of the vehicle, or that an actuation is triggered by user intent in close proximity of the vehicle.**

The limitation of the distance for unsetting of the immobilizer by detection in the interior of the vehicle shall be verified using the following procedure including a tolerance of [1 m /2 m] around the vehicle perimeter:

(a) **The vehicle shall be parked in a secure condition in unobstructed free field condition, this means engine off and all windows, doors and roof shall be closed.**

(b) **The vehicle manufacturer will provide a typical user device for test in agreement with the technical service. The digital key device battery state of charge shall be at maximum.**

(c) **The technical service will define four test points around the vehicle perimeter at a distance greater than [1 m /2 m]. Distance means the distance between the nearest point of the motor vehicle and the user device.**

(d) **The user device is placed at each of the test points. During the attempt to operate the vehicle under its own power, the vehicle door shall be closed. If at one of the test points the vehicle can be operated under its own power, the requirement is not met.**

4.3.3. **The requirements in paragraph 4.3.1. and paragraph 4.3.2. shall not apply during a remote control manoeuvring as defined in UN Regulation No. 79.**

4.4. **Detailed information shall be contained in the owner's manual of the vehicle, or by any other communication means in the vehicle; as a minimum, this information shall include:**

(a) **The method(s) for authorization of the digital key**

(b) **The method(s) for revocation of the digital key**

5. The effectiveness of the system shall not be adversely affected by cyber-attacks, cyber threats and vulnerabilities. The effectiveness of the security measures shall be demonstrated by compliance with UN Regulation No. 155."

6. Verification

Verification of the functionality of the digital key shall be conducted with support of manufacturer's documentation as specified in paragraph 3.

7. Competence of the auditors/assessors
The assessments under this Annex shall only be conducted by auditors/assessors with the technical and administrative knowledge necessary for such purposes. They shall in particular be competent as auditor/assessor for ISO 26262-2018 (Functional Safety - Road Vehicles), and ISO/PAS 21448 (Safety of the Intended Functionality of road vehicles); and shall be able to make the necessary link with cybersecurity aspects in accordance with UN Regulation No 155 and ISO/SAE 21434). This competence should be demonstrated by appropriate qualifications or other equivalent training records."

II. Justification

1. Paragraphs 5.1.5., 6.1.8. and 8.1.6., Clarification on the definition of key: Device was interpreted as being the carrier of the key, calling the key a solution clarifies that the key does not need to be a mechanical device. Multiple devices (multiple key types, multiple solutions) are accepted to operate the same locking systems of the devices in the vehicle today (device to prevent unauthorized use, immobilizer, alarm system), removal of « only » removes the confusion on this point.

2. Paragraphs 5.1.7., 6.1.13. and 8.1.11., adding a definition of "primary user": During the discussion of Task Force Meeting #4 the need for two vehicle users groups evolved. The UN regulation concept does not differentiate other than driver and passengers. With the potential ease of transferring digital keys from one driver to the next, it was requested to differentiate between the vehicle owner, who drives his own vehicle, and a driver, who borrows or rents a vehicle. Example: A rental company may act as a primary users, which can transfer the digital key to a driver renting a vehicle. The rental company does not support that the driver who rents the car can give away the key to additional persons, therefore this driver will not become a primary user, able to authorize digital keys. The addition of a "primary user" reflects the possible existence of multiple levels of user groups.

3. Paragraphs 5.1.8., 6.1.14. and 8.1.12., Adding a definition of digital key: Major differentiator is the possible transfer to multiple devices through a process provided by the vehicle manufacturer. This differentiator is taken as base for the new added definition. It was decided to call this specific electronic solution a "Digital key" to reflect same technology as defined under this term by CCC (Connected Car Consortium).

4. Paragraphs 5.1.9., 6.1.15. and 8.1.13., adding a definition for close proximity.

5. Paragraphs 5.2.16., 6.2.10., 7.2.7. and 8.2.11., includes new additional provisions for digital keys via Annex 11, detailed below.

6. Annex 11 paragraphs 2.1., 3.1. and 4.1.: Digital keys require an authorization process in place.

7. Annex 11 paragraphs 2.2., 3.2., 3.4. and 4.2.: Digital keys require an revocation process in place. Revocation was identified as being the major risk factor for vehicle operation, therefore specific safety measures must be provided to ensure safe operation.

8. Annex 11 paragraphs 4.2.1 and 7. Adding requirements on a standardised method for risk analysis. The text in paragraph 4.2.1 is derived from UN Regulation No. 100 with some changes reflecting the preference to the ISO standards. The text in paragraph 7 is derived from the UN Regulation No. 157.

9. Annex 11 paragraphs 2.3., 3.3. and 4.3: Digital keys require the unlocking of the device to prevent unauthorized use and the unsetting of the immobilizer remote operation to be limited.

The current text of UN Regulation No. 116 does not restrict the range of remote controls. The range of the systems used is depending on the used technology and test condition between 6 m and 11 m.

The proposal aims on three levels of the remote operation distance for digital keys depending of the device to accomplish different use cases:

(a) No limitation for alarm systems, to allow users to use the trunk of their vehicle for parcel delivery service and keep control on the alarm setting. The user is enabled to limit the time window where the alarm of his vehicle is unset such that the delivery can take place.

(b) Annex 11, paragraph 4.3.1.: Limitation of the devices to prevent unauthorized use to close proximity. The main intent of the device to prevent unauthorized use is to prevent from tow away thefts. Therefore a restriction to an area were the user would become aware of someone attempting a tow away is proposed.

(c) Annex 11, paragraph 4.3.2: Limitation of the immobilizer to either the interior of the vehicle for passive start systems (smart start), which require the detection of the authorized digital key prior to start of the engine, or as alternative in close proximity combined with an dedicated activity of user intent on the device used as vehicle key. The set immobilizer prevents to start up the vehicle for driving away. To limit the remote operation for the immobilizer more strictly intents to protect the user from total vehicle theft while standing near the vehicle. The allowance for close proximity is therefore combined with user intent: "User intent" is included to make it clear that conscious activation is required by the user when in close proximity of the vehicle e.g. by (and not limited to) PIN code, QR or barcode, fingerprint scanning.

The field of receiver/antenna are typical circular, while vehicle perimeters tend not to be circular. The signal receiver of the immobilizer will typically be more oriented to the driver’s side, not the passenger side. The electrical fields concerned are not restricted by the materials used in the vehicle body. This results in a technical limitation to exactly match the signal’s limitation to the vehicle interior. Understanding these limitations a test procedure including a tolerance to what is meant by "vehicle interior" and clarifying the conditions of a pass/fail criteria has been added to the passive start system (smart start) use case.

10. Annex 11 Paragraph 4.4: Digital keys require additional information in the vehicle (e.g. owner’s manual).

11. Annex 11 Paragraph 5: Digital keys require compliance with UN Regulation No. 155 on Cyber Security.

12. Paragraphs 13.3. and 13.4.: Addition of transitional provisions in alignment with European General Safety Revision 2 provision for Cyber Security and with the decision of WP.29 at its 182nd session (November 2020)