Cybersecurity and data protection – Part A) Focus areas for presentation at the IG ITS/AD meeting in November 2015 Part B) Issues for discussion Part C) Preliminary Draft proposal for Guidelines on measures ensuring cybersecurity and data protection of connected vehicles and vehicles with automated driving technologies (ADT)

Part A)

I. Focus areas from the perspective of the German Government's on automated and connected driving

The digitalization of mobility and the associated increase in the amount of data are creating new requirements to be met by vehicle safety and infrastructure and the protection of personal rights. Automated and connected driving systems thus require clear cybersecurity standards and data protection requirements.

Automated and connected driving systems are under the obligation to perform their functions safely and reliably across national borders. The rights to individual mobility data have to be regulated clearly.

The objective of the German Government is to ensure that vehicles are protected from external interference and manipulation. And the principles of general data privacy law apply to data protection.

II. Focus areas from the perspective of G7 transport minsters

Regarding cybersecurity and data protection it is stated in the declaration of the G7 Ministers of Transport and the European Commissioner for Transport on 17th of September 2015 (see Annex):

"With regard to automated driving … ensuring data protection and cybersecurity are of outstanding significance and will require sustained cooperation among the G7 transport ministers and the European Commissioner for Transport."

Part B)

Issues for discussion

1. The use of the clear definitions should be provided for the outline of Work item 7.

2. Evaluation of focal points by IG-ITS-AD

3. Preparation of guidelines for cybersecurity and data protection as a short-term measure.

4. At the conference of G7 transport ministers in September 2015 it was agreed to establish a working group for the coordination of the most crucial issues concerning automated driving. The IG-ITS-AD should consider the results of this working group (in particular on on cybersecurity and data protection).

5. These results are expected to be available in September 2016 and should be utilized by IG-ITS-AD for further activities in developing globally harmonized specifications.

Part C)

Preliminary draft proposal for Guidelines on measures ensuring cybersecurity and data protection of connected vehicles and vehicles with automated driving technologies (ADT)

Preamble

The digitalisation of mobility and the associated increase in the amount of data are creating new requirements to be met by vehicle safety and infrastructure and the protection of the rights and freedoms of data subjects.

Automated and connected driving systems thus require clear cybersecurity standards and data protection rules. It has to be ensured that vehicles are protected from external interference and manipulation.

The guideline is intended to present requirements to manufacturers for systems to be installed in vehicles to provide a high level of cybersecurity and to ensure data protection. If a manufacturer fails to comply with the requirements of the guidelines, they must guarantee security in a similar manner.

This guideline is intended as interim guidance until the completion of on-going research and collaboration activities and the development of more detailed globally harmonized specifications on cyber-security and data protection.

Scope

This guideline addresses the measures for connected vehicles and vehicles with automated driving technologies (ADT) with regard to cybersecurity and data protection.

Measures for cybersecurity and data protection shall include hardware and software.

1. Definitions

1.1 Connected vehicle is a vehicle with a device installed designed to allow a wireless connection or communication with external devices, cars, networks or services.

1.2 ADT – Automated Driving Technologies – *definition to be added after agreement in IG-ITS-AD*

1.3 Cybersecurity – means preservation of confidentiality, integrity and availability of information in the Cyberspace, i.e. the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

1.5 Data protection - means a natural person's right to respect for his or her private and family life, home and communications with regard to the processing of personal data.

1.6 Privacy by design - means a controller's obligation to implement technical and organisational measures appropriate to the controller's processing activity which are designed to implement data protection principles with the aim of protecting the rights of data subjects by reducing the likelihood and severity of the risk for his or her private and family life, home and communications.

1.7 Privacy by default - means a controller's obligation to implement technical and organisational measures which ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

2. Requirements

Connected vehicles and vehicles with ADT are intended to be fitted with measures ensuring cybersecurity and data protection and shall fullfill the requirements set forth below.

- Everyone's right to his or her private and family life, home and communications has to be respected.

- Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

- The principle of fair and transparent processing of personal data means in particular
  - respecting the identity and privacy of the data subject,
  - not discriminating against data subjects based on their personal data,
  - paying attention to the reasonable expectations of the data subjects with regard to the transparency and context of the data processing,
  - maintaining the integrity and trustworthiness of information technology systems and in particular not secretly manipulating data processing,
  - taking into account the benefit of data processing depending on free flow of data, communication and innovation, as far as data subjects have to respect the processing of personal data with regard to the overriding general public interest.
- The manufacturer, supplier [and service provider] shall take into account the degree of risk for the right and freedoms of individuals.
- To minimize the risks for the data subject's privacy the means of anyonymization and pseudonymization techniques shall be used.
- Data subjects (e.g. vehicle owners or drivers) shall be provided with comprehensive information as to what data are collected and processed in the deployment of automated and connected driving systems, for what purposes and by whom. Data subjects shall give their consent to the collection and processing of their data on an informed and voluntary basis.
- The collection and processing of personal data shall be limited to data that is relevant in the context of collection and processing and any such data shall be obtained by lawful and fair means, and where appropriate, with the information and consent of the data subject. If applicable, the data subject shall have the right to withdraw his or her consent if it involves functions that are not necessary for the operation of their vehicle or for road safety.
- In addition, automotive manufacturers and component suppliers [and service providers] shall, both at the time of the determination of the means for processing and at the time of the processing, implement appropriate technical and organizational measures and procedures to ensure that the data subject's privacy is respected. The design of data processing systems installed in vehicles such shall be data protection friendly, i.e. taking data protection and cybersecurity aspects into account when planning the components ("privacy by design") as well as designing the basic factory settings accordingly ("privacy by default").
- Connected vehicles and vehicles with ADT shall be equipped with measures for cybersecurity taking into account the latest national and international standards.

- Automotive manufacturers and component suppliers [and service providers] must ensure that there is adequate protection against manipulation and misuse both of the technical structure and of the data and processes.

- As the automation and interconnectivity of driving functions increases, the issues of data encryption and cybersecurity will become more important. To prevent non-authorized access to vehicles, automotive manufacturers and component suppliers [and service providers] shall ensure the secure encryption of data and communications by the use of state-of-the-art information and communication technologies

- In addition, UNECE Regulation No 116 shall be supplement by mandatory security-related requirements for the approval of automated and connected driving systems for road traffic.

- As there will be no longer safety without security, e.g. ISO 26262 which establishes standards for the functional safety of critical electric and electronic components or systems in vehicles shall be reflected in the light of security-related requirements for safe automated and connected driving systems for road traffic.

- The connection and communication of connected vehicles shall be separated from internal devices and systems generating internal information necessary for the control of the vehicle with appropriate measures. Connected vehicles and vehicles with ADT shall be equipped with measures to ensure a safe mode in case of system malfunction, e.g. by redundancy in the system.
