

Proposal for a new Supplement to the 01 Series of Amendments to UN Regulation No. 62 (Protection against unauthorized use for vehicles of categories L₁ – L₇ fitted with handlebars)

The amendments to the text are in bold for new text and in strikethrough for deleted text.

I. Proposal

Insert new paragraphs 2.6. – 2.9., to read:

- "2.6. **"Key" means any 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 by that mechanical and/or electronic solution.**
- 2.7. **"Primary user" is a user who is able to authorize digital keys. There can be more than one primary users.**
- 2.8. **"Digital key" means a key designed to be transferred to multiple devices by the primary user(s) through dedicated processes.**
- 2.9. **"Close proximity" means a distance of less than 6 m."**

Paragraph 5.11., amend to read:

- "5.11. Electromechanical and electronic devices to prevent unauthorized use
Electromechanical and electronic devices to prevent unauthorized use, where fitted, shall comply with the requirements of paragraphs 5. and 6., mutatis mutandis.
Components that are not embedded in the vehicle (e.g. keys, which are used for activation/deactivation) need not to comply with the test requirements described in paragraphs 5. and 6.
If the technology of the device is such that paragraphs 5. and 6. are not applicable, it shall be verified that care has been taken to preserve safety of the vehicle. The functioning process of these devices shall incorporate secure means to prevent any risk of blocking or accidental dysfunction that could compromise the safety of the vehicle."

Insert a new paragraph 5.13., to read:

- "5.13. **In addition, digital keys shall comply with the provisions of Annex 4."**

Insert a new Annex 4, to read:

- "Annex 4 **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 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, shall be performed.

- 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 21448 (Safety of the Intended Functionality - 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. This proposal for amending UN Regulation No. 62 is aimed at allowing vehicles of categories L₁ – L₇ fitted with handlebars (hereinafter “category L”) to be equipped with a digital key, which has been already permitted under UN Regulation No. 161 for vehicles of categories M₁ and N₁.
2. Relevant requirements established for categories M₁ and N₁ are also appropriate for category L, therefore introduced as-is in this proposal. Following editorial modifications were made for the adaptation.
 - Test requirements are defined in a specific annexe in UN Regulation No. 161. However, as a difference in editorial configuration, they are distributed in more general paragraphs in the case of UN Regulation No. 62. To adequately replicate the intention of the requirement, the wording of reference was recomposed in this proposal.

UN Regulation No. 161

5.3. ...

Components that are not embedded in the vehicle (e.g. keys, which are used for activation/deactivation) need not to comply with the test requirements described in ~~Annex 6~~ paragraphs 5. and 6.

...
 - Reflecting a recent development in the field of ISO, the reference to the standard for the safety of the intended functionality was updated.

UN Regulation No. 161

Annex 9

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 - 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.
3. During the preparation of this proposal, it was identified that the following requirement of the English version of UN Regulation No. 161 states only a subject part, apparently lacking a predicate part. Despite being no doubt in the requirement considering the

context, the predicate part was supplemented in this proposal for full clarity in reference to the corresponding part of its French version, « ... *doit être réalisée* ». In addition, the aforementioned ISO update was also reflected in this sentence.

UN Regulation No. 161

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, **shall be performed.***
