UN ECE Regulation No. 116
GRSG Taskforce on **Key Definition, Session #3**
Web conference on 28 September 2020 (9:00 to 11:00 CET)

DRAFT Minutes

1. Welcome, roll call of attendees

European Commission (EC): Romain LADRET PICIORUS (DG GROW)
Netherlands (NL): Hans LAMMERS (RDW)
United Kingdom (UK): Donald MAC DONALD (DfT)
Germany (DE): Rudolph GERLACH (TÜV), Helge ASMUSSEN, Rania EL ZEIN-KIESOW (KBA),
France (FR): Fabrice HERVELEU (UTAC)
Japan (JP): Ishida HAJIME (JASIC),
China (CN): Lijuan CAO (CATARC)
Korea (KR): Eun Young LEE, Jongsoon LIM (KOTSA),
India (IN): Vishal P.RAWAL (ARAI)

OICA: Alexandra SCHOLZ, Katja JÜRSS, Olivier FONTAINE, Ansgar POTT, Andreas HERGEN, Daniel KNOBLOCH, Tatsuya OTA, Joachim MULLER, Vuthy PHAN, Andreas PERL, Rene NULENS, Rob HARE, Jens SCHENKENBERGER, Michael KNEISSLE, Francesco SIANO, Link BJOERN, Hideki ABE, Toshimitsu YAMAGUCHI, Yves LAGEOT, Benoît MOREAU
CLEPA: Paolo ALBURNO, Simone FALCIONI

2. Adoption of the Agenda

Document: R116KEY-03-01
Agenda is adopted.

3. Adoption of Session #2 draft minutes, revised after follow up session from June 26

Document: R116KEY-02-02-Rev1_Draft minutes revision 1
Minutes are adopted.

4. Actions review

Document: R116KEY-01-02-Rev1_Discussion points
R116Key-03-02_TF116smartkeysVScyber
R116Key-03-03_Proposal-amending-GRSG-2020-24

Discussion starts with definition of key, as improved with last OICA document R116Key-03-03: “digital” key is agreed to be the best wording to address the new concept of smart keys.

Thorough discussion is held to clarify key types, not intended to be delegated to third parties. Netherlands is concerned with effective use of individual smart devices (phones, cards..) not present at time of approval. Known keys already provide electronic code, implemented in dedicated keyfobs. The new concept of digital key introduces a third party in addition to electronic, i.e. cryptographic, code delivered by the vehicle manufacturer. Hence, the solution is not bound to a given hardware. The vehicle manufacturer shall provide a safe and secure backend server, and a third party may provide solutions for connectivity. Decision is to come back to previous “maybe be provided” wording in the key definition.
NL, FR as UK support need for clarification of key types to distinguish pure mechanical or electronic solutions, implemented in a physical dedicated mean, from a digital key.

Improvement proposals are shared, not leading to final agreement(1). Requirement 5.1.5.1. intends to differentiate a solution where only part of the software is delivered from the vehicle manufacturer. As an alternative, key definition may define three key types:

- 5.1.5.1. for pure mechanical key,
- 5.1.5.2. for electronic code in a dedicated keyfob,
- 5.1.5.3. for digital key.

(1) improvement proposal based on WP9/2020/24 document:

"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**. The key is bound to a physical device.
5.1.5.1.	"***DigitalVirtual** key*" **means a key designed as purely as an electronic solution.** This digital key is operated via hardware (e.g. ~~smartphone~~) and/or software, which may be **provided by another party than the vehicle manufacturer. The** digital key **does not include the hardware / software it is implemented i**n. The digital key is not bound to a physical device. "

a. Key codification (R116KEY-02-02 §4.d).

Not addressed during this session.

b. Cyber requirement (R116KEY-02-02 §4.b): IWG cyber security and OTA August 24 meeting output,

Task Force secretariat reports GRVA chair exchange on July 19th (R116Key-03-03). Cyber experts position is that connected accesses are covered within Annex 5 of Regulation 155(2), not identifying other need than proposed WP9/2020/24 requirement 9. (copy-pasted from new ALKS regulation). Common understanding is shared on software update not being an issue.

GRVA Secretary requested assessment of the expected significance of the upcoming cyber security regulation for the envisaged amendments to UN Regulation No. 116 has been delegated to cyber expert, Jens SCHENKENBERGER. DE raises the need to get written statement from IWG CS to GRVA-GRSG chairs: cyber expert shall contact GRVA chair.

(2) http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

c. Operational range versus scenario as park assist (R116KEY-02-02 §4.c),

NL and UK recall strong expectation to improve theft protection, requiring provisions as per functional boundaries. OICA (CLEPA) supports same concern, as already shared during previous sessions, but this Task Force is not intended to address general issues. This would need a dedicated IWG with extended Terms of Reference.

No time left to discuss OICA proposals as per R116Key-03-03.

5. Other

Next meetings shall give more time for discussion (3 hours) and will be confirmed according doodle pool:

- Session #4 between Nov. 2nd – Nov. 12th: https://doodle.com/poll/mb4xq453be5serh3
- Session #5 between Dec. 2nd – Dec. 12th: https://doodle.com/poll/a62uzv6zmxgh8867