GRSG, Task for the definition of Key

Regulation n°116

PROTECTION AGAINST UNAUTHORIZED USE

GRSG call for support

from

GRVA/CS & OTA

to

GRSG/Task-Force on KEY

Background (1)

- **Discussions on smart keys (for e.g. car sharing) were initiated at GRSG beginning 2014,** (see detailed history in document R116KEY-01-06
  1. 2014: EC request to clarify definition of “key”
  2. 2015: further discussions, decisions on whether amendment is needed postponed to 2016
  3. 2018: OICA proposal GRSG-115-20 (updated as GRSG-117-31 in 2019)
  4. 2020: “Task Force R116 on KEY” was officially launched aiming for consolidation of the proposal

     ➔ Cyber security provisions require GRVA support.

- Current text GRSG-117-31-Rev.1 contains **requirements on cyber-security** inspired from new ALKS Regulation:

  “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 compliance with UN Regulation No. 155”

- **Proposed for GRSG adoption at October 2020 session (119th GRSG).**

Background (2)

- **Smart keys** (can be Virtual/Digital) discussions ended in the introduction of explicit requirements for definition and documentation (functional safety): GRSG requested support from the Task Force.

  For example: clarification of the difference between current key and smartphone key:

  1. access services: issuing key or operation authority, authorizing key and vehicle, leave alone the key, lending and borrowing of key, sharing business.
  2. other services: remote thermal comfort, servicing, tracking..

- **Concept of Digital Key:** Discussions until GRSG-117 revealed different understandings on the possible functionalities. The discussions led to the need of clarifying the technical concept of digital key/virtual keys working with smart devices. The task-force refers to CCC (Car Connectivity Consortium, https://carconnectivity.org/) that works on standardization for digital keys for cars, where smart phone devices are used to start vehicles. All material available on UN wiki .

- **GRSG-118,** July 2020:
  - the consolidated working document produced by the “Task Force R116 on KEY” was not commented.
  - GRSG suggested to call for support from GRVA/CS & OTA on the item of Cyber-security.
  - Item of Smart Keys is postponed to GRSG session of October 2020

Call for support (1)

- **GRVA/IWG cyber security & OTA** is called to confirm that "CS/CSMS regulation covers smart keys/applications on phones"

- **Specifically these parts seem relevant**:
  1. Risk assessment, design, testing, monitoring, response.
  2. While all type approval requirements apply, those which may be particularly pertinent relate to suppliers, risks and risk mitigation, testing.

- **Within Annex 5** (List of threats and corresponding mitigations) **all the potential impacts listed in part 4** (Possible attack impacts) look relevant.

Call for support (2)

Preliminary analysis of the possibly relevant threats:

- Item 16.1 calls out remote keys.
- Other risks should also be considered as they may be relevant (references taken from Table A1 of Annex 5):

4.3.1 - back-end servers - all
4.3.2 - communication channels
- 4.1 spoofing
- 6 - all
- 8 - denial of service
- 9 - privilege access
- 10 - viruses

4.3.3. - updates - all
4.3.5 - external connectivity
- 16.1. - remote keys
- 17 - hosted apps
- 26 - crypto used
- 27 - design failures
- 28 - software bugs
- 31 - data transfer