Submitted by the expert from SAE International

Informal document **GRVA-15-18**
15th GRVA, 23-27 January 2023
Provisional agenda item 5(a)

Proposal for amendments to the interpretation document of UN Regulation No. 155 (Cyber Security and Cyber Security Management System)

Submitted by the experts from SAE International*

The text reproduced below was prepared by the experts from SAE International. It aims at improving the applicability of examples given in Tables A1 and B1 in Annex 5 in UN Regulation No. 155 regarding risks due to spoofing of messages or data received by the vehicle. It is based on informal document GRVA-13-29 and on ECE/TRANS/WP.29/2022/61.

The proposed modification to the interpretation document makes it clear that cryptographic authentication is allowed but not required for authentication of GNSS messages. This is consistent with the approach of the contracting parties, some of whom plan to deploy cryptographic authentication in their GNSS constellations and some of whom have not currently announced plans to do so.

A. Part A

[...]

3. Guidance on the requirements of the Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system (UN Regulation No. 155)

[...]

AB. Paragraph 7.3.4.

"7.3.4. The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.In particular, for type approvals first issued before 1 July 2024 and for each extension thereof, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred

* In accordance with the programme of work of the Inland Transport Committee for 2022 as outlined in proposed programme budget for 2022 (A/76/6 (Sect.20), para 20.76), 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.

to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority."

Explanation of the requirement

The intention of this requirement is to ensure that vehicle manufacturers implement appropriate mitigation measures in accordance with the results of their risk assessment.

The manufacturer should provide reasoned arguments and evidence for the mitigations they have implemented in the design of the vehicle type and why they are sufficient. This may include any assumptions made, for example about external systems that interact with the vehicle.

The technical mitigations from Annex 5, Parts B and C shall be considered wherever applicable to the risks to be mitigated. The Manufacturer may present a rationale not only for a listed mitigation from Annex 5 being "not relevant or not sufficient", but also may present a rationale, that another mitigation other than the ones listed in Annex 5 is appropriate to the respective risk. That rationale may be substantiated by a risk assessment and risk rating showing the appropriateness of the alternative mitigation. This is to allow the adoption of new or improved defensive technologies.

For existing architectures that were developed before the enforcement of UN Regulation No. 155, it may not have been possible to develop the architecture so that all mitigations in Annex 5, part B and C were implemented. Therefore, for approvals first issued before 1 July 2024, other appropriate mitigations for identified cyber security risks are permitted.

Further technical modifications/updates leading to extensions of those existing types after 1 July 2024 should be performed as much as possible in accordance with Annex 5. This should consider the risks and confirm they continue to be managed or reduced. Where there is deviation from Annex 5 this should be explained and rationalised.

For modifications or updates the Technical Service/Approval Authority may confirm that they consider the risks are appropriately managed, including any deviations, and may confirm that extensions can be issued after 1 July 2024 based on the method and criteria published to UNECE, in line with Chapter 5 of UN Regulation No. 155.

The following clarifications should be noted:

(a) The design decisions of the manufacturer should be linked to the risk assessment and risk management strategy. The manufacturer should be able to justify the strategy implemented;

(b) The term "proportionate" should be considered when choosing whether to implement a mitigation and what mitigation should be implemented. If the risk is negligible then it may be argued that a mitigation would not be necessary;

(c) Protection from identified risks means to mitigate the risk.

(d) Referring to row 1 of table B.1 in Annex 5 Part B: The validity of received messages may be carried out by any appropriate means. For example, for V2X, digital signatures might be applied to the message. For example, for GNSS, the technique used might be the Galileo Commercial Authentication Service (CAS) using cryptographic authentication, or technologies such as directionality, dual antennas, signal strength, and consistency of velocity.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(d) ISO/SAE 21434:2021 describes the determination of risk and the deduced cybersecurity goals and cybersecurity concept based on the identified risks. The results are documented in “[WP-09-03] Cybersecurity goals” and “[WP-09-06] Cybersecurity concept”;

(e) BSI PAS 11281: 2018 and other standards regarding claims, arguments and evidence may be used to justify the design decisions of the manufacturer.

The following could be used to evidence the mitigations used:

(f) Evidence that mitigation measures were introduced according to the necessity of measures, this includes:

(i) the reason, if mitigation measures other than Annex 5 Part B and C are applied;

(ii) the reason, if mitigations listed in Annex 5 are not applied;

(iii) the reason, if mitigation measures are determined to be unnecessary.