Submitted by OICA

Informal document **GRSG-121-37**
(121st GRSG, 12-16 April 2021
Agenda item 10(b))

Proposal for a Supplement to UN Regulation No. [161] [new] UN Regulation on uniform provisions concerning the protection of motor vehicles against unauthorized use and the approval of the device against unauthorized use (by mean of a locking system)

Submitted by the Experts of OICA

The text reproduced below is based on the discussions made at the Task Force R116 on key and identifies the changes to be made to ECE/TRANS/WP.29/2021/48 to have the equal level of specification for digital keys as it is proposed from the Task Force for UN Regulation No. 116.

I. Proposal

Paragraph 2.8., amend to read:

"2.8. "*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 2.10. to 2.12., to read:

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

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

2.12. *"Close proximity"* means a distance of less than 6 m."

Insert a new paragraph 5.1.16., to read:

"**5.1.16. In addition digital keys shall comply with the provisions of Annex 8.**"

Add a new Annex 8, to read:

"Annex 8

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' 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' of the vehicle.

2.2. "*Revocation process*" means any method to prevent the digital key to operate the 'device to prevent unauthorized use' 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' 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:**

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. **The requirements in paragraph 4.3.1. shall not apply during a remote control manoeuvring and remote control parking 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. Prior to the finalization of creation of this regulation a task to update UN Regulation No. 116 was started. With this task’s finalization there is a need to align the text of this UN Regulation No. [161].