



Economic and Social Council

Distr.: General
26 August 2025

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

197th session

Geneva, 11–14 November 2025

Item 4.7.4 of the provisional agenda

1958 Agreement:

Consideration of draft amendments to existing

UN Regulations submitted by GRSG

Proposal for Supplement 1 to the 01 series of amendments to UN Regulation No. 62 (Protection against Unauthorized Use for Vehicles of Categories L₁ – L₇ Fitted with Handlebars)

Submitted by the Working Party on General Safety Provisions*

The text reproduced below was adopted by the Working Party on General Safety Provisions (GRSG) at its 129th session (ECE/TRANS/WP.29/GRSP/108, paragraph 39). It is based on ECE/TRANS/WP.29/GRSG/2025/2, not amended. It is submitted to the World Forum for Harmonization of Vehicle Regulations (WP.29) and to the Administrative Committee (AC.1) for consideration at their November 2025 sessions.

* In accordance with the programme of work of the Inland Transport Committee for 2025 as outlined in proposed programme budget for 2025 (A/79/6 (Sect. 20), table 20.6), 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.

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.
 - 4.4. 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 fulfilling the technical requirements of UN Regulation No. 155.
 6. Verification

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

The assessments under this Annex shall only be conducted by auditors or 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."
