

## eSecurity Working Group

The development, deployment and use of intelligent vehicle systems contributing to road safety assumes a large-scale technology infrastructure for communication and co-operation. However, road transport could be made vulnerable by the accidental or malicious misuse of this very infrastructure. The eSecurity Working Group joins European stakeholders to discuss these vulnerability aspects and agree on concerted measures.

### Objectives

- Investigate security needs that address the vulnerability of road transport caused by the misuse of networked and co-operative systems
- Integrate existing and emerging RTD initiatives in order to
  - support the introduction of security technologies in parallel to the progress of the technology infrastructure
  - ensure compatibility to legal and certification aspects
- Provide qualified recommendations regarding technology requirements (networks, architecture, systems & components and their interaction), standardisation needs and legal provisions

### Main Achievements and Challenges

The WG, which started in April 2007, has agreed on the following activities:

- State of the art
- Stakeholders and possible misusers
- Misuse cases (or threats) and risk analysis
- Security requirements
- Organisation requirements
- Measures for quality assurance and responsibilities
- Research requirements
- Conclusions

### Future activities

- Next meeting: 16 October 2007 in Brussels
- Internal draft version of recommendation document (April 2008)

### Intended Stakeholders

- Industry stakeholders (OEMs and suppliers)
- Network operators
- Public authorities
- Service providers and researchers

OEM and public authority participation is critical to discuss organisational requirements and the measures for quality assurance and responsibilities.

### Co-chairs

Christoph Ruland, University of Siegen  
Antonio Kung, TRIALOG

christoph.ruland@uni-siegen.de  
antonio.kung@trialog.com