Informal document GRSG-116-40
(116th GRSG, 1-5 April 2019
Agenda item 12.)

UN Regulation No.116

OICA's work summary

- **key testing**, GRSG/2018/25:
  clarification on those 'hand components' not impacting vehicle safety/not subject to 'engine component' testing

- **smart keys**, GRSG-115-20, became GRSG/2019/7:
  discussion on introducing electronic devices, not subject to type approval, robust against any threats

- **regulation split,** summary tracking file with 3 proposals:
  revised documents, to be tabled as working documents for GRSG 117 in October

Regulation No. 116, previous discussion progress

- **key testing**, ECE/TRANS/WP.29/GRSG/2018/25

  Clarification on those ‘hand components’ not subject to ‘engine components’ testing, not impacting vehicle safety.

  - Some Contracting Parties support exiting this item from the split of the regulation

  ➔ if all agree on the fact that these are inappropriate testing (see tracking file – R116 testing explanation sheet), then these testings become a quality issue with OEMs’ experience. Still, external threats are a matter of concern, with answers in the regulation (see forthcoming discussion on smart key).

- **smart keys**, ECE/TRANS/WP.29/GRSG/2019/7

- **regulation split,** 4 documents leading to GRSG-116 informal documents

Regulation No. 116, discussions progress until 1 April 2019

- **key testing**, ECE/TRANS/WP.29/GRSG/2018/25

- **smart keys**, ECE/TRANS/WP.29/GRSG/2019/7

  Discussion on introducing a pure electronic key and wonders on how electronic devices, not subject to type approval, are robust against any threats.

  - D had concerns about
    - introducing a pure electronic key,
    - robustness against any threats..
  - F expect operational safety of such SW-HW are under control by OEM.
  - OICA : this not to be applied in the regulation, but matter of discussions within expert UN WG ; still may be referred to for explanation of vehicle context/specific smart access challenges.

  ➔proposal to address differences between the access solutions with security threats..

- **Regulation split,** 4 documents leading to GRSG-116 informal documents

Regulation No. 116, discussions progress until 1 April 2019

- **key testing**, ECE/TRANS/WP.29/GRSG/2018/25

- **smart keys**, ECE/TRANS/WP.29/GRSG/2019/7

- **regulation split,** 4 documents leading to GRSG-116 informal documents

  Aim is to table official documents at GRSG-117 in October 2019: deadline **12 July 2019 .**

  - Summary presented. EMC should be officially mandated to TF GRE
  - Marking proposal generated discussions: “optimisation proposal seem unnecessary
  - It may come to a simplification (see next slide)

  ➔exchanges on identified issues (EMC, marking) ; no further comments

Regulation No. 116, GRSG-116

Outcomes of meeting April 1st

- **key testing**, GRSG/2018/25
  - Ready for adoption

- **smart keys**, GRSG-115-20 became GRSG/2019/7
  - Further discussions still needed to clarify scope of UN R116
  - See next 3 slides: state of play on access issues, threats and mitigation measures.

  ➔ **Aim of 1 April meeting: Collecting CPs' views**

- **regulation split**, exchanges on identified issues ; further comments on GRSG-116-06 (Locks), -07 (Immobilizers) and -08 (Alarms) and their justifications per GRSG-116-09 (tracking list) :
  - Recall of basic principle: pure splitting of UN R116 (no new issues)
  - Call for a GRSG's mandate to GRE TF-EMC on EMC annex
  - J to provide position on marking issue
  - "Mechanical key" annex: to be removed from draft regulation on Locks

  ➔ **Aim of 1 April meeting: collecting comments aiming final adoption at GRSG-117 (October 2019)**

Regulation No. 116, GRSG-116

Outcomes of meeting April 1st

- **smart keys**, GRSG-115-20 became GRSG/2019/7 (**key testing**, ECE/TRANS/WP.29/GRSG/2018/25)
  - Open discussion on key testing shifted to ‘smart key’ and ‘reg. Split’.
  - Further discussion needed to clarify scope of R116 and further requirements to tackle experienced and new access threats (incl. cyber)
  - OICA’s presentation on active status of access issues, threats and measures

  ➔ Aim is to gain CPs’ position.

OICA: R116 meeting material

Clarification of the difference between current key and smartphone key

- **access services:**

  issuing key or operation authority, authorizing key and vehicle, leave alone the key, lending and borrowing of key, sharing business

- **other services:** remote thermal comfort, servicing, tracking..

Regulation No. 116, GRSG-116

Outcomes of meeting April 1st

- **Clarification between current key** (including short range remote electronic code) **and smartphone key:** how to use, risk, countermeasure.. leading to clarification on new devices/services
  - **user access services:** Issuing key, Authorizing key and vehicle, Leave alone the key, Lending and Borrowing of key, Sharing business

focus of our discussion

	Current key	Smartphone key	Other.. biometric identification
Access services Issuing -Authorizing - Sharing	Mechanical/hand free access commands	Smartphone, watch, other..	Fingerprint, eyeprint..
Risk	Unauthorized copy (tap mismatch..), relay attack, (no safe sharing business)	Complex protocol (tap transmitted info) Hacking	Consumer integrity (no car sharing)
Countermeasure	Safe protocol + consumer recommendation.	**Safer** protocol + consumer recommendation (multiplayer cross-verified security)	Consumer recommendation
Proof	None	OEM ensure the safety in use; may submit declaration.	No
Regulation requirement	Low level (protection level as per 5.2.7.: at least 50,000 variants and shall incorporate a rolling code and/or have a minimum scan time of ten days	If the specific requirement is amended, the new theft method will be created.	Not compliant to 5.2.7. ⇩ **need for amendment**

  - **other services:** remote thermal comfort, servicing, tracking (inc. e.g. remote engine control)..

- **rational:** Of course each OEM has to ensure the security for the feature of smartphone key, but it is not feasible that technical service inspect whether this verification is proper or not. Making requirement is not feasible either, as guideline to unauthorized used !

  If any requirement is necessary, it could be only, “The manufacturer shall ensure the safety in use” or “The manufacturer shall ensure the safety in use and submit declaration”.

Regulation No. 116, GRSG-116

Outcomes of meeting April 1st

- **Clarification between current key** (including short range remote electronic code) **and smartphone key**

It is fair to say that there is no reason to block the R116 discussion for smartphone access systems for reasons of Cyber Security. UN ECE has a Resolution in place and is developing an updated UN ECE measure in form of a UN-R, UN GTR or Guideline.

1. Smartphone access is a new issue that connects the vehicle to the outside environment but there exist other connectivity applications already in the vehicle for which there are no specific Cyber Security requirements (Blue tooth connection, Multi-media screens and related applications as Apple car play, android, emergency call, …).
   ➔ today it is left up to the individual OEM to ensure the CS for its vehicle and customer

2. UN ECE already issued a Cyber Security guideline for connected vehicles as part of R.E.3 (Annex 6). This is what contracting Parties today expect from OEM's on a voluntary basis. We don't see a reason why R116 related application would have to be treated differently in view of Cyber Security from other connectivity application on the vehicle.

3. UN ECE is in the process of establishing a draft Regulation on Cyber Security. This draft regulation may be adopted as a regulation under the 1958 agreement, 1998 agreement or as new guideline. The decision will be taken at GRVA and WP.29 and whatever is the outcome it will set the next step for managing Cyber Security in UN ECE. Again we see no reason why R116 related applications would have to deviate from this direction by specific Cyber Security requirements within R116.

TF CS/OTA mitigation recommendations: ECE/TRANS/WP.29/GRVA/2019/2, where:
➔ it shall cover all thinkable threats/mitigations to be considered for smartphone accesses risks (table B.5.16),
➔ it still will have to be revised and updated according news and experience..

TF CS/OTA test phase GRVA-02-03

Regulation No. 116, GRSG-116

Outcomes of meeting April 1st

- **regulation split**: exchanges on identified issues (marking, EMC) ; further comments on last amended documents and justifications tabled

	New draft regulations	Justifications for modifications to original UN ECE n°116 regulation relevant parts	Major issues
LOCK, antitheft devices	GRSG-116-06	GRSG-116-09	Marking a single component for multiple regulations (not including RF), leading to proposal: see next slide
IMMOBILIZER,	GRSG-116-07		
ALARM,	GRSG-116-08		
Proposal for EMC annex update	*Already considered along OICA EMC TF: ongoing proposal to be shared at GRE level.*		Updating EMC standard references, simplifying and clarifying testing (immunity)
Summary sheet	GRSG-116-XX based on *final_Regulation_116.pptx*		

Detailed review of tracking list, any open/new issues ?

➔ See next slide on EMC and marking

➔ Discussion on further improvments for October updated Working Documents,

➔ Discussion on further needs.

Regulation No. 116, GRSG-116

Outcomes of meeting April 1st

- **regulation split**: exchanges on identified issues (marking, EMC), extract from summary sheet:
  - **EMC:**
    a. Proposal for annex 9 update (first PSA proposal shared on OICA TF, February 22nd) ; may be more than editorial (including removing IEC) and will need further expert discussion within GRE TF (next 17th session on March 4th): need for an official mandate from GRSG to GRE, TF EMC to be delivered at least as informal for GRSG-117, October 2019.
    b. Shall lead to R10 amendment proposal for clarification of (high frequency) immunity test.

  - **marking:** Reference is given in requirement 4.5 not to repeat  marking. If necessary, it may lead to following proposals (not included in ongoing split proposals):
    a. Proposal for unique approval mark, requirement 4.8: applicant shall provide information and document for a single mark.

    In the case of a component approved separately as an immobilizer, the approval mark shall be affixed by the manufacturer to the major element(s) of the device. In the case of a component approved as an immobilizer under this regulation and an alarm system under UN Regulation No. **XXX and/or a [locking system] under UN Regulation No.YYY, ~~both approval marks~~** ~~shall be affixed by the manufacturer to the major element(s) of the device~~ **the applicant may provide through the communication form the approval mark affixed by the manufacturer to the major element(s) of the device stating that this component also complies to Regulation XXX and/or Regulation YYY.**

    b. Proposal for adding approval mark tracking in the communication form, e.g. annex 2a:

    1.6.1 Approval or Extension No. of approval mark origin:

    with details added in the information form, e.g. annex 1a

    1.5.1 Origin of the ECE approval mark:

Regulation No. 116, GRSG-116

Outcomes of meeting April 1st

Conclusion:

1. Smart key solution is welcomed as it could be a safer access solution to the devices to protect against unauthorised used of the vehicle, without need of amending UN R116 (OEM shall ensure cyber-safe design thanks to the cyber security requirements (work is ongoing).
2. Regulation split needs
   a. EMC Annex: Support from GRE for update under GRSG mandate
   b. Markings: Simplified provisions
   c. “Mechanical key” Annex: to be removed from GRSG-116-06 as not initialy addressing Locks in UN R116 ;

➔ Last call for comments by end of May 2019, aiming official documents for adoption at GRSG-117, October 2019.

Request for guidance

Guidance requested from GRSG-116 :

is there a need for a regulation 116 Task Force (with CP's lead) ?

➔ Need for new definitions for keys (including new electronic solutions) ?

➔ Need for new regulation (e.g. on tracking, remote engine control, others) ?

➔ Need for further practical work (at GRVA-CS/OTA - including testing) ?

Informal discussions attendees

25/2/2019 - 5/3/2019 web exchanges:
Germany: helge.asmussen@kba.de
France: fabrice.herveleu@utacceram.com
OICA:
alexandra.scholz@opel-vauxhall.com
ofontaine@oica.net
uwe.topple@vda.de
benoit.job@honda-eu.com
katja.jurss@volvocars.com
rene.nulens@toyota-europe.com
vuthy.phan@renault.com
andreas.hergen@bmw;
gerald.koch@volkswagen.de
thomas.s.weiss@daimler.com
benoit.moreau@mpsa.com

1/4/2019 – GRSG pre-meeting:
Germany: helge.asmussen@kba.de
gerlach@de.tuv.com
Japan: s-morita@jasic.org
minoura@jasic.org
n-tanaka@ntsel.go.jp
ka-koba@shinsa.ntsel.go.jp
Koichi_Kamiji@n.t.rd.honda.co.jp
a-hirao@mail.nissan.co.jp
OICA: alexandra.scholz@opel-vauxhall.com
ofontaine@oica.net
benoit.job@honda-eu.com
katja.jurss@volvocars.com
rene.nulens@toyota-europe.com
vuthy.phan@renault.com,
michael.kneissle@daimler.com
benoit.moreau@mpsa.com