

Why we need an eSecurity Working Group?

- Acceptance of electronic systems
- No Safety without Security

Proposed Draft Terms of Reference of a Working Group on: "eSecurity" Technologies

What is the objective of the group?

Investigate eSecurity needs, which address the vulnerability of Road Transport introduced by the misuse of networked and co-operative systems, integrate existing and emerging RTD initiatives and provide a communication platform of all major stakeholders in order to support the introduction of eSecurity technologies in parallel to the technical progress and compatible to legal and certification aspects. Derived from a profound threat and attack scenario qualified recommendations need to be developed regarding the technology requirements (networks, architecture, systems & components and their interaction), which are complemented by advise regarding the legal provisions and standardisation needs for implementation. The WG will disseminate its findings through the well established eSafety communication strategy and will support the work of respective eSecurity RTD projects. Since industry (OEM:s and suppliers), network operators, public authorities, service providers and researchers have to join forces the efficient interaction of all stakeholders is paramount.

Initial topics comprise:

- ☞ **Protection against unauthorised mobile remote access and wired access on networked vehicles including the full electronic system and its components and data against manipulation and subsequent misuse (e.g. wired & tele- data / software transfer)**
- ☞ **Protection of electronic motor vehicle components against e-assaults (e.g. viruses, trojans, spy-ware, spam, etc.) and of digital data stored in the motor vehicle and road infrastructure against unauthorised access and manipulation**
- ☞ **Protection of motor vehicles, fleets and road infrastructure by securing telematics and co-operative system applications**
- ☞ **Establishment of the legal requirement catalogue on necessities in MS and European legislation, certification, and inspection procedures next to the eSecurity Standards survey**

Who should be in the group?

About 10 – 15 persons representing all stakeholders Automotive Manufacturers and Suppliers, Telecom Operators and Service Providers, Authorities and Road Operators, Research Establishments and Academia