mFUND
Das Startkapital für die Mobilität 4.0

Rail2X

SIEMENS
Ingenuity for life

DB

DLR

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Dralle Systementwicklungen

Rail2X and ITS Security

Slawa Lang, Siemens Mobility GmbH;
“Rail2X” consortium

Safety meets Security 2019

How secure is an ITS communication system and can it be extended to rail traffic?

SIEMENS
Ingenuity for life

Rail2X?

Contents

SIEMENS

Ingenuity for life

C-ITS

Intelligent Transportation Systems

ITS shall make (road) traffic safer, more environmentally friendly, more efficient and more comfortable

SIEMENS
Ingenuity for life

Intelligent Transportation Systems (ITS)

Essential for ITS is communication:

Traffic participant ↔ other participant

Traffic participant ↔ infrastructure

→ Cooperative-ITS (C-ITS)

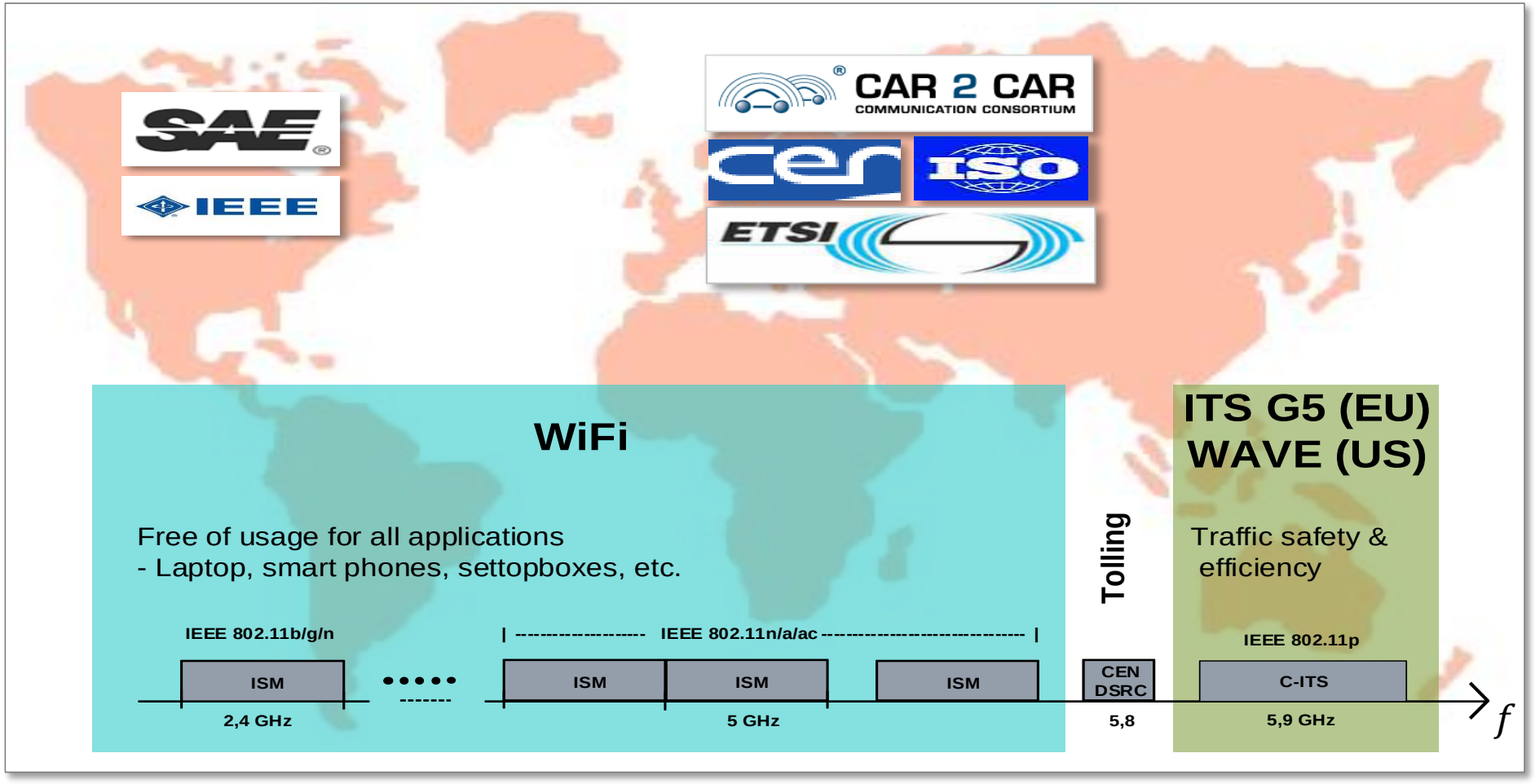
In road traffic:

Car2X, Car2Car communication

Vehicle2X uses special Wi-Fi, but 5G mobile communications could be used too

SIEMENS
Ingenuity for life

Vehicle2X – Standardization activities, frequency allocation



SIEMENS
Ingenuity for life

Rail2X

Vehicle2X technology in rail traffic

www.siemens.com/mobility

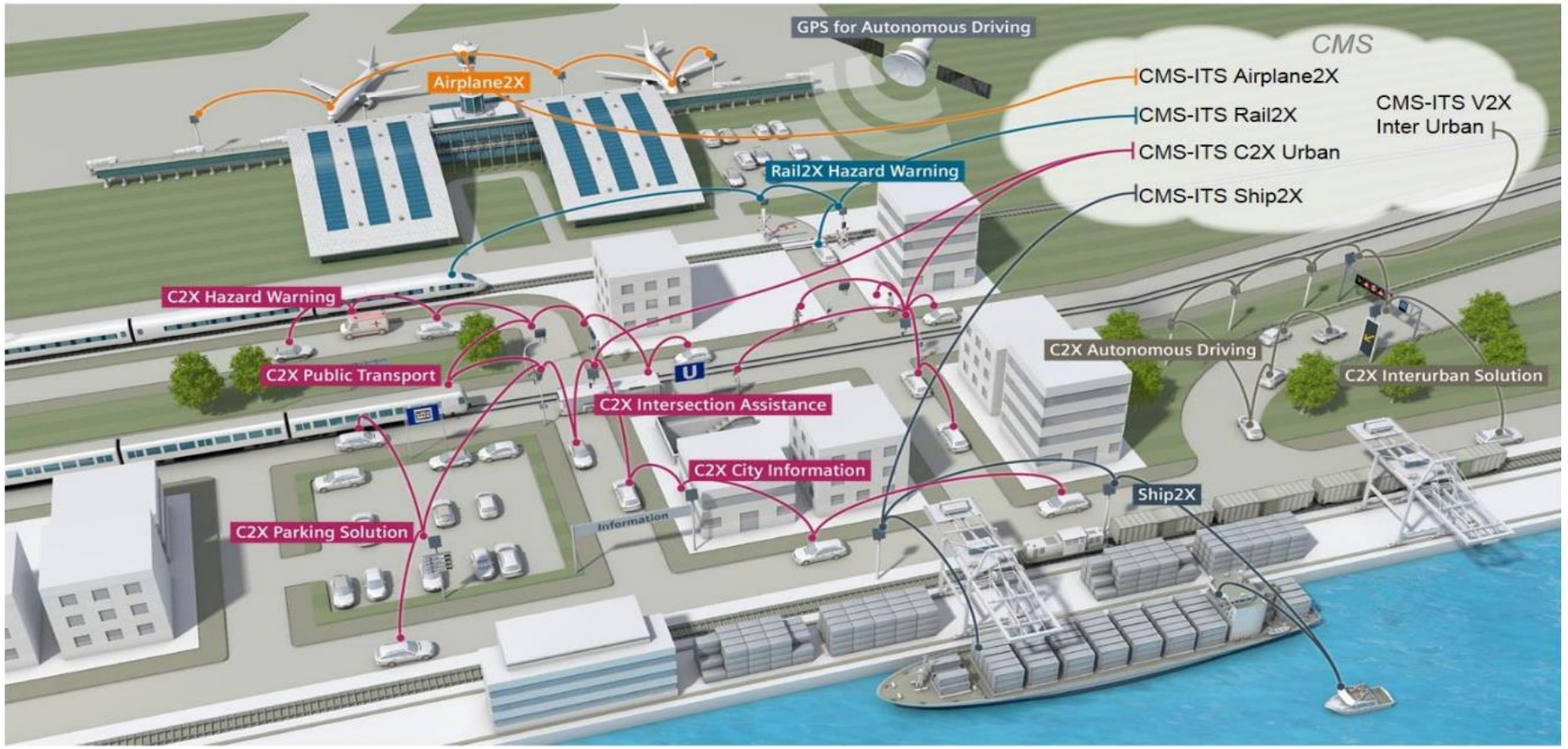
Road ITS shall be adapted to rail traffic, to facilitate efficient services

SIEMENS
Ingenuity for life

Rail2X – Smart Services

Adaptation of Wi-Fi Car2X communication to rail traffic / for rail ITS

→ increased safety
→ improved comfort
→ more efficient maintenance
→ cost reduction

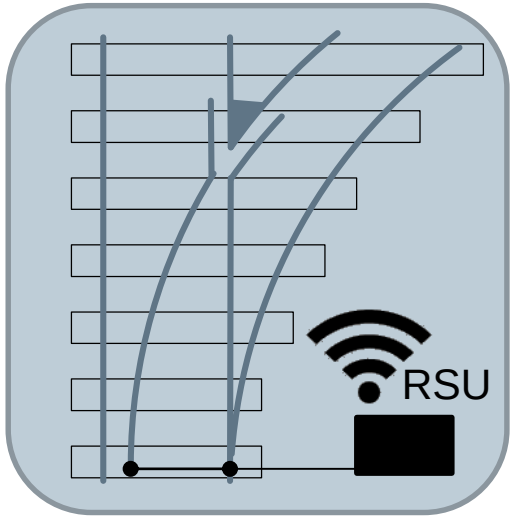


Feasibility and reasonableness are demonstrated based on 3 use cases at Erzgebirgsbahn

SIEMENS
Ingenuity for life

Rail2X – Use cases

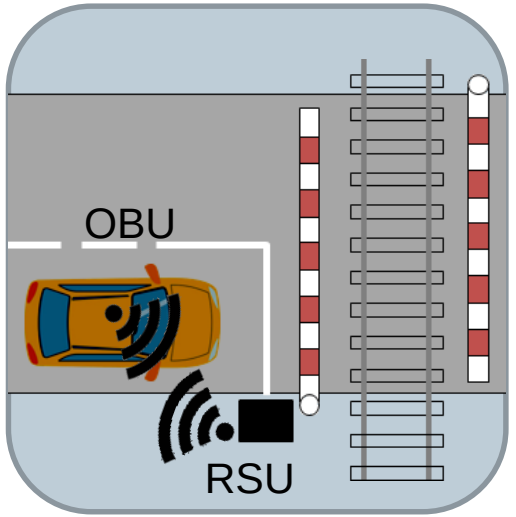
1: Service and diagnosis



Data exchange
Infrastructure ↔ train

→ inexpensive data capturing
→ more efficient maintenance

2: Barrier crossing on call



Information exchange
Vehicle ↔ level crossing

→ increased safety
→ improved comfort

3: Request stop

Information exchange
Train ↔ station

→ inexpensive communication
→ more efficient regional traffic

Data can be captured inexpensively and analyzed centrally

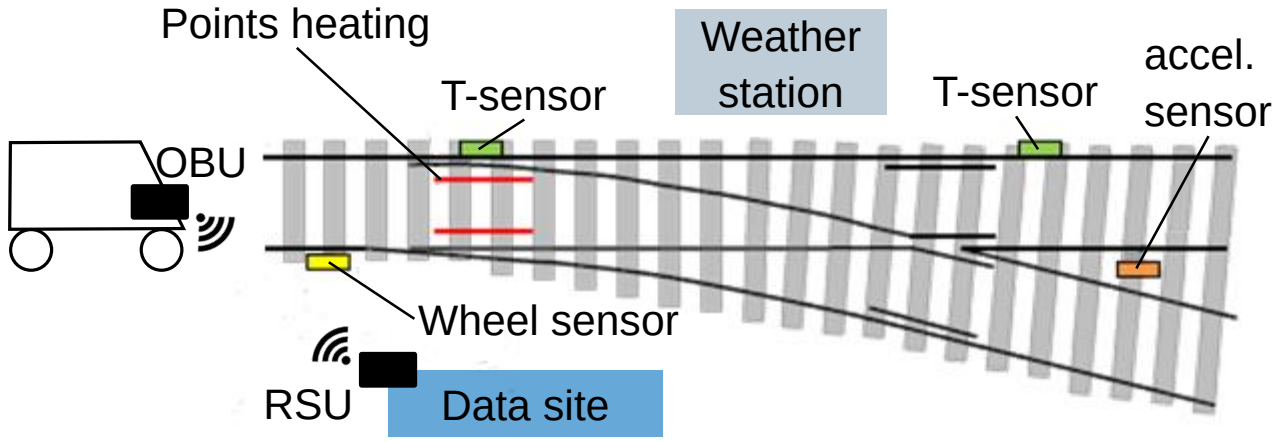
SIEMENS
Ingenuity for life

Use case 1: Service and diagnosis

- Collection of (sensor) data at important infrastructure locations (e.g. points)
- Collection of data by passing trains with Rail2X
- Transfer of data to central server e.g. in depot
- Saving and analysis of data at central place

→ inexpensive data capturing without permanent communication link

→ more efficient maintenance



Concept of barrier on call remains by more efficient log on and off

SIEMENS
Ingenuity for life

Use case 2: Barrier crossing on call

- Barrier on call:
  normally closed, opens upon logging on (if safe)
- Traffic participants without Vehicle2X:
  manual log on and off as usual
- Traffic participants with Vehicle2X:
  automatic log on and off via communication with level crossing; display of acknowledgement

→ improved comfort
→ shorter waiting times
→ increased safety

Regional traffic becomes efficient by inexpensive and comfortable request stops

SIEMENS
Ingenuity for life

Use case 3: Request stop

- Request stop:
  Train stops only upon request of passengers in train or at station
- Transmission of stop request at station to train via Rail2X
- Transmission ‘Train stops’ from train to station via Rail2X

→ improved comfort
→ inexpensive communication
→ more efficient regional traffic

A hopping station increases communication range

SIEMENS
Ingenuity for life

Hopping station

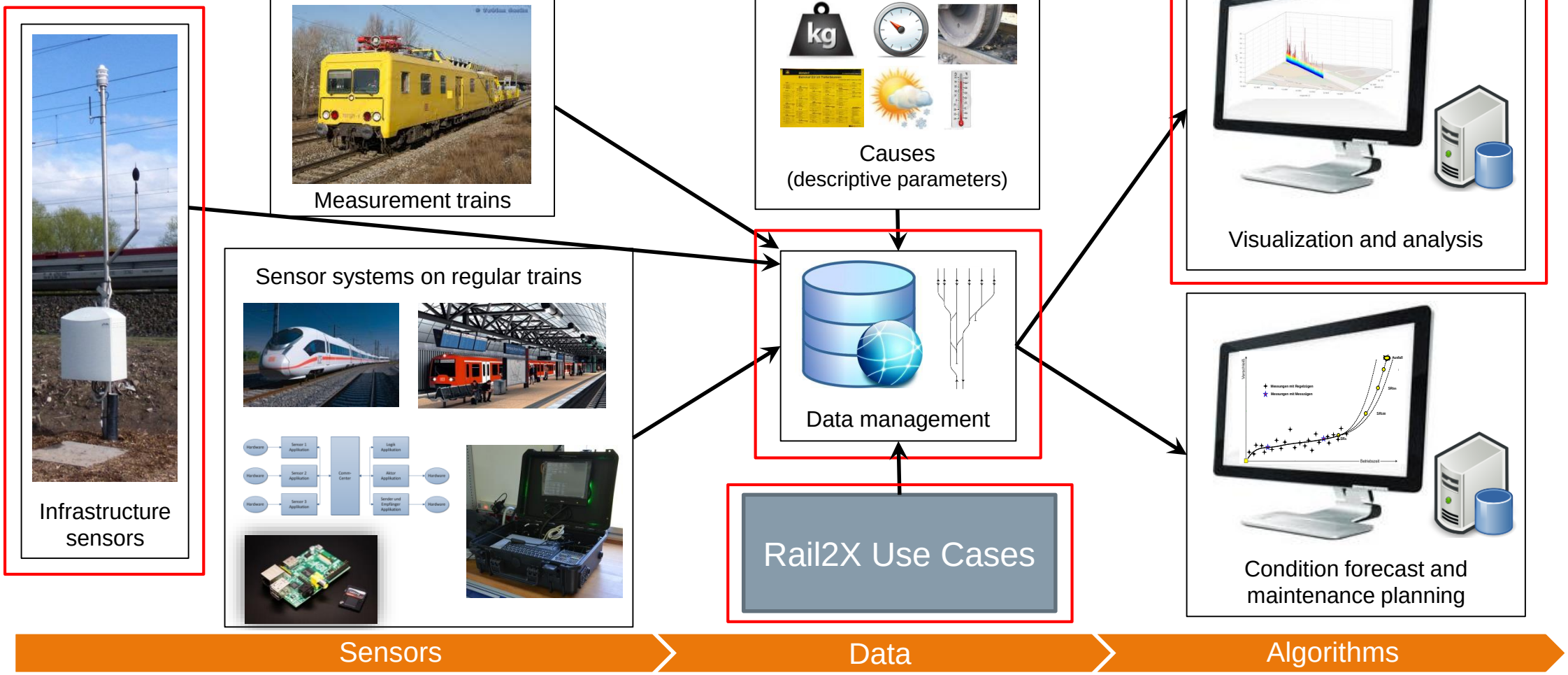
- Hopping station:
  forwards Rail2X messages
- Placement e.g. in curves without line of sight

→ increased communication range

Data shall be collected, analyzed and used for better maintenance among others

SIEMENS
Ingenuity for life

System environment with data server



SIEMENS
Ingenuity for life

ITS-G5 PKI

Security architecture of Vehicle2X communication

There exist different kinds of ITS messages which shall fulfill different security goals

SIEMENS
Ingenuity for life

Message models

Individual Public Messages (broadcast)

Authentication, authorization, integrity → All

Authentication, authorization, integrity, privacy → All

Individual Private Messages or Security Associations (unicast)

Authentication, authorization, integrity, confidentiality, (privacy) → Specific recipient

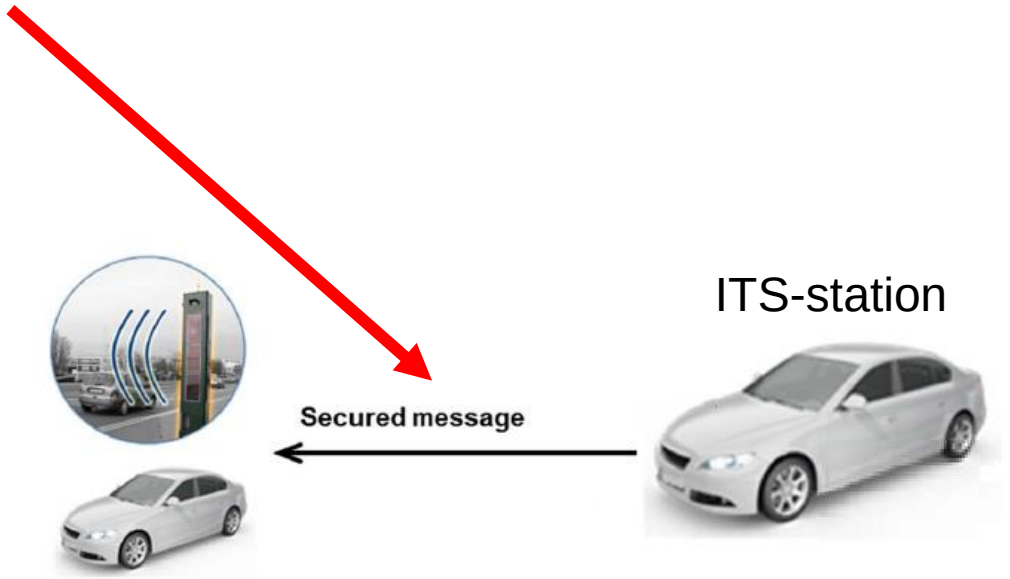
Security Association:
- Setting up of a secure communication channel
- Confidential communication

How to establish a secure communication between ITS-stations?

SIEMENS
Ingenuity for life

PKI architecture / C-ITS trust model

How to establish a secure communication between ITS-stations?

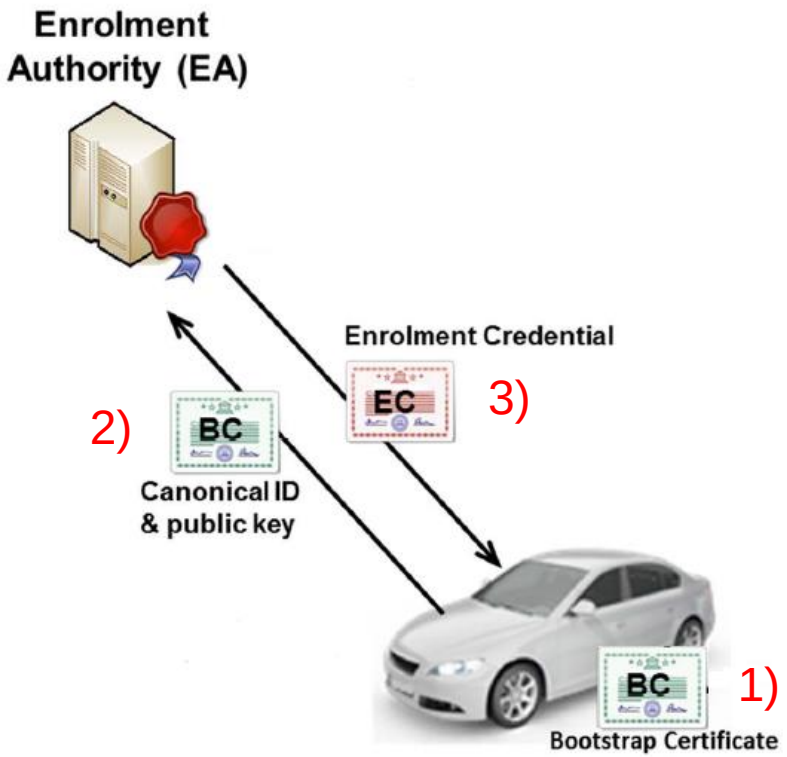


First the ITS-station registers with its predefined profile at the EA, to obtain eligibility

SIEMENS
Ingenuity for life

PKI architecture / C-ITS trust model

1) ITS-station obtains ID, keys and profile from manufacturer or operator, e.g. in form of a BC
2) ITS-station requests eligibility at EA with BC
3) After review EA issues general eligibility to participate at ITS in form of EC

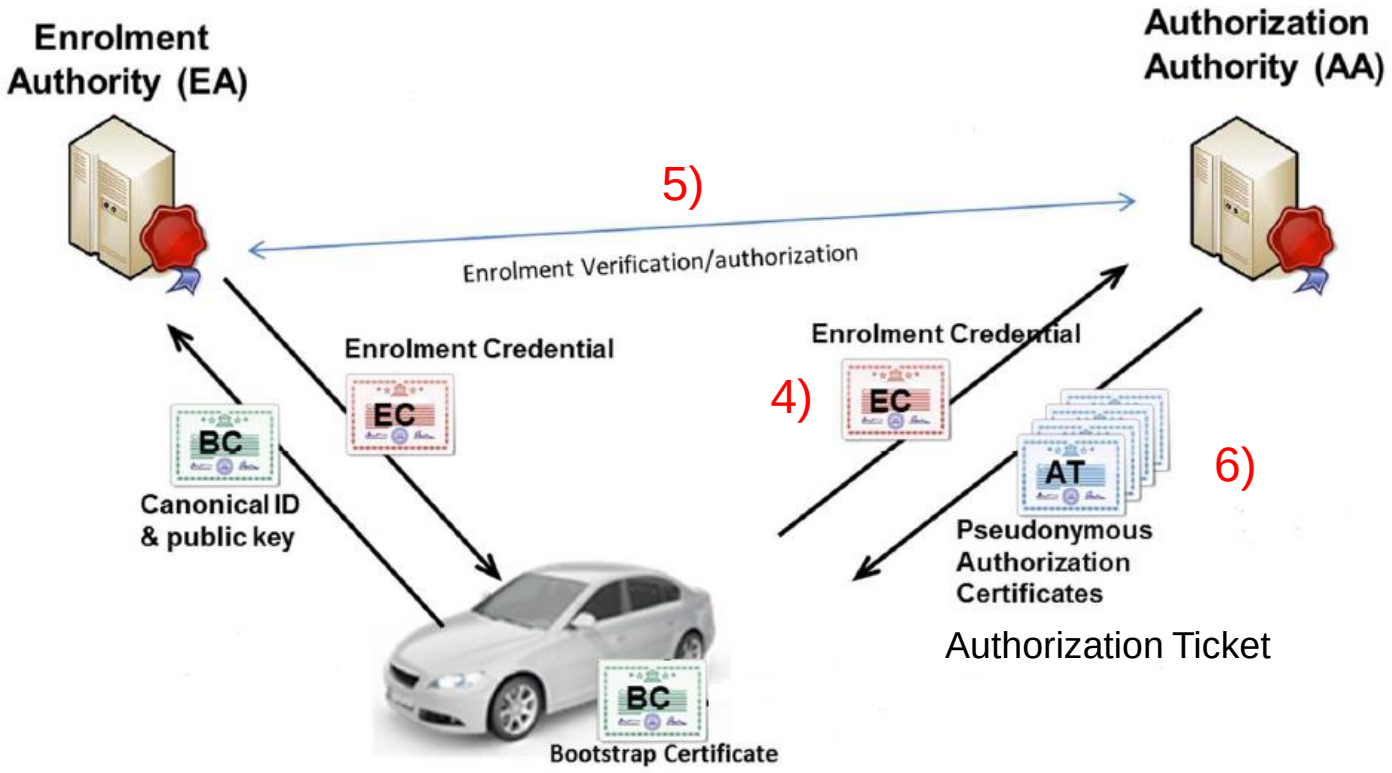


Then the ITS-station requests from the AA specific, pseudonymized authorizations

SIEMENS
Ingenuity for life

PKI architecture / C-ITS trust model

4) ITS-station requests specific authorizations at AA with EC
5) AA reviews EC via consultation with EA
(AA does not obtain true identity of ITS-station)
6) AA issues authorizations in form of ATs
(with data unknown to EA)

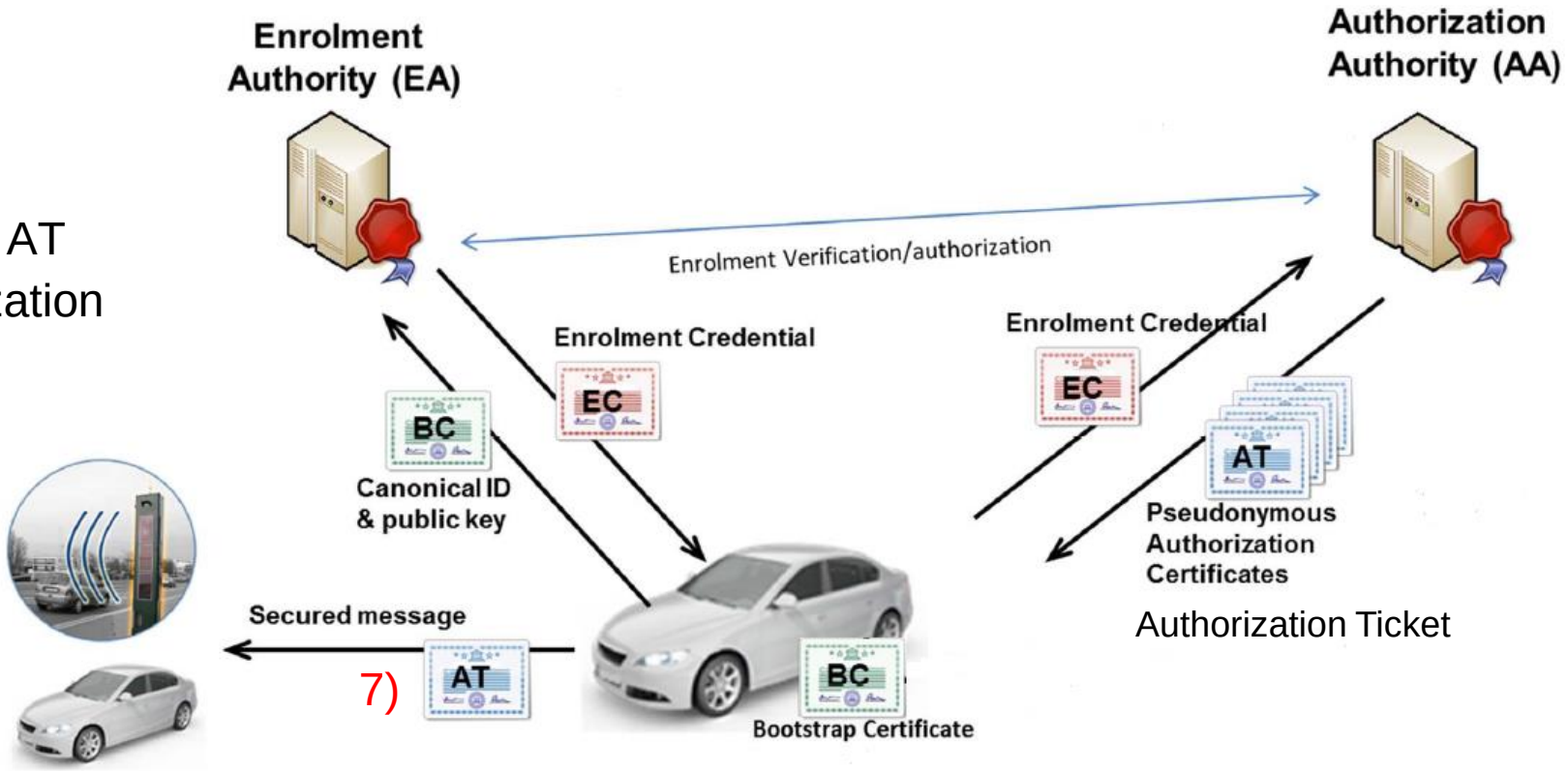


With authorizations communication is possible, in accordance with the principles authentication, authorization, privacy

SIEMENS
Ingenuity for life

PKI architecture / C-ITS trust model

7) ITS-station sends signed messages with corresponding AT for authentication and authorization



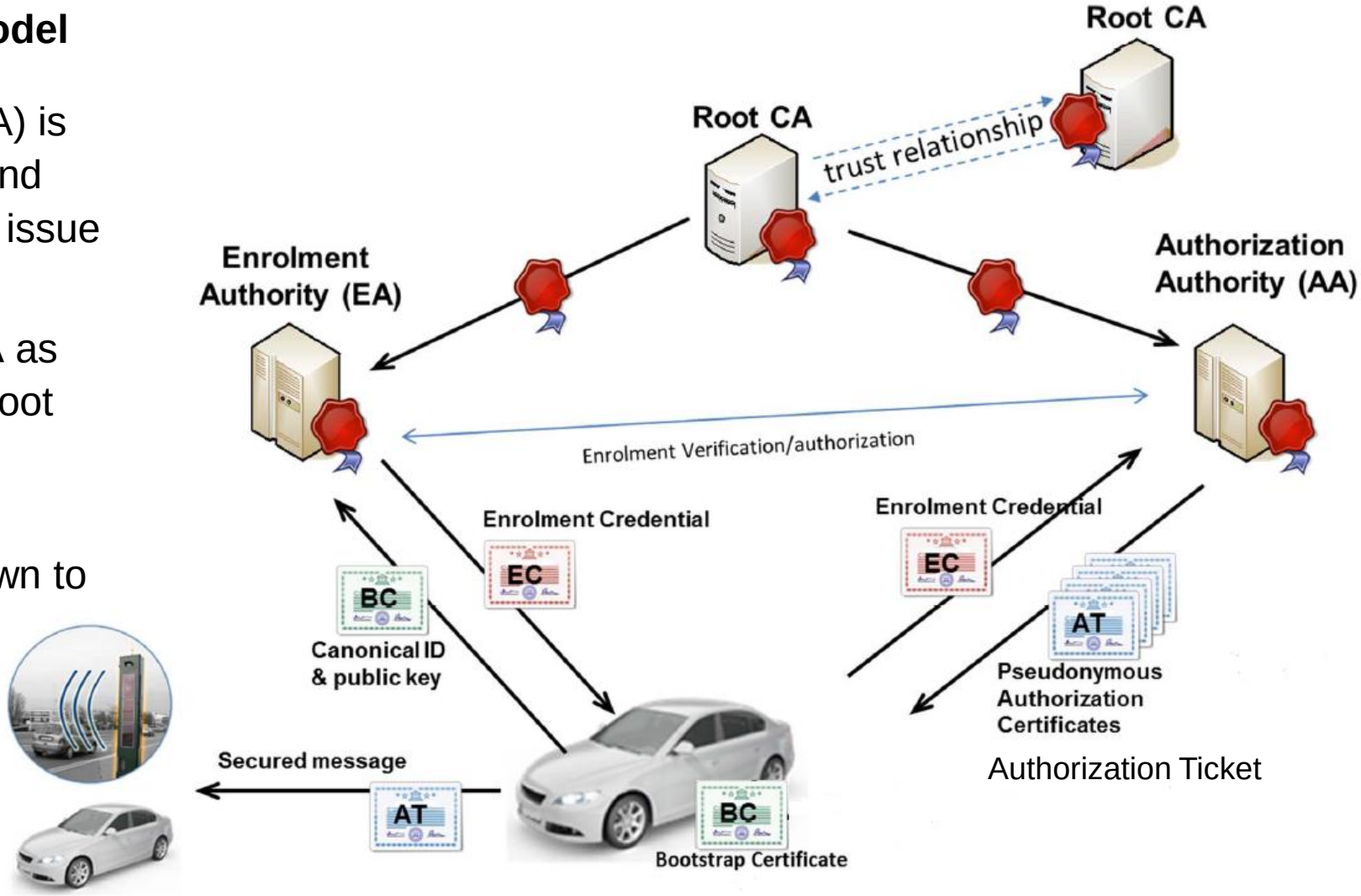
EAs and AAs obtain permission to issue certificates from a Root Certification Authority

SIEMENS
Ingenuity for life

PKI architecture / C-ITS trust model

- Root Certification Authority (CA) is highest certification authority and certifies that EAs and AAs can issue ECs or ATs resp.
- There can be a single Root CA as an absolute entity or several Root CAs which verify each other
- Concrete: set of Root CA certificates is in place and known to all. One can apply for a certificate.

From standard:
ETSI TS 102 940



SIEMENS
Ingenuity for life

ITS-G5 security

Security aspects of Vehicle2X communication

Security Services operate within the layers of the communication architecture, as well as across in the management

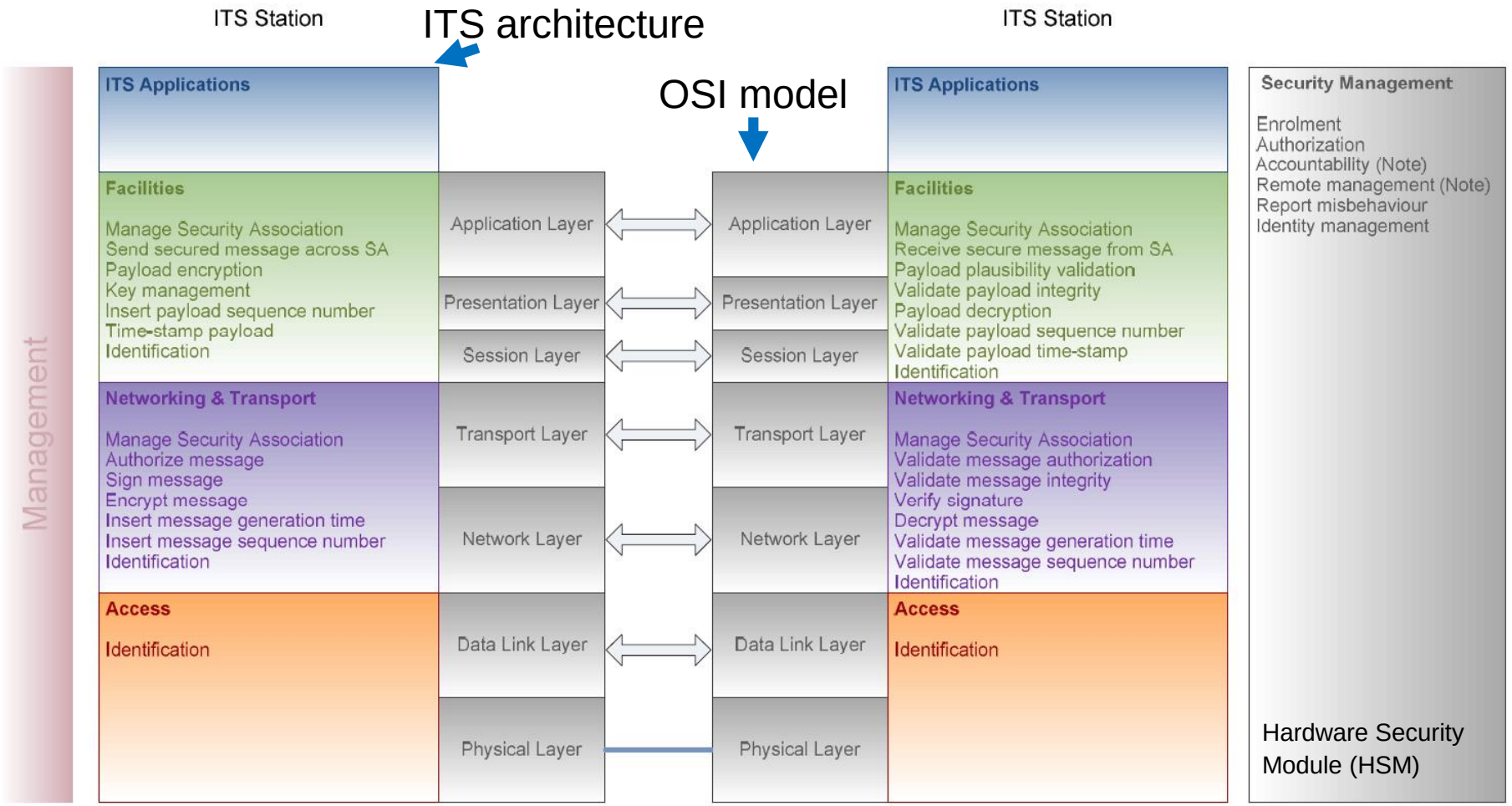
SIEMENS
Ingenuity for life

ITS security in communication architecture

Security Services offer

- Authentication
- Authorization
- Accountability
- Integrity
- Confidentiality
- Privacy
- Availability

From standard:
ETSI TS 102 940



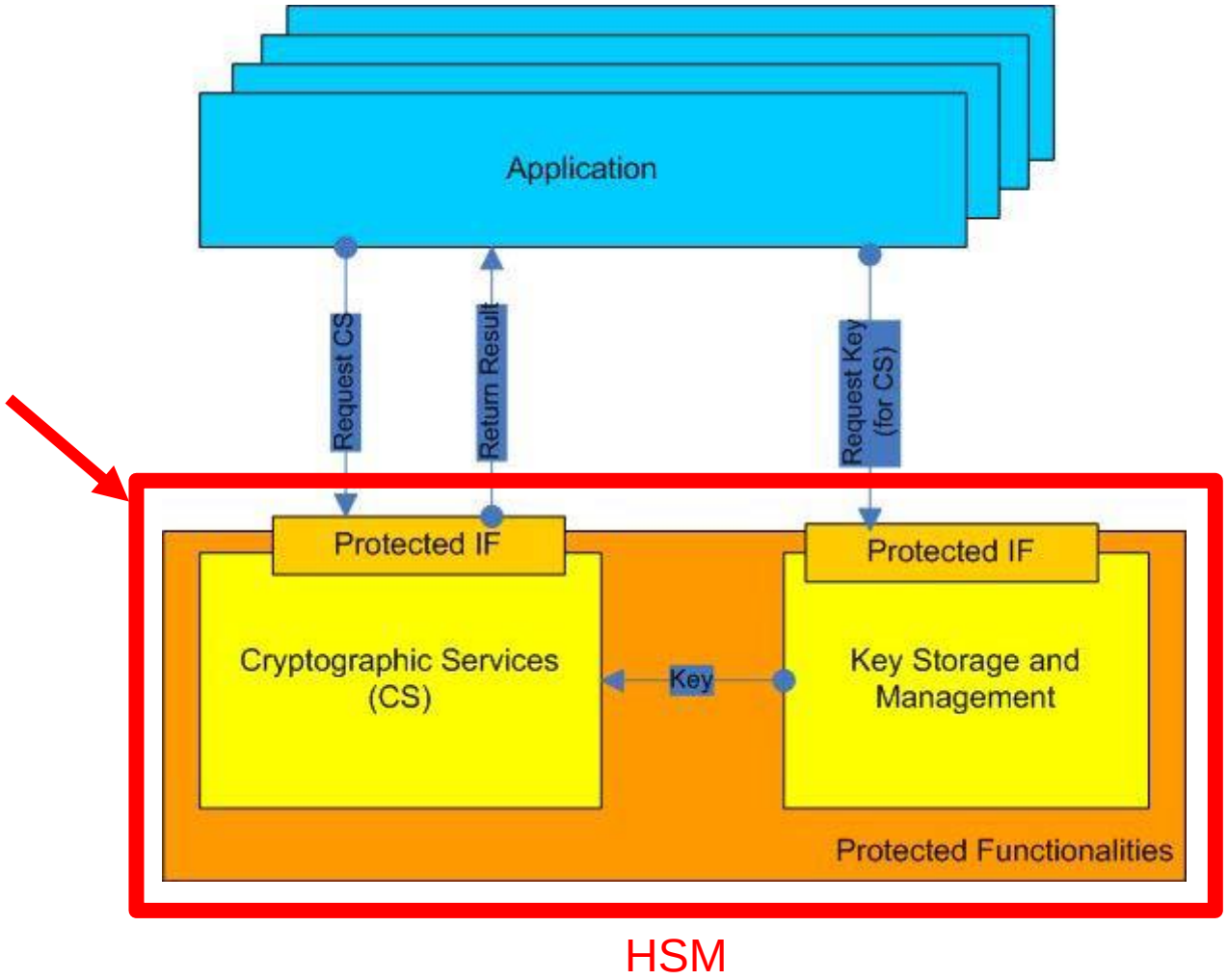
An HSM is responsible for communication encryption and PKI handling

SIEMENS
Ingenuity for life

Hardware Security Modul (HSM)

HSM:

- Secure saving of private keys
- Secure execution of cryptographic functions
- Access to sensible data / keys only with explicit permission and via protected interfaces
- Siemens ESCoS RSU has an HSM



From standard: ETSI TS 102 940

SIEMENS
Ingenuity for life

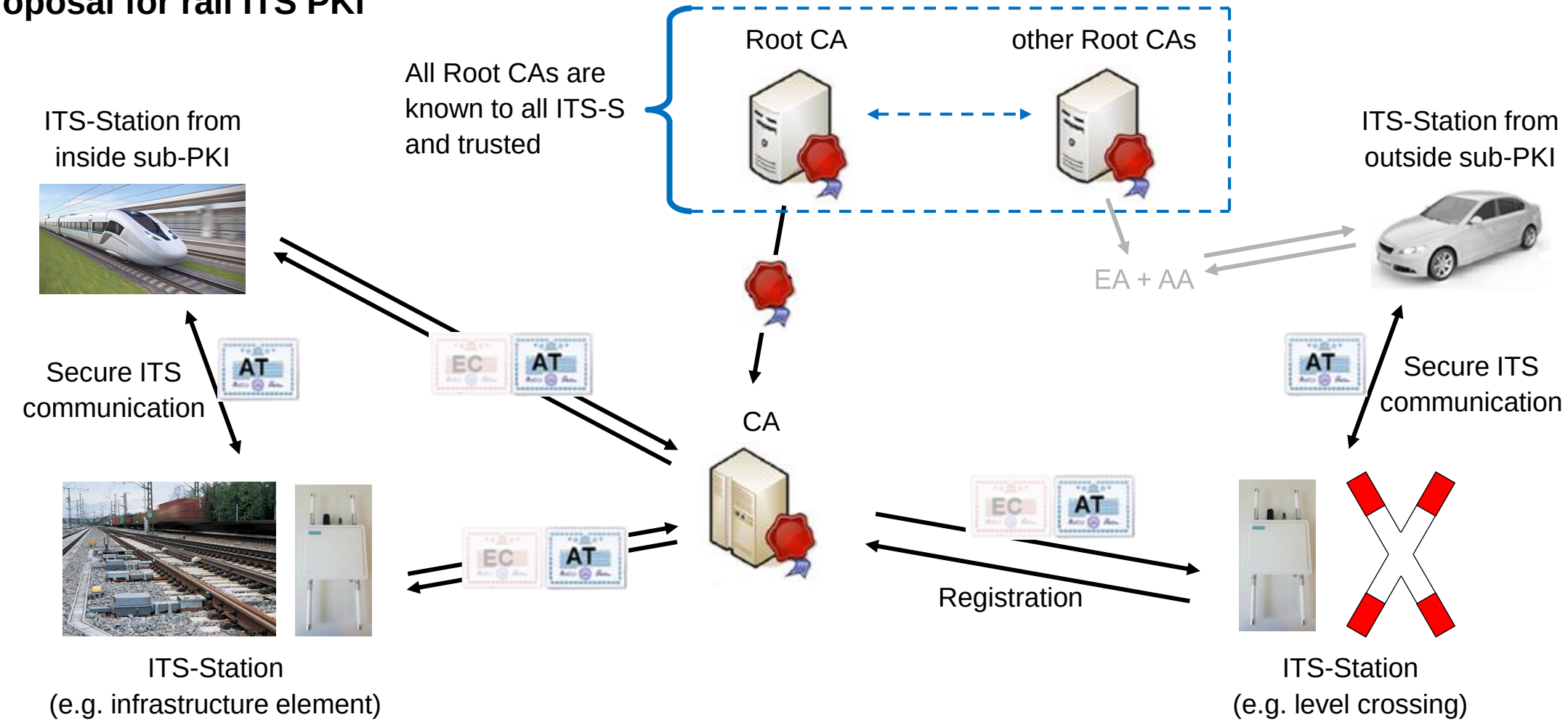
Rail ITS PKI

Structure of PKI for rail-specific ITS applications

A rail-specific sub-PKI as part of the whole ITS PKI is conceivable

SIEMENS
Ingenuity for life

Proposal for rail ITS PKI



Contacts

Dr. Slawa Lang
Siemens Mobility, MO MM R&D SYS SR

Telephone: +49 174 2634873
E-mail: slawa.lang@siemens.com

Prof. Dr. Jens Braband
Siemens Mobility, MO MM R&D SYS

Telephone: +49 173 6062831
E-mail: jens.braband@siemens.com

Ingo Schwarzer
DB Systel

Telephone: +49 30 29716370
E-mail: ingo.schwarzer@deutschebahn.com