Transmitted by the expert from OICA

Informal document **GRSG-117-31**
117th GRSG, 08-11 October 2019
Agenda item 13

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

Submitted by the expert from the International Organization of Motor Vehicle Manufacturers

The text reproduced below was prepared by the expert from the International Organization of Motor Vehicle Manufacturers (OICA) to amend the definition of keys taking into account innovative vehicle alarms systems. It is based on the official document GRSG/2019/7, presented at the 116th session of the Working Party on General Safety Provisions (GRSG) (see report ECE/TRANS/WP.29/GRSG/95, para. 48) and on informal document GRSG-115-20, presented at the 115th session of the Working Party on General Safety Provisions (GRSG) (see report ECE/TRANS/WP.29/GRSG/94, para. 49). The modifications to the current text of UN Regulation No. 116 are marked in bold characters for new text, and strikethrough for deleted text.

I. Proposal

Paragraph 5.1.5., amend to read:

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

5.1.5.1. "*Virtual key*" means a key designed as purely electronic solutions and implemented in hardware (e.g. smartphone) and/or software, and which may be provided by another party than the vehicle manufacturer. The electronic solution does not include the hardware / software it is implemented in."

Add new paragraph 5.2.16.:

"**5.2.16. Virtual keys shall comply with the provisions of Annex 11.**"

Paragraph 6.1.8., amend to read:

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

6.1.8.1. "*Virtual key*" means a key designed as purely electronic solutions and implemented in hardware (e.g. smartphone) and/or software, and which may be provided by another party than the vehicle manufacturer. The electronic solution does not include the hardware / software it is implemented in."

Add new paragraph 6.2.11., to read:

"**6.2.11. Virtual keys shall comply with the provisions of Annex 11.**"

Add new paragraph 7.3.6.3.:

"**7.3.6.3. Virtual keys shall comply with the provisions of Annex 11.**"

Paragraph 8.1.6., amend to read:

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

8.1.6.1 "*Virtual key*" means a key designed as purely electronic solutions and implemented in hardware (e.g. smartphone) and/or software, and which may be provided by another party than the vehicle manufacturer. The electronic solution does not include the hardware / software it is implemented in."

Add a new paragraph 8.3.5.1.4., to read:

"**8.3.5.1.4 Virtual keys shall comply with the provisions of Annex 11.**"

Add a new Annex 11, to read:

"Annex 11

Safety provisions for virtual keys

1. General

The purpose of this annex is to specify the requirements for documentation and verification for virtual keys used to operate a device to prevent unauthorized use, to operate an alarm system and/or to operate an immobilizer and for which type approval is being sought.

2. Definitions

2.1. "*User*" means a person who operates a vehicle and is possessing a valid key for the vehicle.

2.2. "*Vehicle owner*" means a natural person or legal party who is the holder of the registration certificate for the vehicle.

2.3. "*Virtual key system*" means the vehicle system that allows virtual keys to operate a locking system.

2.4. "*Authorization*" of a virtual key means that the user can operate the device to prevent unauthorized use, to operate the alarm system and/or to operate the immobilizer of the vehicle with the dedicated virtual key. An authorized virtual key is a valid key.

2.5. "*Deactivation*" of a virtual key means any method to withdraw the authorization from a virtual key. A deactivated virtual key is an invalid key.

2.6. "*Safety concept*" is a description of the safety measures designed within the virtual key system to ensure safe operation of the vehicle.

2.7. "*Boundary of functional operation*" defines the boundaries of the external physical limits (e.g. distance) within which the virtual key is able to operate a device to prevent unauthorized use, to operate an alarm system and/or to operate a immobilizer of the vehicle.

3. Documentation

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

3.1. A description of the virtual key system which gives an explanation of the main function.

3.2. A description of the methods for authorization of the virtual key(s) by the vehicle owner.

3.3. A description of the methods used to provide user with an authorized virtual key.

3.4. A description of the methods used to deactivate a virtual key.

3.5. A description of the boundary of functional operation.

3.6. A safety concept: strategy for safe properties of "the virtual key".

4. Requirements for Safe Operation

It shall be verified that care has been taken to preserve safety of the vehicle. The functioning process of the device to prevent unauthorized use, the alarm system and/or the immobilizer shall incorporate secure means to prevent any risk of blocking or accidental disfunctioning which could compromise road safety. Deactivation of a virtual key shall not result in an unsafe condition.

5. Verification

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

II. Justification

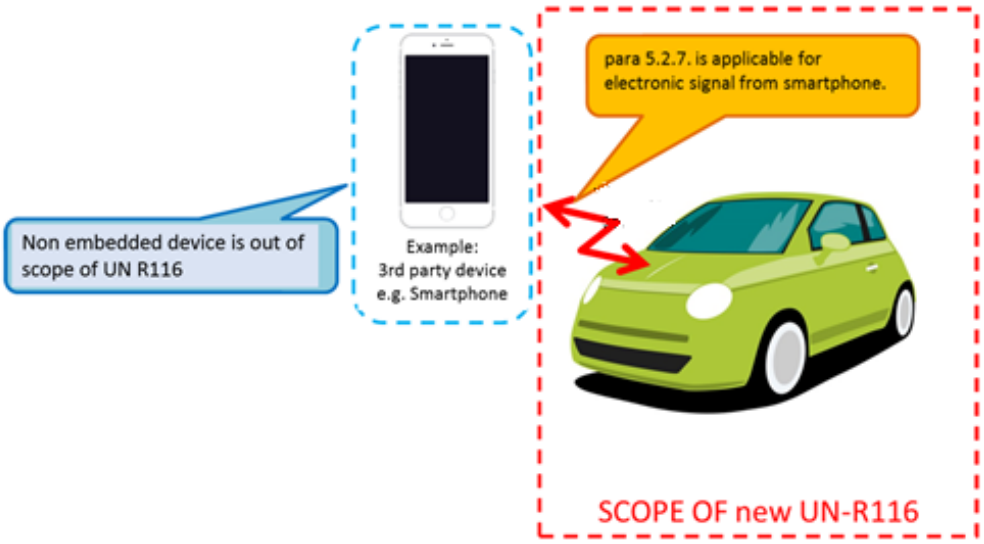
1. At the 106th session of GRSG (May 2014), the expert from the European Commission (EC) informed GRSG about new innovative vehicle alarm systems, such as silent alarm or door-unlocking, using smart phone (GRSG-106-38) and questioned the need to develop an appropriate amendment to UN Regulation No. 116. The topic was further discussed at the 107th session of GRSG (September 2014). The expert from Germany provided the information (GRSG-107-08) that type approval of some of these solutions had been refused because the smart phone signal was considered an additional key, not provided by the vehicle manufacturer, which could potentially interfere with the original alarm system from the manufacturer.

2. However, the key itself is merely an activation device, not a protection device (anti-theft device). Each device of the UN Regulation (device for unauthorized use, alarm system or immobilizer) may have its own key for locking/unlocking. For example, locking and unlocking of the door lock system is not in the scope of UN Regulation No. 116.

3. To access the vehicle, not only physical keys can be used but also purely electronical ones.

4. According to the current definition of "key", a smartphone cannot be covered as "only by that device". This is the reason why "electronic solution" is added to definition. The hardware (e.g. smartphone) and software transmitting the electronic solution to the vehicle are not in the scope of UN Regulation No. 116. If the electronic solution is defined as a key, it is reasonable that the electronic solution transmitted from the hardware fulfils

the requirements of paragraph 5.2.7. (Electrical/electronic locking systems - See figure below).



5. The proposal introduces a distinction between a key as an electronic solution and as hardware and software used to transfer this electronic solution, and amends UN Regulation No. 116 such that new innovative systems are appropriately addressed in the regulation. New innovative systems use components that are not embedded in the vehicle: this means e.g. devices, hardware, operating systems, communication channels, backend servers which are used for setting or unsetting locking systems, by transferring the electronic solution.

6. The proposal clarifies that the electronic solution must fulfil the requirements of UN Regulation No. 116 as being a key, while all hardware and software only used for transferring the electronic solution are not covered by the scope of UN Regulation No. 116. Still according to paragraph 5.4., the manufacturer must ensure the safety of the vehicle.

7. A new subparagraph was added to each key definition (paragraphs 5.1.5, 6.1.8 and 8.1.6) to clearly separate a pure electronic solution ("virtual key") from any key solutions where the hardware used to transmit the electronic solution is provided by the vehicle manufacturer with the vehicle (e.g. Smart key cards). The key definition itself was revised such that it allows in parallel different physical and/or electronic solutions for the device.

8. To each part of the regulation a paragraph (5.2.16, 6.2.10, 7.3.6.3 and 8.3.5.1.4) was added to include specific provisions for virtual keys as defined in new Annex 11.

9. Annex 11 was added including provisions for virtual keys.

As long as a key was a "device" handed over as physical to the vehicle owner, the vehicle owner was in the control of, or aware of:

- how many keys he bears;
- the activity to borrow someone a key;
- the activity to request a key back from someone;
- the transfer of a key when the vehicle is sold;
- the destruction of a key or loss of its function when the battery is down.

These "normal" activities have not been explicitly mentioned in the regulation, due they are bound to a key being a physical device handed over from one person to another person.

The discussions with the expert of Germany in the past months revealed a need to specify similar situations in case when a virtual key have been identified, due to the fact that the activities are not exactly the same in the virtual case, and that those differences are not obvious. Annex 11 is proposing to include:

(1) Authorization management requirements to mirror the transfer of keys between persons. It should be noted that in the traditional world these activities do only include the involved persons (e.g. vehicle owner and vehicle driver or vehicle buyer) and the key device. In the virtual world, all involved persons must in addition identify themselves to the authorization management software which can be proprietary to the vehicle manufacturer or to a third party. This identification and the treatment of the data involved in authorization management of virtual keys must comply with the national regulations of data protection and are not in scope of UN Regulation No 116.

(2) Deactivation of keys is mirroring the request to get a key back from someone, but is not 100% the same function. It opens the possibility to withdraw a key from a person without his acknowledgment. Whether or not this is legal depends on national laws protecting ownership. Nevertheless the proposal requires that the deactivation must be such that no unsafe condition is created.

(3) Boundary of Functional Operation: For the traditional physical key it is 100% clear that the boundary of functional operation is the insertion into the physical locking system of the device. With smart key systems the functional operation is extended to an area around the vehicle. A pure virtual key could in principle be transmitted from everywhere in the world to the vehicle depending on the chosen technology. This includes the possibility that the person operating a device for unauthorized use, an alarm system or an immobilizer may not have the necessary knowledge of the current condition of the vehicle (parked, in operation). The national laws on remote control are currently not harmonized, while some automated functions (e.g. remote parking) require a remote control. Some authorities for example ask for extended boundaries of functional operation under special legal conditions. To remain technology neutral and indeed neutral to national legislations, the boundary in this proposal is not explicitly set but must be such that no unsafe condition is created.

(4) The application of the functions mentioned above may vary according to the regions and the vehicle manufacturers. Therefore, the Annex 11 requires documentation and explanation of the safety concept for the applied functions of the vehicle manufacturer. Verification should be based on use cases derived from this documentation.