i2010
Intelligent Car Initiative

Safety

eSecurity WG

Antonio Kung. Trialog
Univ.-Prof. Dr. Christoph Ruland. University of Siegen
Co-chairs

European Commission
Information Society and Media

Motivation

- Support of the reliability of eSafety
- Protection of eSafety functions
- Prevention of critical road safety effects which result from electronic vehicle systems
- Preventing of misuse or malpractice, including **privacy infringement**
- Establishment of new R&D fields
- Providing of recommendations, code of practice, standardisation
- Transparency of implemented safety and security functions
- New fields of business (See “Terms of Reference”)

Focus of Working Group

- **Focus 1**: Data protection
  - Impact of eSafety (applications) and telematic services onto security (data protection, article 29 aspects, etc.).
- **Focus 2**: Intrusion
  - Impact of security onto eSafety (hardware and software security, attacks, manipulations, DoS, in car communication, car-to-car, car-to infrastructure, etc).

Activity A1: State of the Art

- Definition of terms
- Control instruments
- Legal situation in different countries
  - EU
  - Non EU
- Liberalization
- Comparison to WELMEC

Activity A2: Roles of partners in eSecurity business (= possible attackers)

- Development phase
  - Hardware- and software developer
- Production phase
  - Manufacturer
- Operating phase
  - dealer, Owner, User, anybody
- Maintenance phase
  - Authorized garage, Brand own, Non brand own
  - Unauthorized garage
- De-Installation phase
  - Re-Installation

Activity A3: Threats

- Manipulation of hardware or software
- Location tracking
- Implementation trapdoors and trojan horses
- Denial of service
- Unauthorized access
- Unauthorized commands
- Unintended risks, for example by interferences on the communication system, failures of CAN gateway, overload of CAN gateway by entertainment system
- Levels of threats
- Levels of damages

Activity A4: Security requirements

- Data integrity
  - Recognition of modifications (when and by whom?)
  - Prevention of modifications
- Authentication of origin of commands, software, etc.
- Revocable anonymity
- Access control
- Authorization system
- Strong Firewalls between communication system used by eSafety functions and all other communication systems
- Secure software download
- Priorities of measures
- Monitoring, Logbook
- Policy configuration
- Security strength update

Activity A5: Organizational Requirements

- Security Infrastructure
- Security management

Activity A6: Regulation requirements

- Recommendations for manufacturers
- Approval administration
- Regulation and approval of software
- TÜV – on the spot instead of periodic
- Import of vehicles
- …

Activity A7: Research requirements

- Secure Car Communication System
- Car Communication Firewall
- RFIDs in cars for manipulation detection
- Digital Signatures in InCar-, Car-to-Car, and Car-to-Infrastructure Communication
- Data protection mechanisms

Activity A8: Results

- Input for the European Commission
  - Recommendations
  - code of practice
  - recommendations for standardisation
  - establishment of R&D fields and coordination
- Reporting and support to the eSafety Steering Group feasibility and cost studies
- Aspects of type approval and control

Time Table to be Discussed

- April 2007
  - Setting work working group and working process, creation of template document
  - **April 20th, 2007 : 1st meeting**
- Focus 1
  - May 2007 : A1, A2, A3
  - June 2007: A3, A4, A5
  - September 2007 A7, A8
  - October 2007 F1 Review of recommendation document
- Focus 2
  - November 2007 A1, A2, A3
  - December 2007-January 2008 A3, A4, A5
  - February 2008 A7, A8
  - March 2008 : Review of recommendation document

E-Mail from Article 29

I would like to thank you for inviting us to participate in the eSecurity working group which is a part of the eSafety Forum.

As I have already outlined during the In-vehicle telematics workshop, **it is very important to take data protection and privacy issues into consideration from the very beginning, therefore, we welcome your invite**.

Furthermore, I would like to kindly ask you whether you could also address a **more concrete invitation to the Article 29 Working Party**. As our unit is the secretariat of the WP, it would be sufficient to address it to the Secretariat of the Art 29 WP using our contact details and we will promptly inform the members. Should you have any questions or comments, please, do not hesitate to contact us directly.

Thank you.
Kind regards,
Hana Pechackova
Desk Officer, Legal Affairs and Policy
European Commission
Directorate General Justice, Freedom and Security
C 5 Data Protection Unit
46 Rue du Luxembourg
1000 Brussels