

Secure Vehicle Communication



Security Solutions for eSafety Applications

Tim Leinmüller
DaimlerChrysler AG,
Research Vehicle IT and Services

Mykonos, 8 June 2006



■ Introduction

- Sevecom
- Standardization
- Privacy, Security and Gradual Deployment
- Summary





eSafety Projects

SEVECOM

Projects

- Aide
 - Driver Vehicle Interface
- EASIS
 - Electronic Architecture
- PReVENT
 - Preventive Safety
- GST
 - On-line safety services
 - GST-SEC



New projects

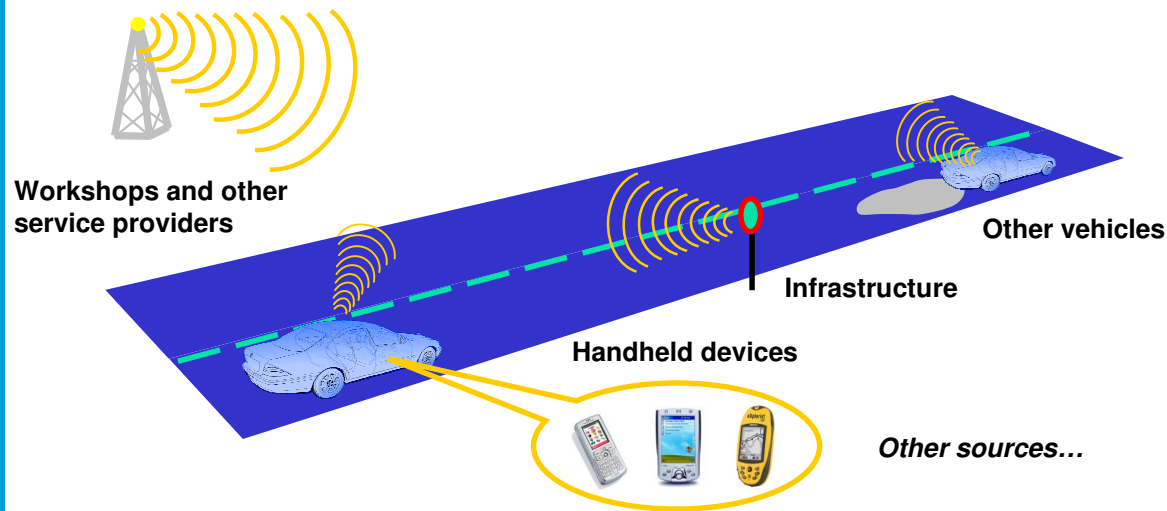
- SafeSpot
 - Cooperation for road safety
- CVIS
 - Cooperation for traffic efficiency
- Coopers
 - Seamless services along the travel chain
- COMeSafety
 - Coordination
- SEVECOM
 - Security of cooperative systems





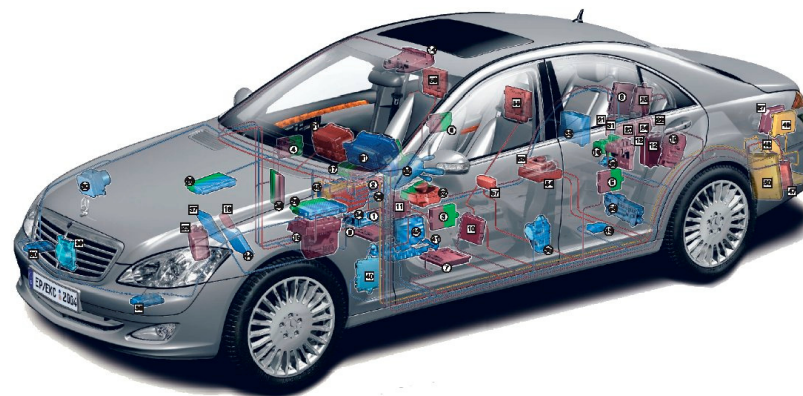
The Communicating Vehicle

SEVECOM



External communication

(V2X communication
i.e. V2V and V2I)

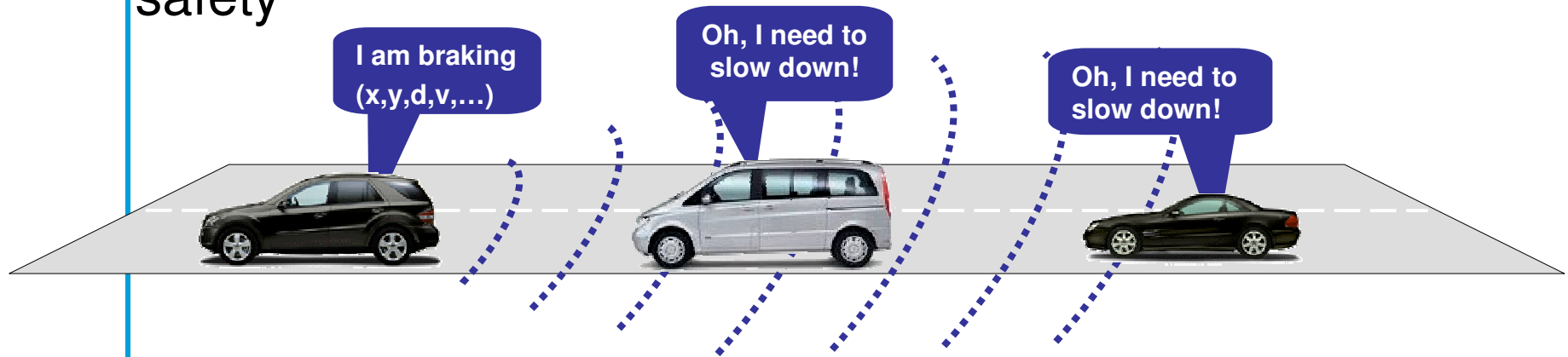


Internal communication

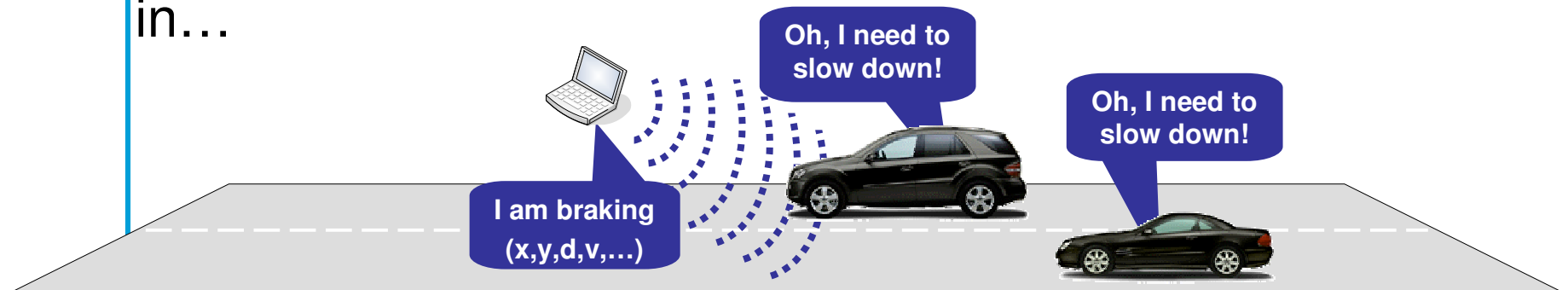


V2X Communication - Security *SEVECOM*

- Sharing information among vehicles helps to improve safety



- However, inadequate security support could easily result in...

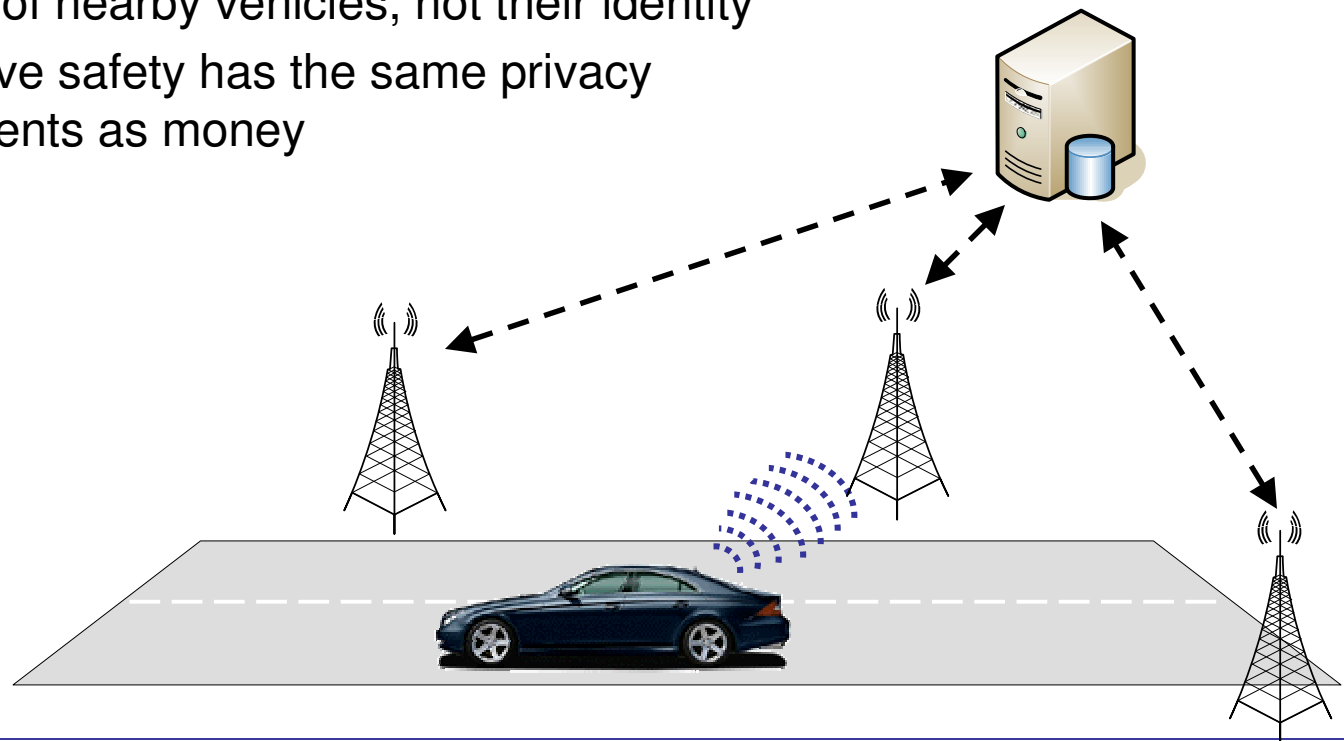




V2X Communication - Privacy

SEVECOM

- C2C / C2I communication in itself should not make it easier to identify or track vehicles
- If the privacy of the drivers is violated, the technology will not succeed
 - Active safety applications require knowledge on activities of nearby vehicles, not their identity
 - Automotive safety has the same privacy requirements as money





- Introduction

- Sevecom

- Standardization

- Privacy, Security and Gradual Deployment

- Summary





SE-cure VE-hicle COM-munication *SEVECOM*

- 3-year project 2006-2008



- Partners

- Trialog (Coordinator)



- DaimlerChrysler

DAIMLERCHRYSLER

- Centro Ricerche Fiat



- Philips



- Ecole Polytechnique Fédéral de Lausanne



- University of Ulm



- Budapest University of Technology and Economics





- Mission
 - Define a consistent and future-proof solution to the problem of V2V/V2I security
- Focus
 - Communications specific to road traffic
 - Messages related to traffic information
 - Anonymous safety-related messages
 - Liability-related messages
- Approach
 - Collaboration with eSafety projects
 - Collaboration with the C2C consortium



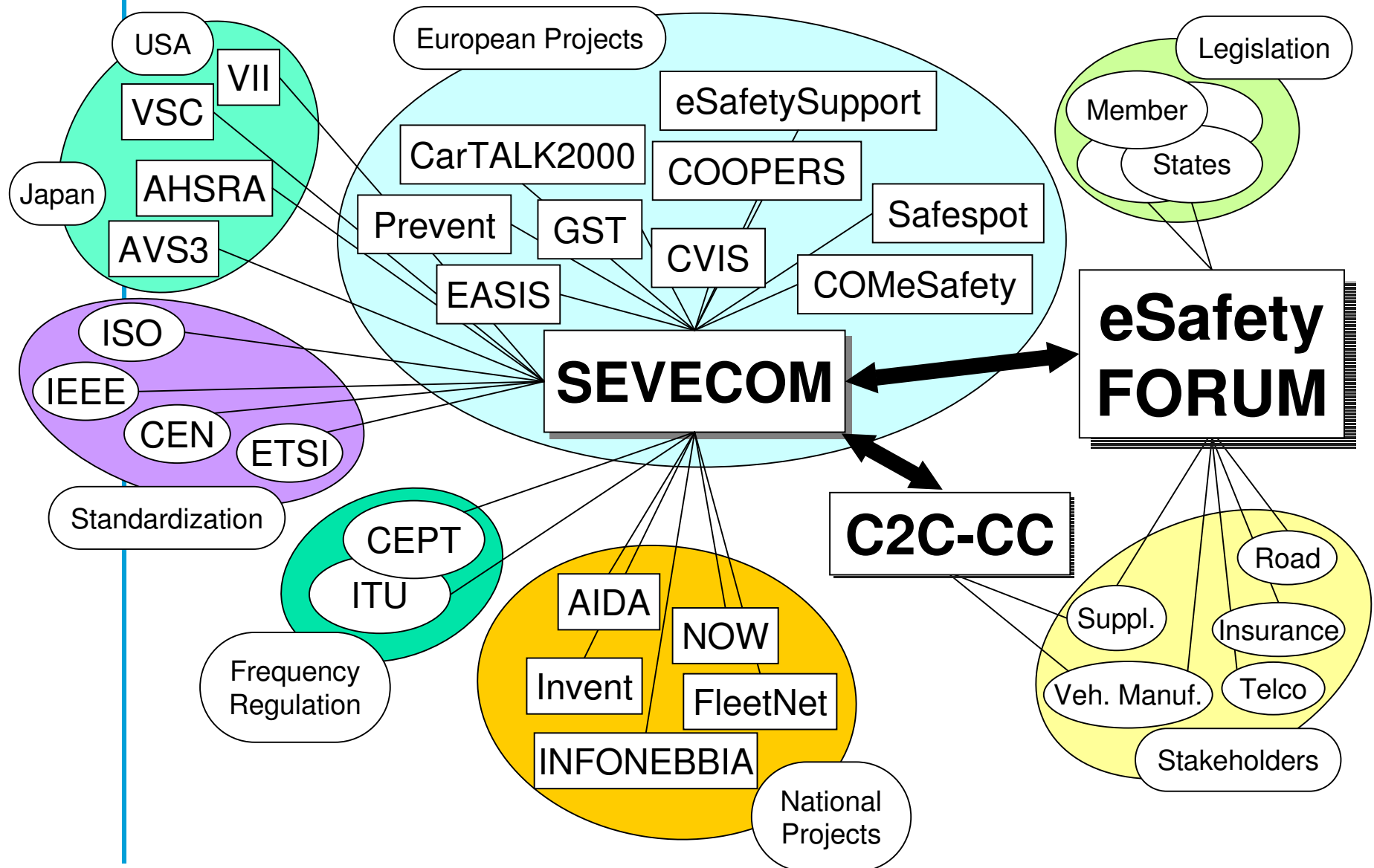
- Introduction
- Sevecom
- Standardization
- Privacy, Security and Gradual Deployment
- Summary





Research and Standardization

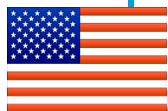
SEVECOM





Standardization and Consortia

SEVECOM



IEEE 802.11p: WAVE
(Wireless Access for the Vehicular Environment)

IEEE 1609: DSRC
Dedicated Short Range Communication

IEEE 1609.2: WAVE Security



CAR 2 CAR
COMMUNICATION CONSORTIUM

ETSI ERM TG37

Radio Basis System: WAVE – IEEE 802.11p

Standardization worldwide on Telematics: ISO TC 204 WG 16 (CALM)

Vehicle Infrastructure Integration Initiative (VII)
Vehicle Safety Communication Cons. (VSC)

DAIMLERCHRYSLER



TOYOTA



GM



Car2Car Communication Consortium
(C2C CC)



DAIMLERCHRYSLER

NEC

PHILIPS

FT/AT



- Introduction
- Sevecom
- Standardization

■ Privacy, Security and Gradual Deployment

- Summary





Security and Privacy

SEVECOM

- Current proposals for security in VANETs and V2X communication rely on certificates and pseudonyms
 - Security: certificates
 - Privacy: pseudonyms that change over time
- However
 - PKI based certificates are expensive
 - Certification Authority (CA) has to be coordinated on a European level (laws, etc.)
 - Someone needs to setup and run the CA
 - Certificates need to be maintained
- Who will pay for certificates / the CA?
 - Manufacturers – NO
 - Customers – NO



Gradual Deployment...

SEVECOM

- Deployment of VANETs will take several years
 - Most active safety applications require a considerable node density
- Deployment cost, especially in the beginning, have to be as low as possible
 - Selling a system that is going to work in a couple of years from now, is impossible
 - Spending money in advance probably won't pay off for vehicle manufacturers, or at least they're not willing to take the risk
- ➔ Therefore, a strategy with successive deployment is required, including a simple and inexpensive market introduction strategy



...Security

SEVECOM

- V2X communication
 - Usage of a permanently available online certification infrastructure
 - Alternatives
 - Mechanism to determine that a message has been sent by an authorized node
 - Possibility to preload key material during (bi-)annual service checks
- In-vehicle communication protection
 - Example: protection of sensor data transport against in-vehicle attackers
 - Tamper resistant hardware
 - Securing previously insecure in-vehicle communication

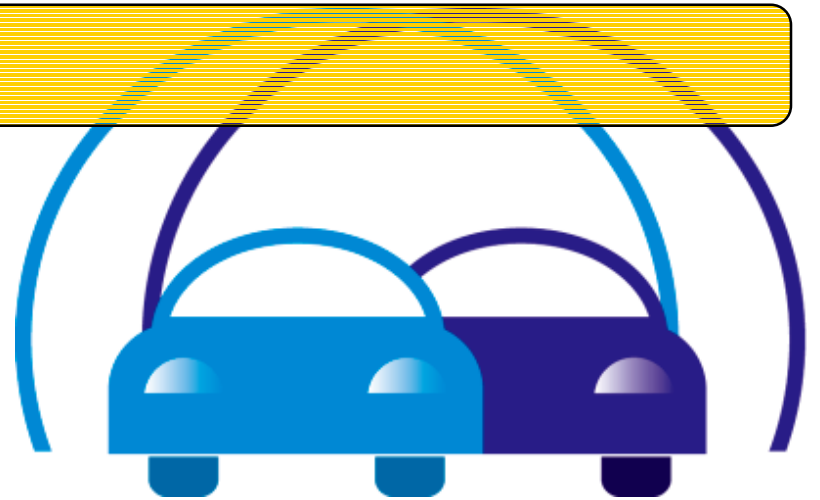


- Usage of a permanently available online certification infrastructure is not desirable, due to deployment cost and operational cost
 - Furthermore
 - Quasi central key distribution all over Europe
 - Cross-national administration and different laws
- Tamper resistant hardware must not increase cost
 - Especially if used solely for the purpose of V2X-communication
- Securing in-vehicle communication systems solely for the purpose of V2X-communication is an exclusion criterion



- Introduction
- Sevecom
- Standardization
- Privacy, Security and Gradual Deployment

■ Summary





Summary

SEVECOM

- V2X communication is an enabling technology for eSafety applications (active safety)
- Research and standardization efforts worldwide are ongoing
 - EU: eSafety initiative, C2C-CC
 - US: DSRC, WAVE, VII, VSC
- Security for V2X communication is a challenging task
 - New requirements unknown to conventional systems
 - Privacy
 - Trust
 - Reliability
- Sevecom is aiming at the definition of a consistent and future-proof solution for V2X security

Secure Vehicle Communication



Thank You

Contact Information

<http://www.sevecom.org>

info@sevecom.org

Tim.Leinmueller@daimlerchrysler.com
