WORKING GROUP 6: Cybersecurity and access to in-vehicle data linked to connected and automated mobility

Motivation

Connected and automated vehicles are generating, storing and using increasing quantities of data. At the same time, wireless connectivity is making it easier to share these data with various actors. The use of these data has potential to change existing business models (e.g. roadside assistance, vehicle insurance, vehicle repair, car rental, etc.) and lead to the development of new services and products. While various market players are competing for such data, there is still no data governance model that is widely accepted across stakeholders.

The opportunities enabled by vehicle connectivity and access to in-vehicle data also bring new threats of cyber-attacks, such as taking remote control of the vehicle. Currently, at the EU level, there are no cybersecurity rules specific to connected vehicles (however, works at the UN level are underway). Without adequate protection, the connected vehicles and their ecosystem (e.g. road side units, data centres for vehicle data) may be exposed to cyber-attacks that can bring vulnerabilities in the system and severely impact the safety and the privacy of their owners and users, as well as other individuals.

Scope

This working group will focus on how testing and pre-deployment activities can be used to, without prejudice to regulatory activities, in particular in the field of vehicle type approval and ITS to:

- Identify best practices to ensure security of smart driverless vehicles against cyber threats for car manufacturers and other actors of the smart mobility ecosystem by taking into account the vulnerabilities and technology robustness level of partially or/and fully automated and connected systems, as well as procedures for reporting cyber incidents
- Identify how access to, and exchange of, vehicle and infrastructure data may be facilitated through testing and pre-deployment activities
- To find a common understanding for addressing technical and legal issues that are relevant for the access, transfer, sharing, use and storage of data, including the use of data by artificial intelligence solutions

The group will also promote collaboration between the various actors (e.g. public authorities, traffic managers etc.) to ensure high quality standards and accuracy of data in line with the Regulation on Free flow of Non-personal Data.