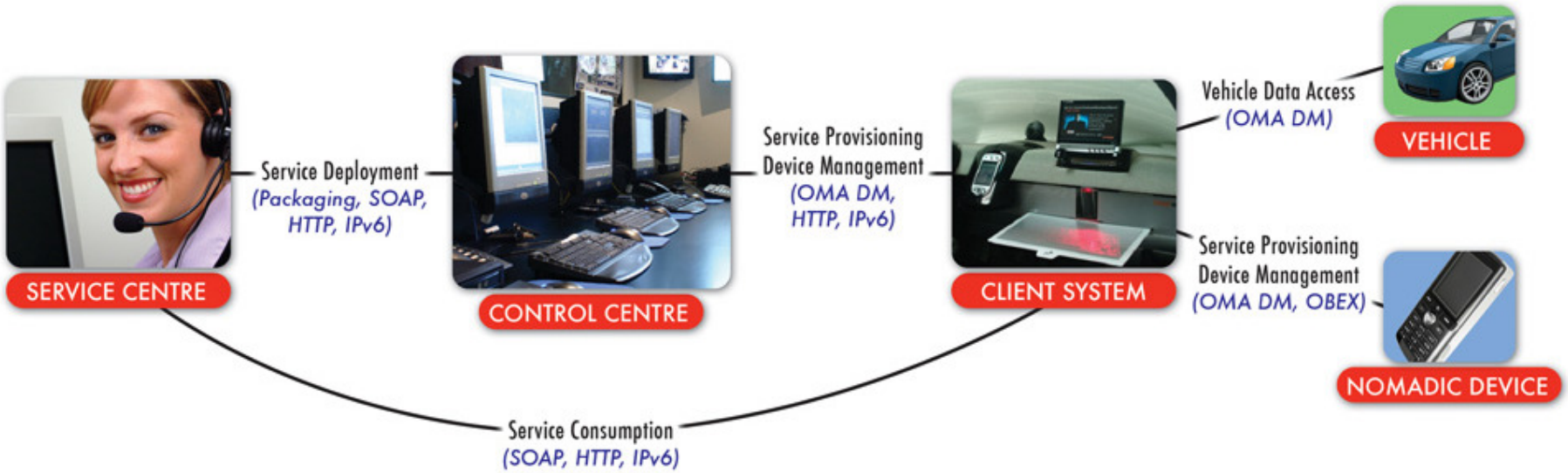
In-vehicle Telematics services and data protection: generating users' confidence

GST project

Antonio Kung (Trialog)
Danny de Cock (KU Leuven)

GST (March 2004-March 2007)

- Define an infrastructure for open telematics applications



GST SEC

- Subproject of GST
  - infrastructure for secure telematics applications

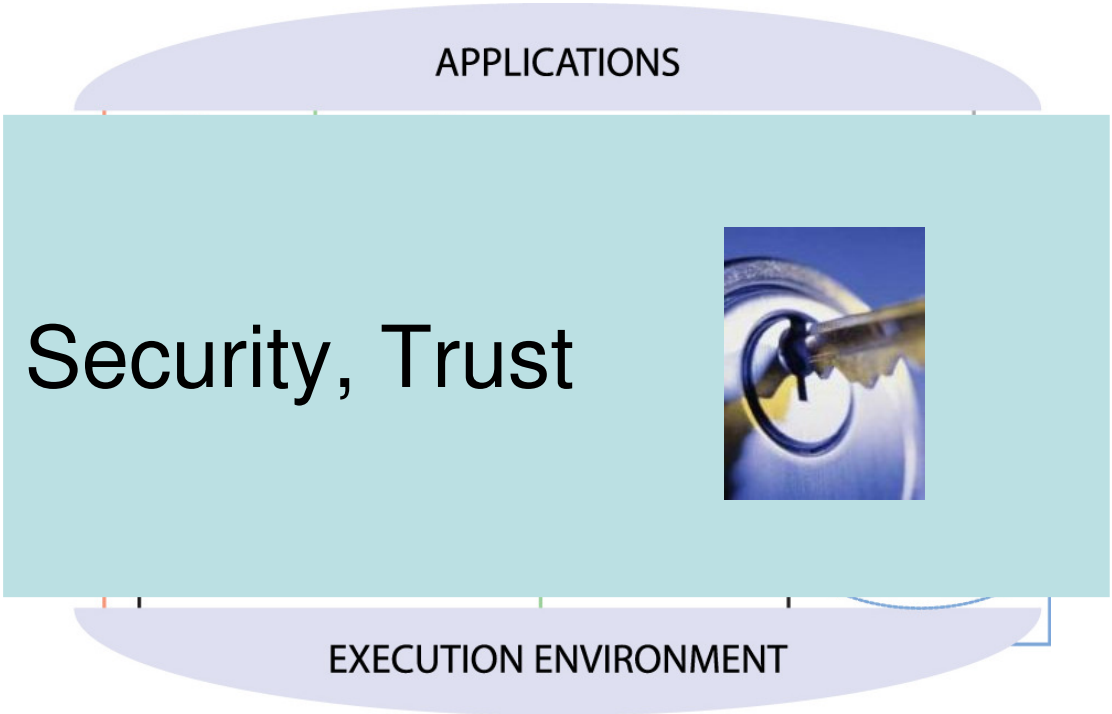
TRIALOG

DAIMLERCHRYSLER

KU LEUVEN

TUM TECHNISCHE UNIVERSITÄT MÜNCHEN

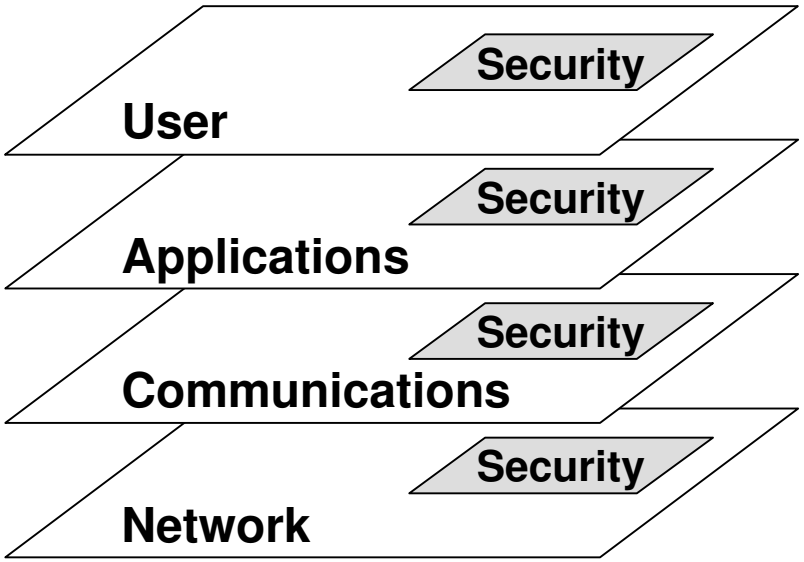
Add Security and Trust



Why (raison d'être)

- Creating trust
  - Understand requirements
- Fundamental problem
  - Awareness and integration from the start
    - Organisational aspects (PK Infrastructure)
  - Heterogeneous technology
  - Trust value chain

GST's Security Focus



Focus

Strong authentication of {user, device, service provider} ✔

Applications integrity

Secure communications ✔

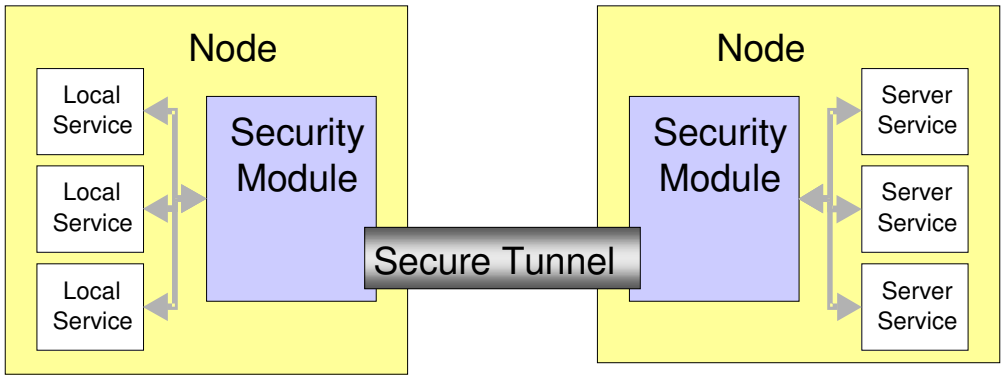
Network access

Requirements

- Critical requirements (45 requirements)
  - Business trust
    - e.g. Distributed authorisation
    - e.g. Authentication services
  - Secure communication and trusted execution platforms

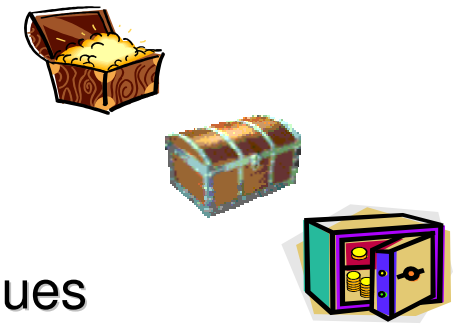
Architecture

- Distributed architecture for authorisation
  - Single sign-on
  - Federated identities /circle of trust
- Architecture
  - secure tunnels
    - Insecure
    - Authenticated
    - Confidential
    - Secure
  - security modules

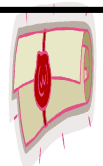
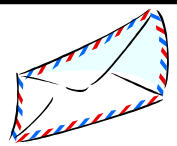


Security – How?

Based on implementation complexity and cost:



- No security mechanisms
- Non-cryptographic techniques (e.g., CRC, hardware enclosures,…)
- Combine the above with cryptographic techniques

Security Levels		Protect Confidentiality	
		Yes	No
Protect Integrity	Yes	Secure 	Authenticated 
	No	Confidential 	Insecure 

Security – What?

- Data exchanged between users and service providers
  - User requests service
    - Information and data exchange
  - Service provider provides service
    - Client-server model
- Application data
  - Used by the services

Trust Value Chain

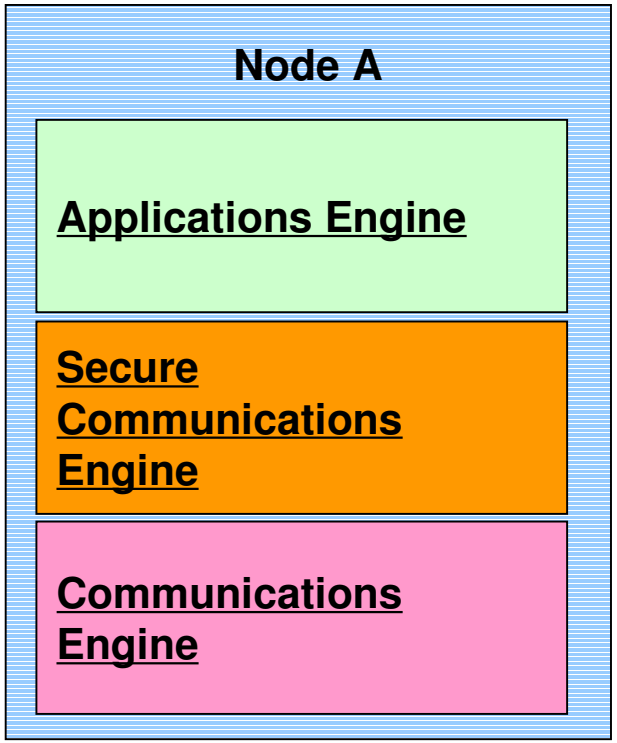
- Vehicle manufacturer
  - Vehicle
- Service provider
  - Vehicle
  - In-vehicle devices
- User
  - Vehicle
  - In-vehicle devices
  - In-vehicle supported services

Depends

Trust
=
Business
=
Money

Network security vs. Enhanced Privacy vs. Data Protection

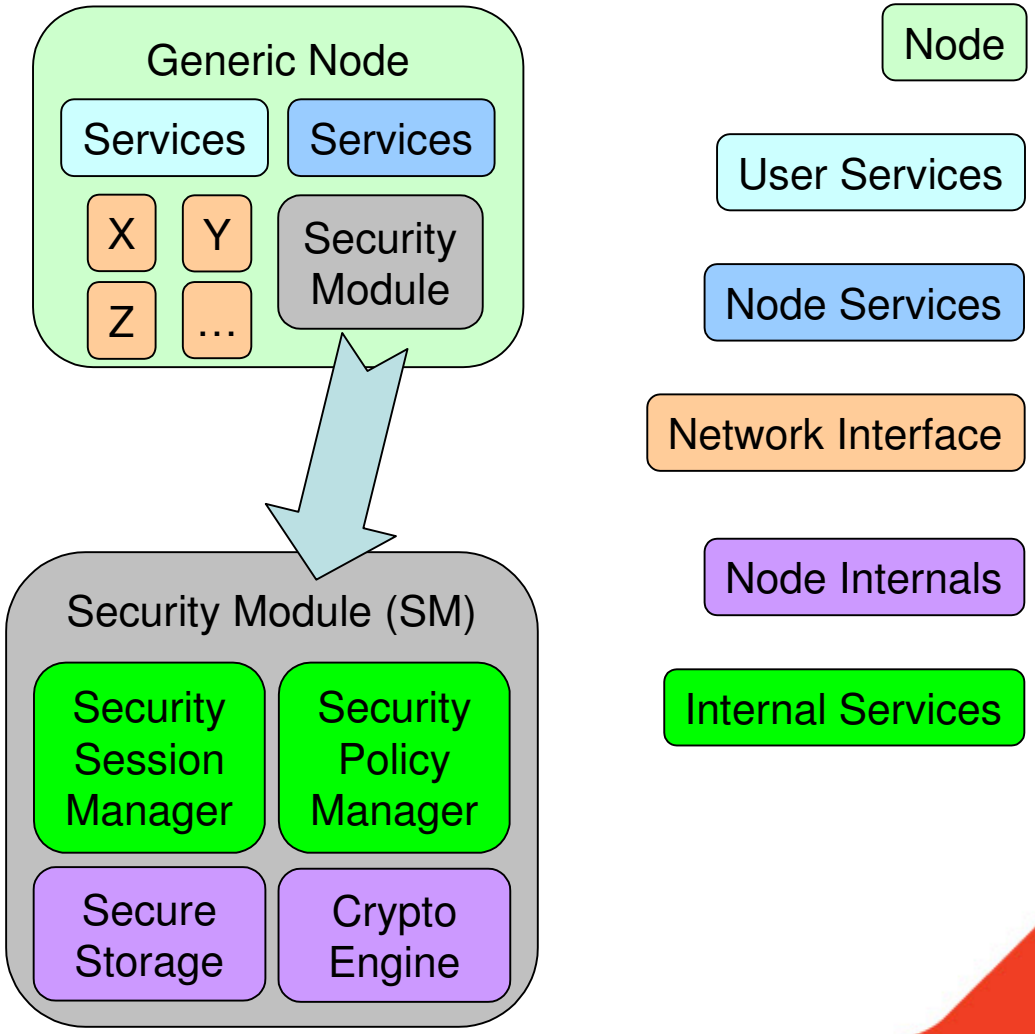
- Application security
  - Data protection
    - Prevent abuse
- Network security
  - Secure communications
    - Protect integrity and confidentiality
- Network access
  - Privacy
    - Who is exchanging information?
    - Protect access



Nodes and Security Modules

Key Features of a Security Module:

- One SM per Node
- SM = e.g., OSGi bundle
- SM offers services to other bundles
- SM initialized by manufacturer
- Initialized SM ready to be used
- Combination of hard- and software
  - Hardware ➔ Non-cloneable
  - Software ➔ Risk for cloning
- Provide true strong authentication
- Secure communications rely on SM
  - Insecure
  - Authenticity
  - Confidentiality
  - Secure = Auth. + Conf.



SM Functionality

- Secure persistent storage engine
  - User data, Communications session data
- Authentication engine
  - Digitally sign outgoing information
  - Calculate Message Authentication Code
  - Verify incoming authenticated data
- System-wide “trusted” information
  - Root CA certificates
  - Trust anchors with respect to registration proofs
- Operates in client-server mode
  - Difficult to enforce use of security module at client side
  - Server can determine whether the correct SM was used

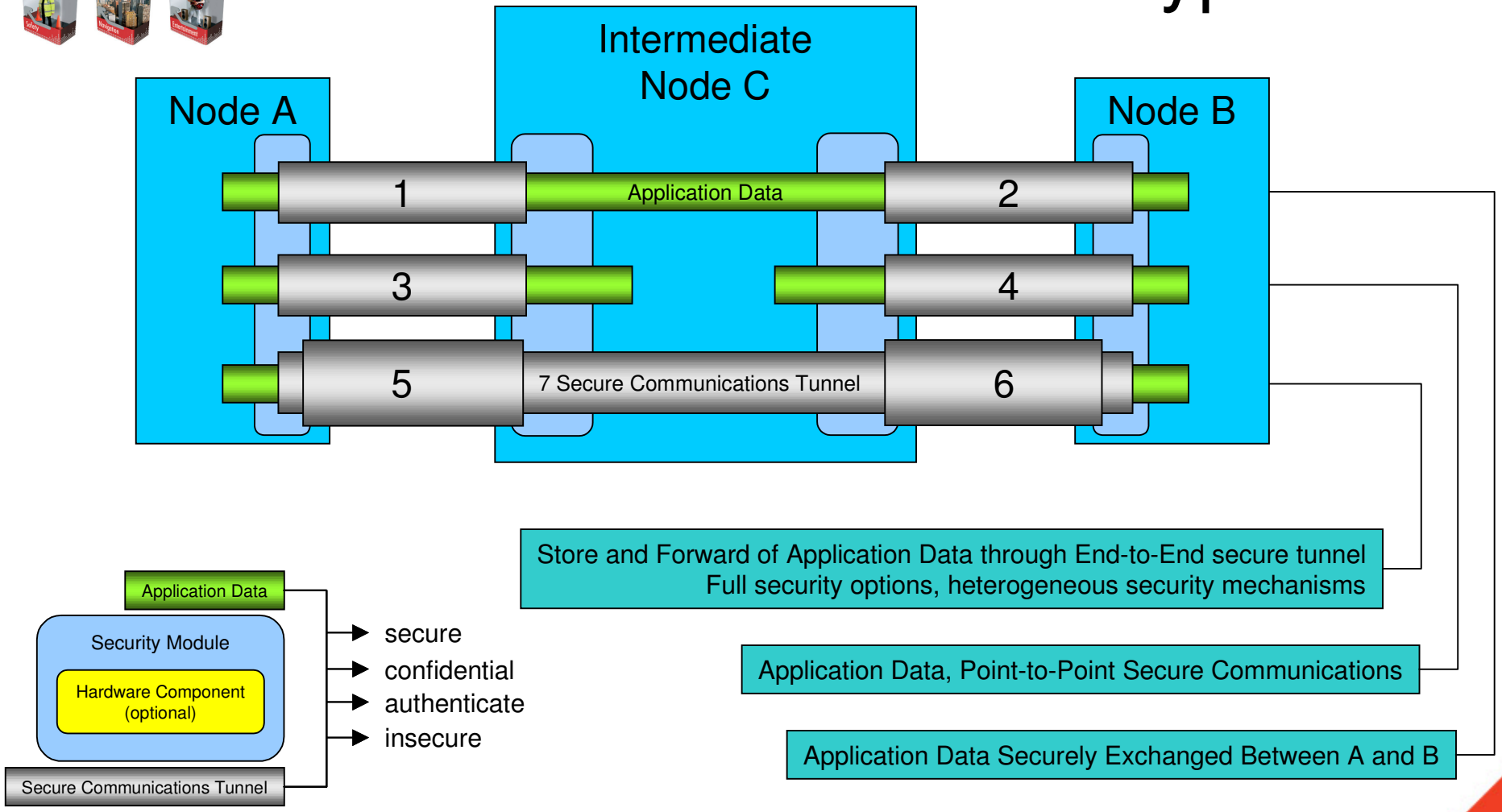
Data Protection

Confidence

Confidence

Trust

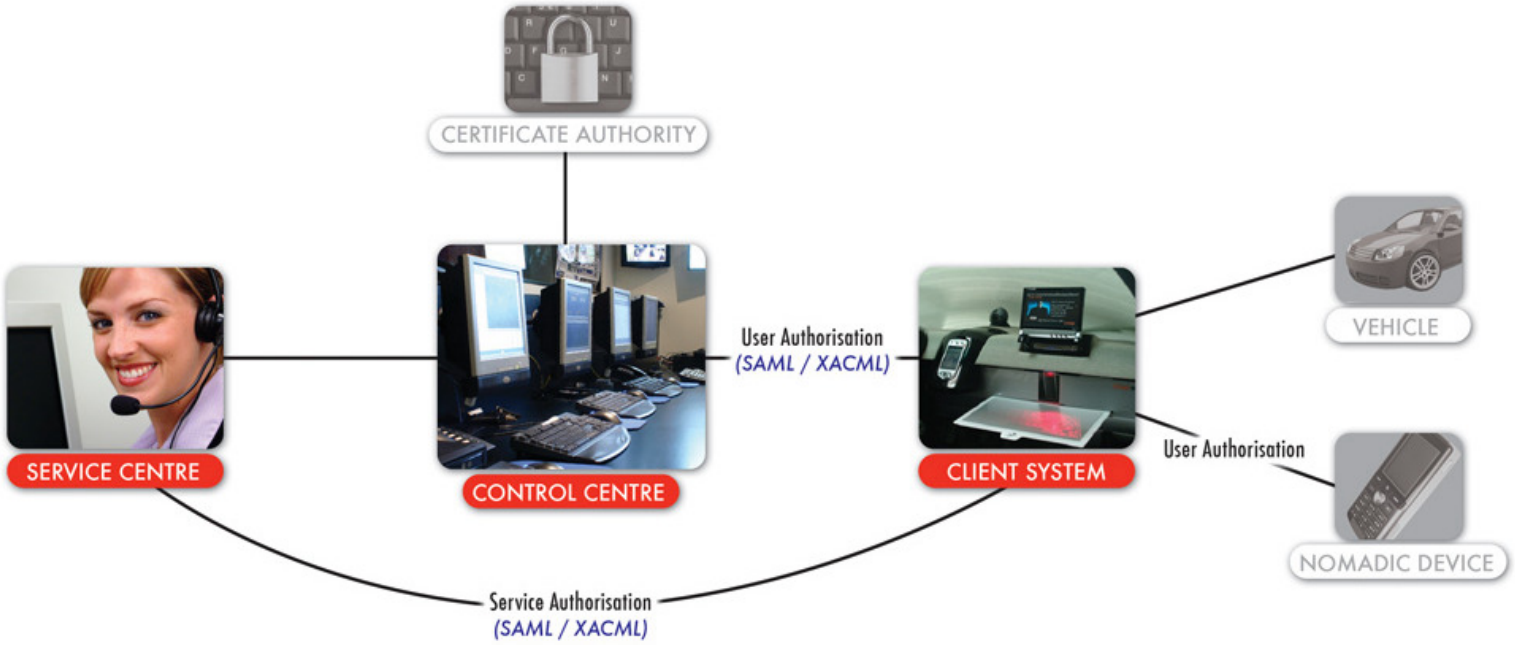
Secure Communication Types



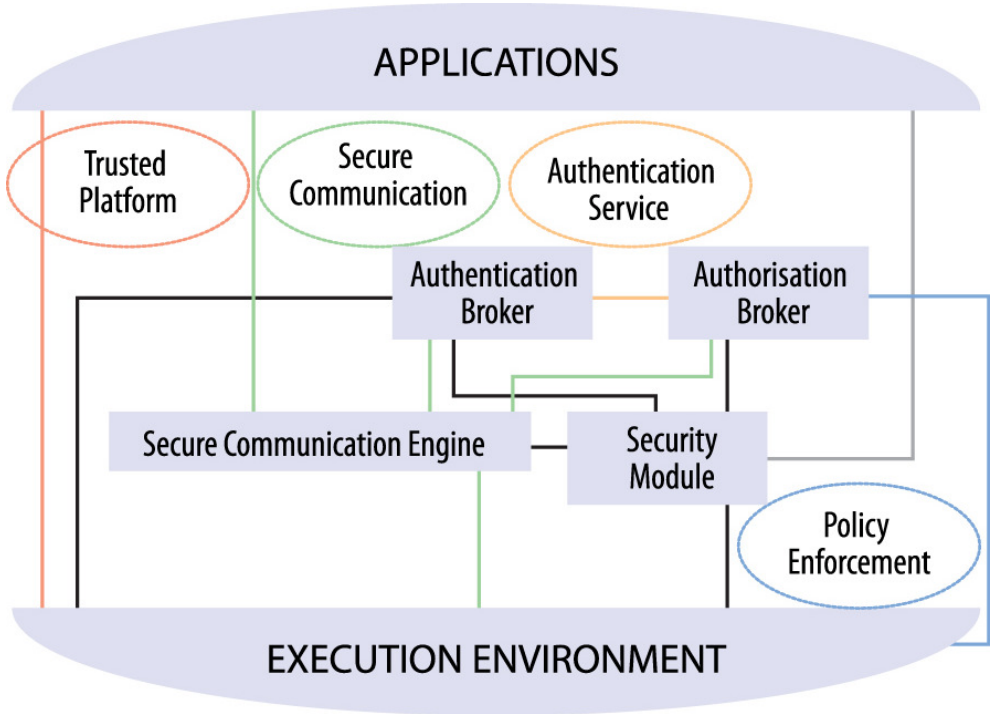
Conclusion (1)

- Privacy enhancing measures
  - Protocols make identification difficult
    - Communication latency
    - Calculation complexity
- Data protection
  - Logging, integrity + access control
- Confidence
  - Not technical – depends on trust and reputation

Conclusion (2) Design Pattern



Conclusion (3) Design Pattern



Conclusion (4) Legacy

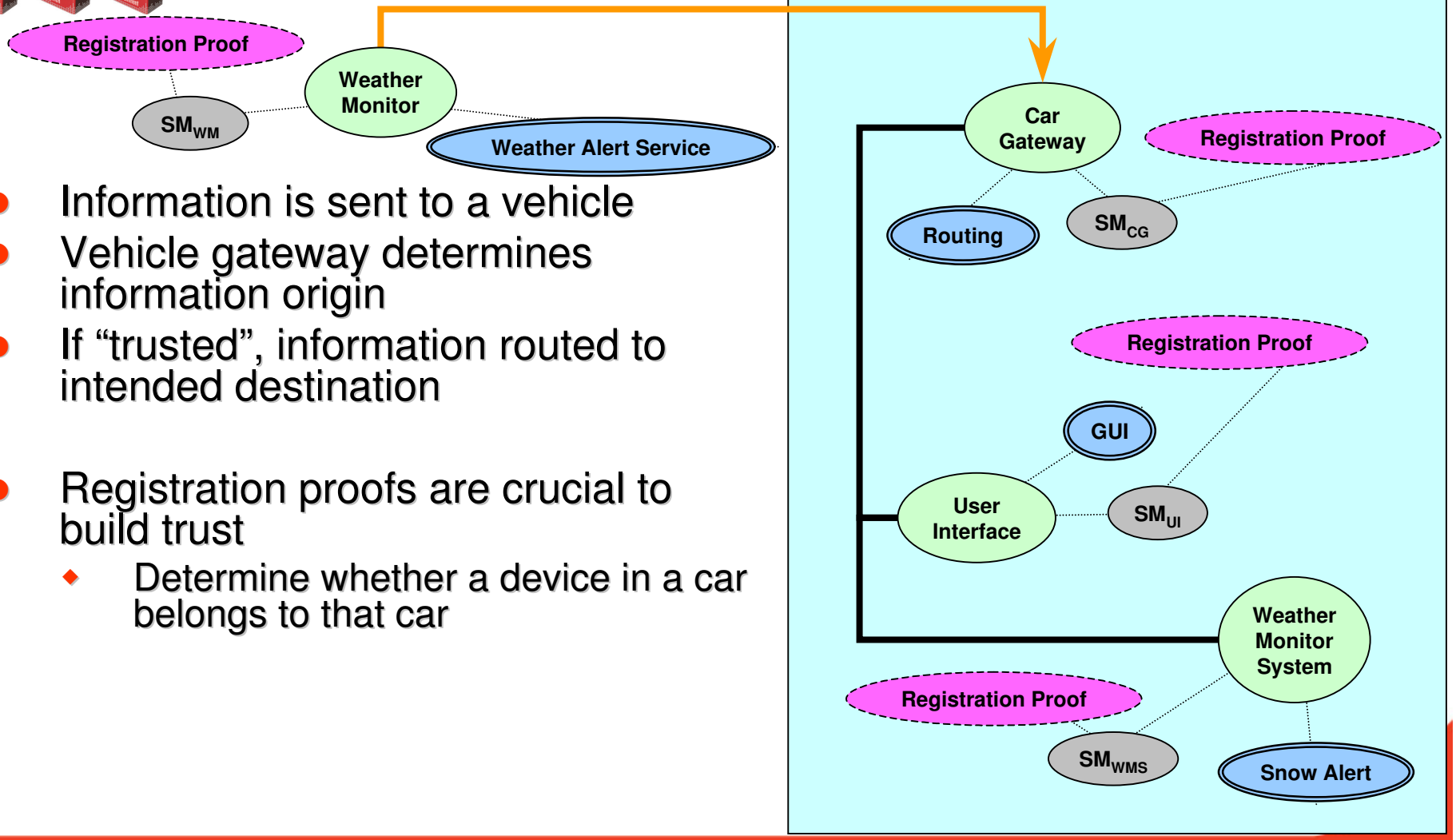
- Sound architecture
  - Development focus: business trust
  - Next step : User trust and privacy
- Identification of roadmap
  - Phase 1: Small market
    - Dedicated OEM solutions, Simple security
  - Phase 2: Large market
    - OEM solutions with federation, Strong Security
  - Phase 3: Open market
    - Security standard with empowerment

Thank you!

Antonio.Kung@trialog.com
Danny.DeCock@esat.kuleuven.be

Backup slides

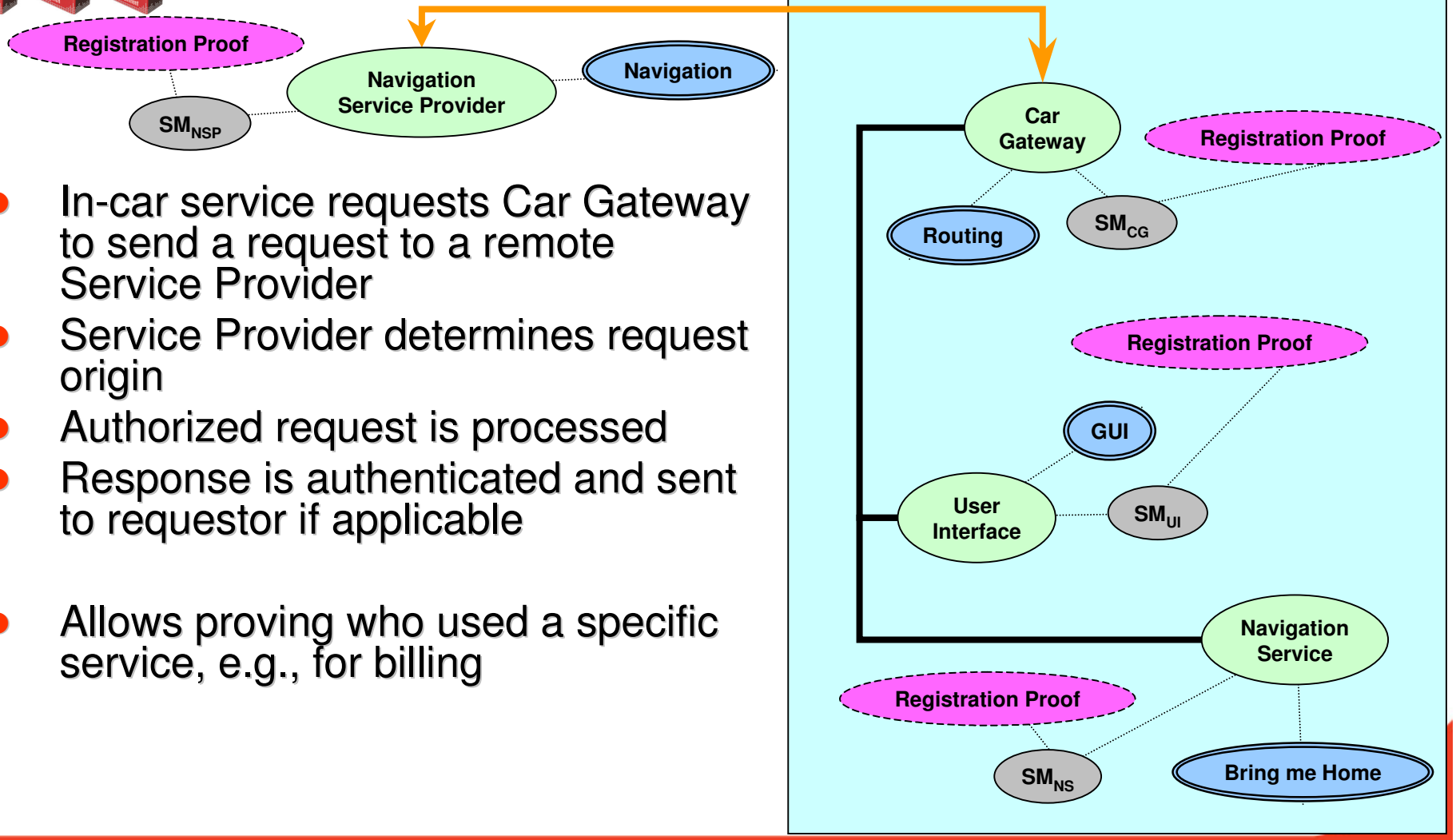
Pushing Data to Car



- Information is sent to a vehicle
- Vehicle gateway determines information origin
- If "trusted", information routed to intended destination

- Registration proofs are crucial to build trust
  - Determine whether a device in a car belongs to that car

Pulling Data to Car



- In-car service requests Car Gateway to send a request to a remote Service Provider
- Service Provider determines request origin
- Authorized request is processed
- Response is authenticated and sent to requestor if applicable

- Allows proving who used a specific service, e.g., for billing