# UN Regulation No. 116
PROTECTION AGAINST UNAUTHORIZED USE

# GRSG/Task-Force on KEY DEFINITION

GRSG-121 / April 2021

# Meeting Attendance

➢ 6th Task-force WebMeeting, March 9th
EC, SE, UK, NL, DE, FR, TK, CN, IR, US, OICA, CLEPA

➢ 5th Task-force WebMeeting, December 10th and 16th
NL, DE, UK, FR, IR (10th) NL, DE, FR, CN (16th), OICA, CLEPA

➢ 4th Task-force WebMeeting, November 12th
SE, NL, IR, DE, UK, CN, FR, KR, OICA, CLEPA

➢ 3rd Task-force WebMeeting, 28th September 2020:
EC, NL, UK, DE, FR, JP, KR, CN, IN, OICA, CLEPA

➢ Follow up of 2nd Task-force WebMeeting, 26th June 2020:
EC, UK, DE, OICA, CLEPA

➢ 2nd Task-force WebMeeting, 18th May 2020:
EC, NL, DE, FR, OICA, CLEPA

➢ 1st Task-force F2F, Brussels, 18th Feb. 2020:
EC, NL, UK, DE, FR, OICA, CLEPA

# Agreements within Task-Force 1-3

➢ Name of the new technology: "Digital Key"

➢ Other remote items, not referred to in UN ECE R116, e.g. power window, heating, are out of scope of R116 and out of scope of Task-Force discussions

➢ Risk of Relay attacks. The protocol used for smart device keys does not increase the risk for relay attacks. Not to be addressed with changes for digital key in the Task-Force.

➢ Digital Keys should not be possible to copy a digital key from ones smart device to another smart device (No duplication). The process preventing this is the pairing process. This process is not defined in UN R116 for traditional keys. For Digital Keys the manufacturer will provide documentation how this process works per Annex 11 (Revocation Process).

  • The OEM is responsible that the paired key only works with the vehicle it is paired with. Whether or not the "APP"/Software remains on an device, when the digital key is no longer paired is not OEM responsibility. (Revocation Process)

  • Unsafe smart device. It is possible to un-pair the key from the vehicle. (Revocation Process).

➢ Limitation of Key. The numbers of existing keys is not restricted by UN R116.

➢ Key Codification. Demonstrated by Cyber Security for Digital Key.

# Agreements within Task-Force 4-5

➢ **Definition of the key:**
(1) Definition is based on the difference between Traditional Key and Digital Key: The digital key can be transferred by the authorized user from one device to another.
(2) Digital Keys are a subset of the Keys, as defined in UN R116.

➢ **Cyber Security:**
Reference of UN R155 risk assessment and risk mitigation plan as per outcome of the discussions between the Chairs (GRSG/IWG Cybersecurity)

➢ **Information to Vehicle Owner:**
Requirement that information on Revocation process and Authorization process must be provided to the vehicle owner.

➢ **Limitation of Key:**
A revocation process needs to be in place for digital key. Concept of a primary user was added.

➢ **Area of Operation of the key:**
(1) Differentiation between the different systems.
(2) No limitation for alarm systems.
(3) Limitation for passive deactivation of device against unauthorized use and intended deactivation of immobilizer in close proximity
(4) Limitation for passive deactivation of the immobilizer to the vehicle interior and test protocol with tolerance from vehicle interior

# Agreements within Task-Force 6
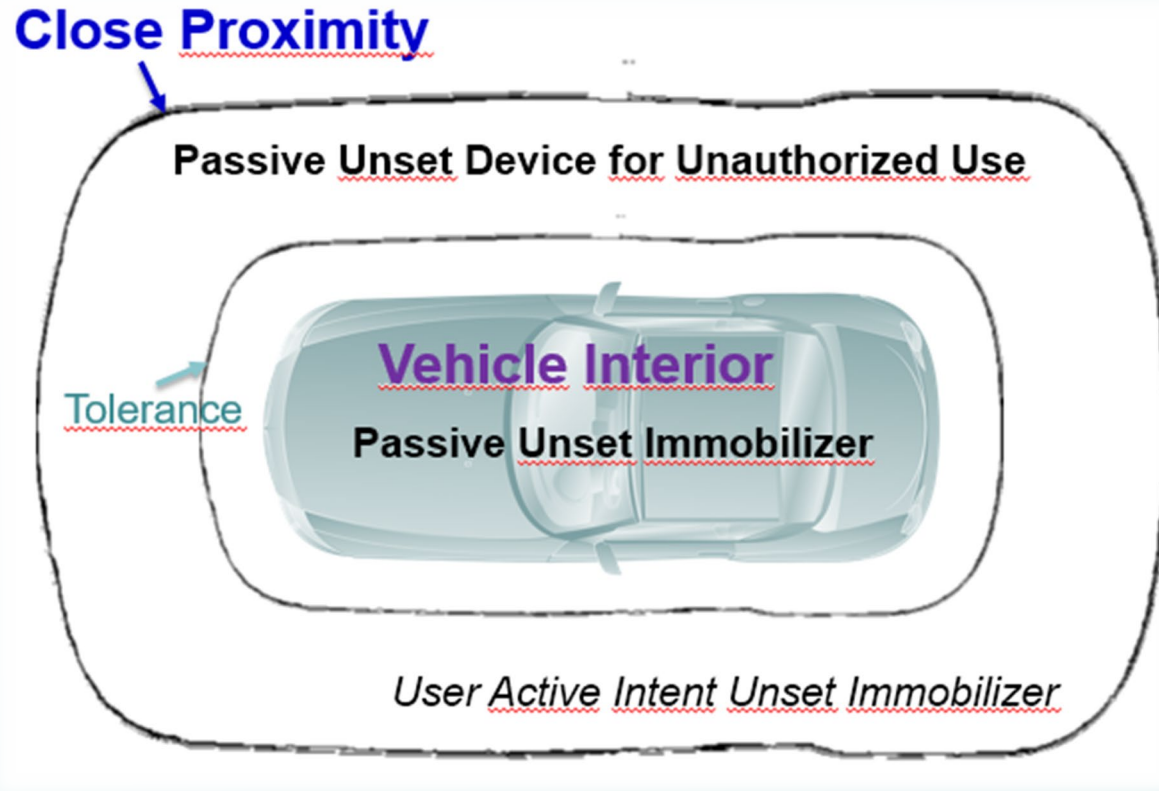


- ➢ Close Proximity = 6 m
- ➢ Corrective Texts
  - ▪ R116Key-06-02
  - ▪ R116Key-06-06
- ➢ Tolerance Vehicle Interior for Test Protocol shall be proposed as = [2000 mm] to GRSG and decided at the GRSG
- ➢ If possible, provide the amendment as a supplement

# GRSG Guidance

(1) Decide on Paragraph 4.3.2:
Tolerance to determine Vehicle Interior [2000 mm],

(2) Decide for Supplement instead of New 01 series,

(3) Adopt Formal Document GRSG/2021/11 as amended by Informal Document and the decision of (1) and (2),

(4) Update of all relevant anti-theft regulations based on the decisions agreed for UN R116 (Working Documents for GRSG-122),

(5) Release the Task Force on Key Definition.

All document to be found on UN [Task force R116 on KEY](#)

# Thank you.