RENAULT NISSAN MITSUBISHI

Consultation on Delegated Act regarding C-ITS

Stakeholder Meeting February 9th 2018

09/02/2018

1. Establish common rules to ensure security of C-ITS communications
2. Ensure the practical application of the General Data Protection Regulation in the area of C-ITS
3. Ensure a forward looking hybrid communication approach
4. Establish common rules on interoperability and compliance assessment
5. Clearly define a set of priority C-ITS services to ensure continuity of C-ITS services

1. Establish common rules to ensure security of C-ITS communications

- The European C-ITS Security Policy shall be sufficiently open to adapt to these future European and International Cyber Security frameworks:
  - Regulation of the European Parliament and of the Council regarding the Information and Communication Technology cybersecurity certification ("Cybersecurity Act‘’)
  - Cyber-security norm ISO 21 434

- CC level EAL4+ might be acceptable for HSM but the security level for the gateway shall be reevaluated

➔ The final Security Policy shall not anticipate any constraint that might conduct to several different references of certification schemes that might not converge and impose contradictory processes and deployments.

➔ Early deployment shall not be subject of any upgrade requirements (ex. retrofitting on already deployed equipment’s) once the European wide converged solution for further C-ITS deployment is available.

2. Ensure the practical application of the GDPR in the area of C-ITS

- Sector-specific regulation should be established in **concertation with all stakeholders** and should aim at establishing a level-playing between all stakeholders of the C-ITS eco-system; specific DPIA methodology shall be applied EU-wide and shared by all stakeholders.

- Strong support of a **roadmap for lawful processing of personal data** used for C-ITS that would give **legal certainty** to operators in the deployment process for C-ITS.

- Any legal bases should always **cover all types of C-ITS services: Day 1 and beyond**.

- The methodology and **frequency of certificate issuance shall be harmonized at EU level** and kept at a best optimized level between privacy and cyber security requirements.

- **Switching off the device or any dynamic configuration would put road safety at risk.** That is why users should only be allowed to personalize their data protection settings with the exception of data used for road safety applications, which would be covered by the legal ground “public interest”.

- Road transportation should not be more restricted than urban rail or inland waterway transport when it comes to preventing accidents.

3. Ensure a forward looking hybrid communication approach

- Concept of « forward looking » is not clear yet. However, the functional and technical architecture shall take into consideration the **results of the feasibility study for coexistences DSCR / LTE-V2X / CBTC** as required by the CEPT mandate.
- In any cases, futures needs for redundancy and/or capacity increase of connectivity means for automated driving shall be evaluated.

4. Establish common rules on interoperability and compliance assessment

- Interoperability & Backwards compatibility & European wide harmonization are key factors!
- Compliance Assessment should consider **self certifications based on common rules.**

5. Clearly define a set of priority C-ITS services to ensure continuity of C-ITS services

- Priority C-ITS services should be based on **realistically achievable and harmonized deployments** in the Member states to allow the same level of quality to our customers.
- In order to preserve scarce spectrum resources, **all use cases related to road safety services – especially those with latency criticality** - shall be considered as priority.