Secure Vehicle Communication

Joint Meeting SEVECOM/CVIS/SafeSpot

11 April 2006

Lämmerbuckel

Joint Meeting Agenda

- 11.50 Presentation of Projects
  - SEVECOM
  - Safespot
  - CVIS
- 12.40 Lunch
- 14.00 Requirements and Use Cases
  - SEVECOM
  - Safespot
  - CVIS
  - Walk-though an example of requirements
- 15.35 Break
- 16.00 Technical Issues
  - Identify mgt
  - PKI infrastructure Other items
  - Protocol Issues
  - Platforms to be used
- 17.00 COMeSafety
  - Requirement convergence
  - Actions
- 17.30 Close

Secure Vehicle Communication

Antonio Kung

SEVECOM Project Co-ordinator

TRIALOG

SE-cure VE-hicle COM-munication

- 3-year project 2006-2008
- Partners
  - Trialog (Coordinator)
  - DaimlerChrysler
  - Centro Riserche Fiat
  - Philips
  - Ecole Polytechnique Fédéral de Lausanne
  - University of Ulm
  - Budapest University of Technology and Economics

SEVECOM

SEVECOM

- 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 project
  - collaboration with the C2C consortium

Security Objectives

SEVECOM

- Architecture and security mechanisms
  - provides the right level of protection.
  - addresses issues such as liability versus privacy
- Fully addressed topics
  - Key and identity management,
  - Secure communication protocols (including secure routing),
  - Tamper proof device and decision on crypto-system,
  - Privacy.
- Investigated topics
  - Intrusion Detection,
  - Data consistency,
  - Secure positioning,
  - Secure user interface.

Development Objectives

SEVECOM

- Cryptosystem
  - Adapted to specific operational environment
    - sporadic connectivity created by moving vehicles and the resulting real-time constraints
    - specific QoS needs
  - Future proof
    - address the variety of today and future threats
  - Deploy-able
    - mainstream: adaptations of existing cryptosystems to the VC environment.
    - Meets low-cost requirements of embedded systems in vehicles.

Milestones

SEVECOM

- Semester 2
  - Requirements
  - Architecture 1
- Semester 3
  - Architecture 2
  - Security Mechanisms 1
- Semester 4
  - Security mechanisms 2
  - Developments 1
  - Investigated topics 1
  - Roadmap 1
- Semester 5
  - Developments 2
  - Investigated topics 2
- Semester 6
  - Validation
  - Roadmap 2

GST- SEC Legacy

SEVECOM

- Subproject of GST (2004-2006)
- Partners

TRIALOG

KU LEUVEN

TECHNISCHE UNIVERSITÄT MÜNCHEN

RENAULT

DAIMLERCHRYSLER

- Architecture and mechanisms for secure telematics applications
- Understand impact for stakeholders
  - e.g. certification in trust value chain

GST-SEC Security Legacy

SEVECOM

- V2I Infrastructure
  - PKI
- Communication
  - Secure Communication Engine handling integrity and confidentiality
- Execution
  - Security Module
  - Authentication & Authorisation Broker
- Application and Services
  - Circle of trust / Federated Identities

GST-SEC Development Legacy

SEVECOM

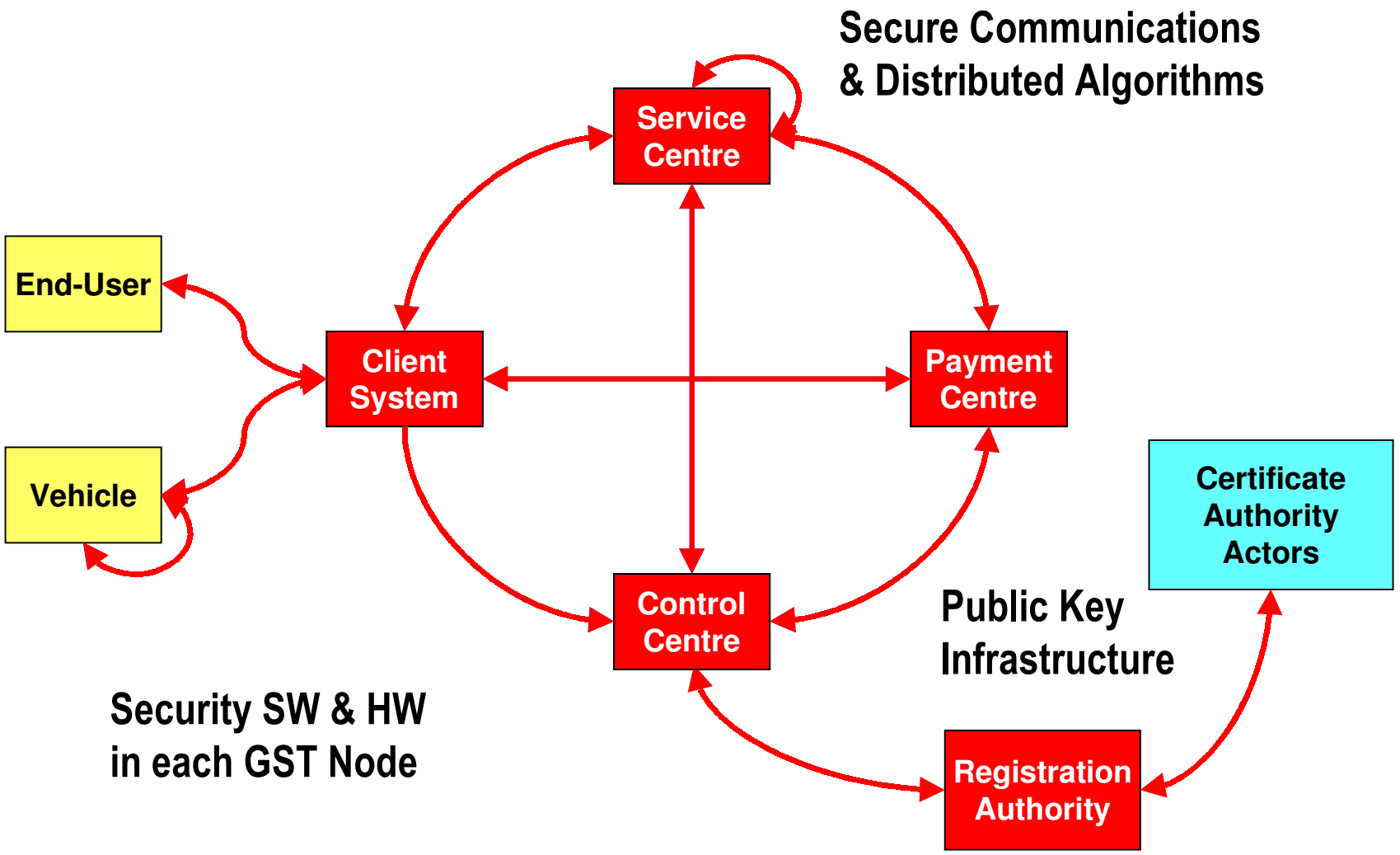
- Future proof architecture
  - Allows introduction of more powerful security technology in the future
- Infrastructure
  - Separation of concerns security versus application
  - Heterogeneous solutions
  - Security components plug-in

Thanks!

Thanks to DaimlerChrysler for hosting this event

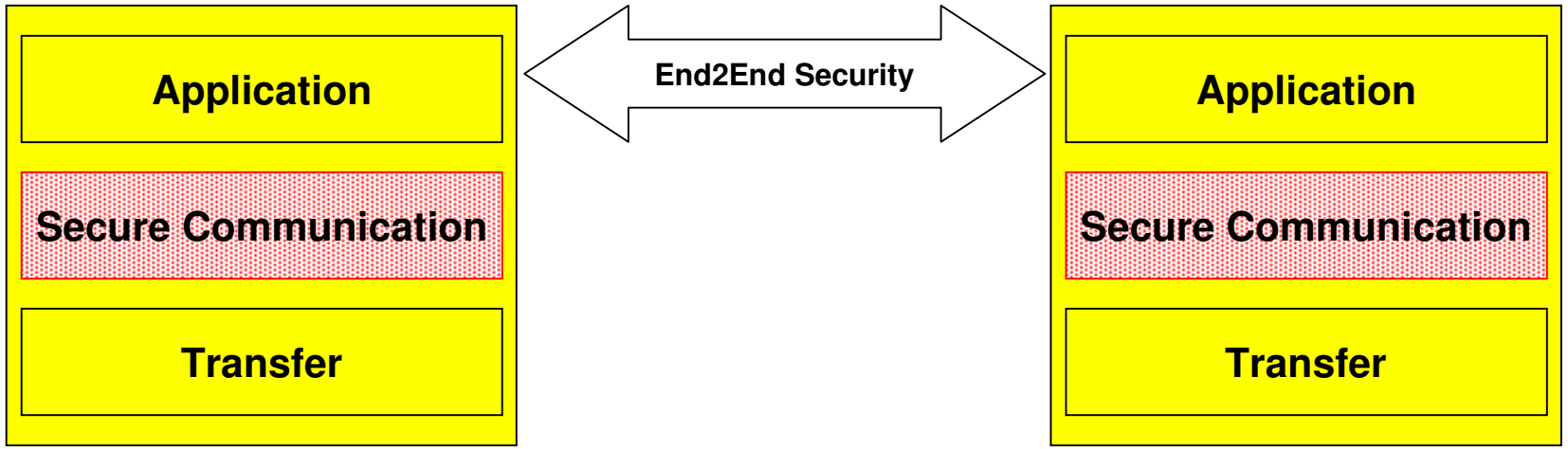
Backup Slides

PKI

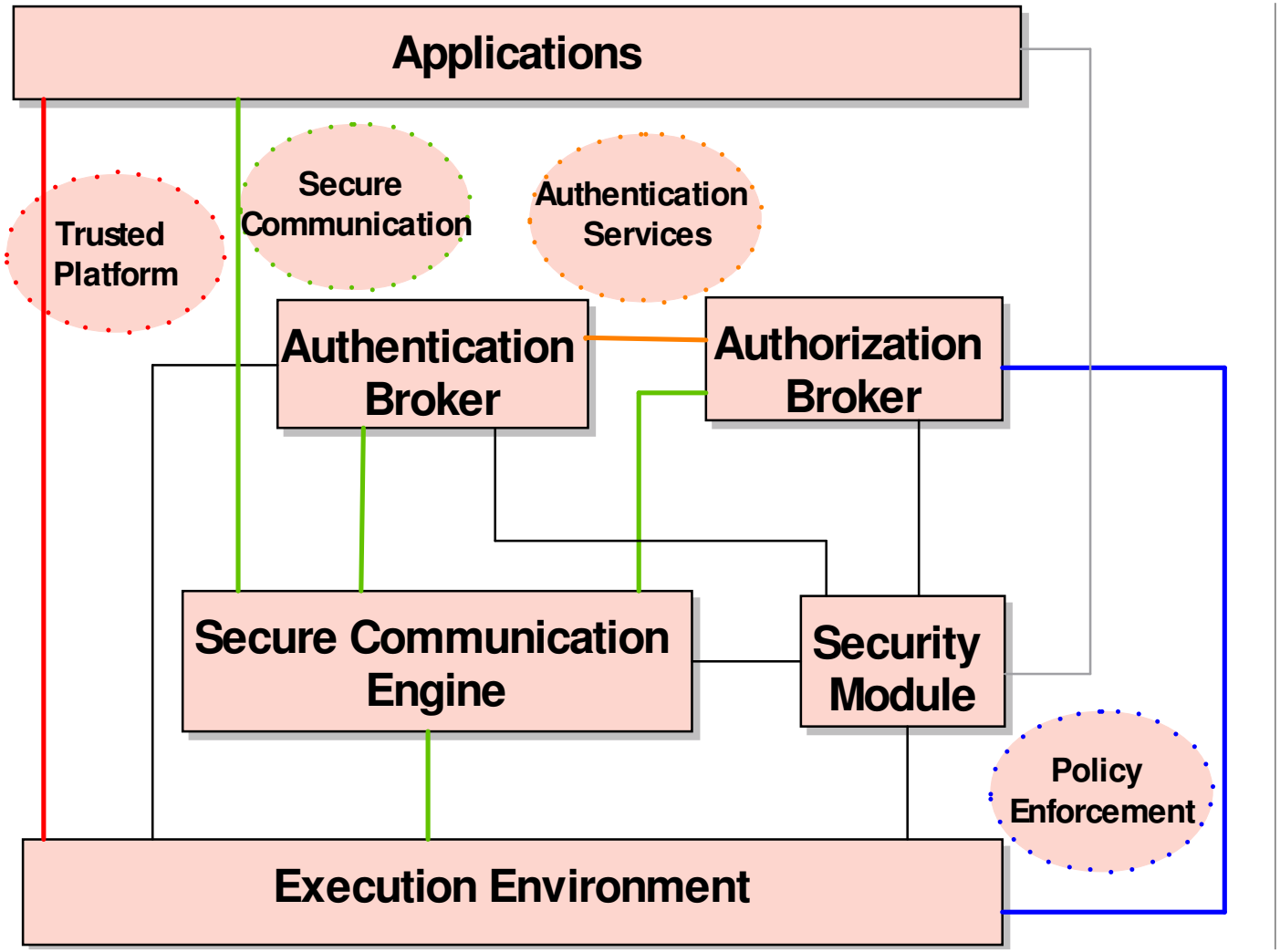

Secure Communications
& Distributed Algorithms
Service Centre
End-User
Client System
Payment Centre
Vehicle
Certificate Authority Actors
Control Centre
Public Key Infrastructure
Security SW & HW
in each GST Node
Registration Authority

Layered Security Architecture

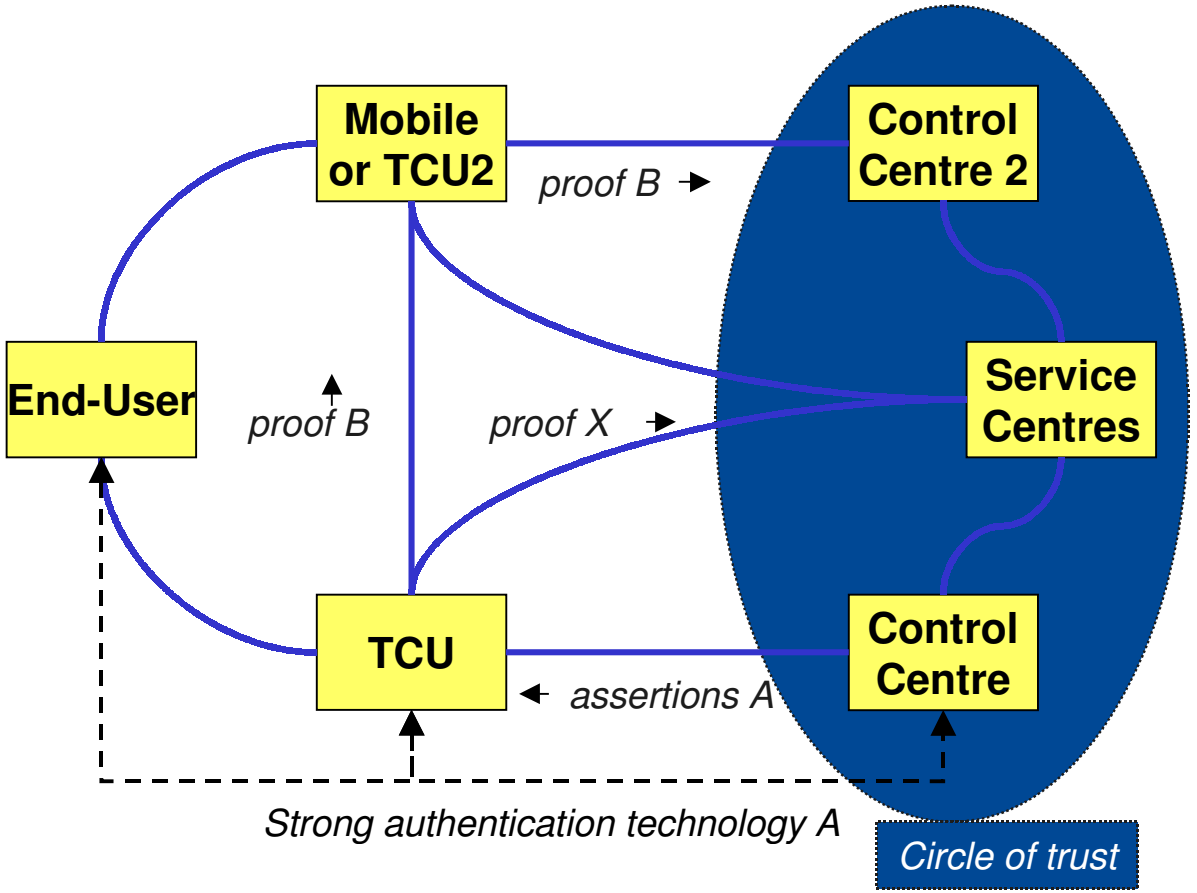
- Security aware GST nodes follow a layered model



Inside the GST Node



Circle of Trust



Specific security solution for Control Centre authentication

Sharing of identification and related responsibilities

Open assertion mechanism for identification sharing