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 und ITS Security

Slawa Lang, Siemens Mobility GmbH;
“Rail2X” Konsortium

Safety in Transportation 12, 2019

Wie sicher ist ein ITS-Kommunikationssystem und kann es auf den Schienenverkehr erweitert werden?

SIEMENS
Ingenuity for life

Rail2X?

Inhaltsverzeichnis

C-ITS

Intelligent Transportation Systems

www.siemens.com/mobility

ITS sollen den (Straßen)verkehr sicherer, umweltfreundlicher, effizienter und komfortabler machen

SIEMENS
Ingenuity for life

Intelligent Transportation Systems (ITS)

Essentiell für ITS ist Kommunikation:

Verkehrsteilnehmer ↔ andere Teilnehmer

Verkehrsteilnehmer ↔ Infrastruktur

→ Cooperative-ITS (C-ITS)

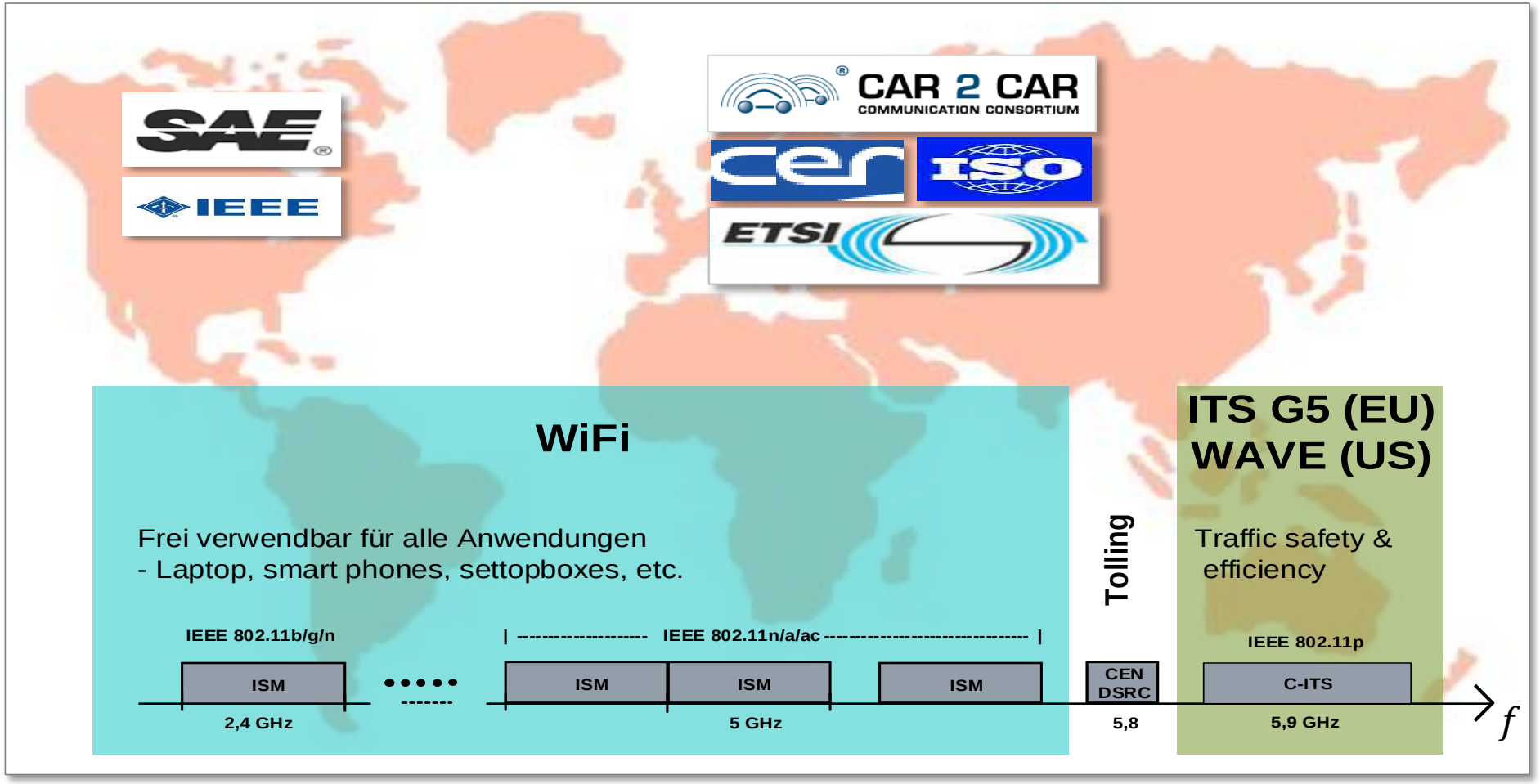
Im Straßenverkehr:

Car2X, Car2Car Kommunikation

Vehicle2X verwendet spezielles Wi-Fi, aber 5G Mobilfunk kann auch verwendet werden

SIEMENS
Ingenuity for life

Vehicle2X – Standardisierung, Frequenzzuweisung



SIEMENS
Ingenuity for life

Rail2X

Vehicle2X-Technologie im Bahnverkehr

 www.siemens.com/mobility

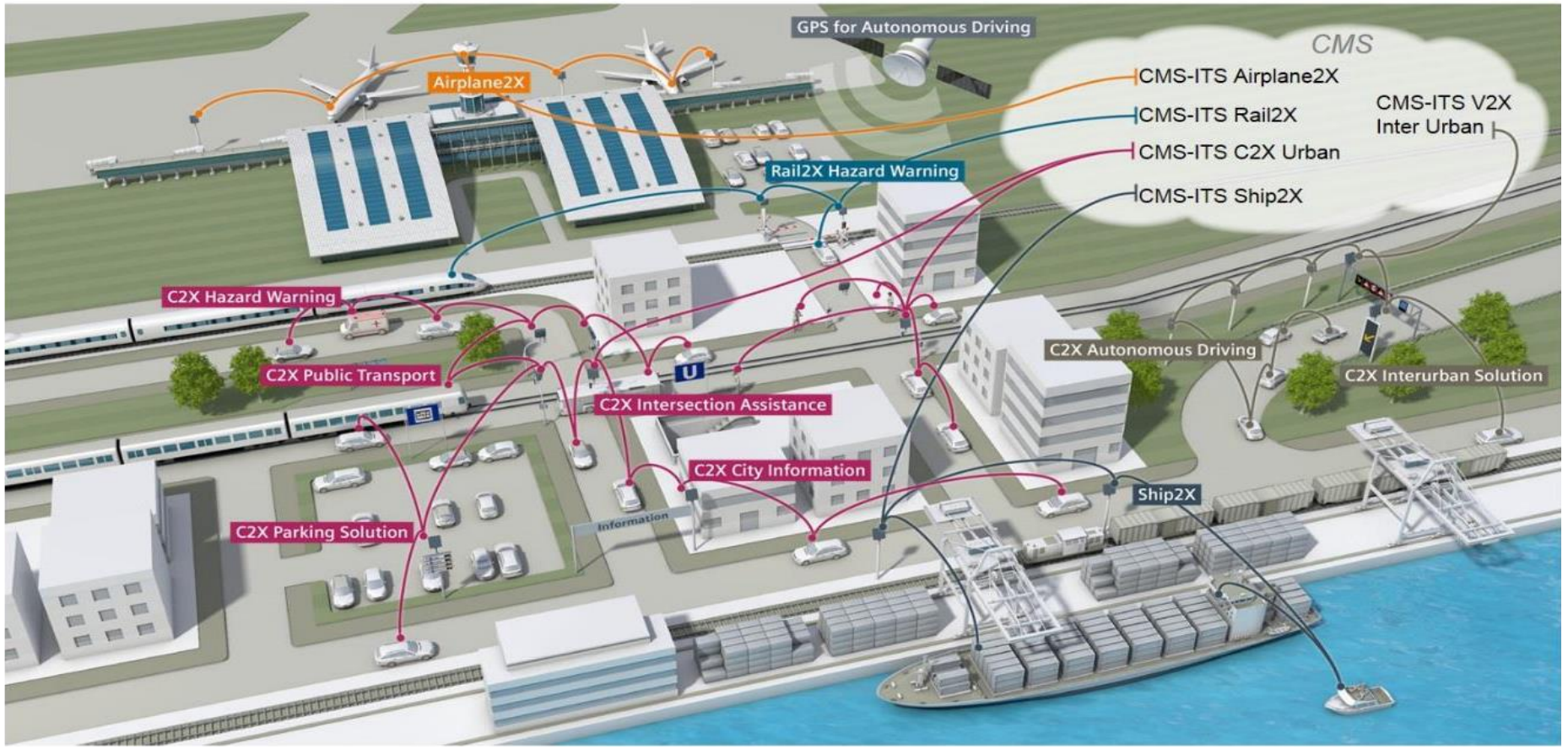
Straßen-ITS soll auf Schienenverkehr adaptiert werden, um effiziente Services zu ermöglichen

SIEMENS
Ingenuity for life

Rail2X – Smart Services

Adaption der Wi-Fi Car2X-Kommunikation auf Schienenverkehr / für Schienen-ITS

- → erhöhte Sicherheit
- → verbesserter Komfort
- → effizientere Instandhaltung
- → Kostensenkungen

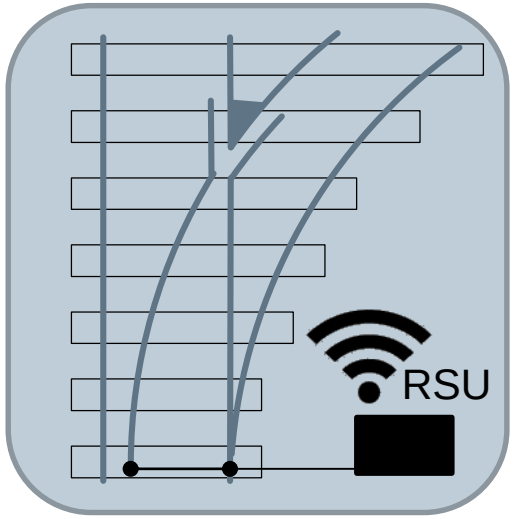


Machbarkeit und Sinnhaftigkeit werden anhand von 3 Use Cases bei der Erzgebirgsbahn demonstriert

SIEMENS
Ingenuity for life

Rail2X – Use Cases

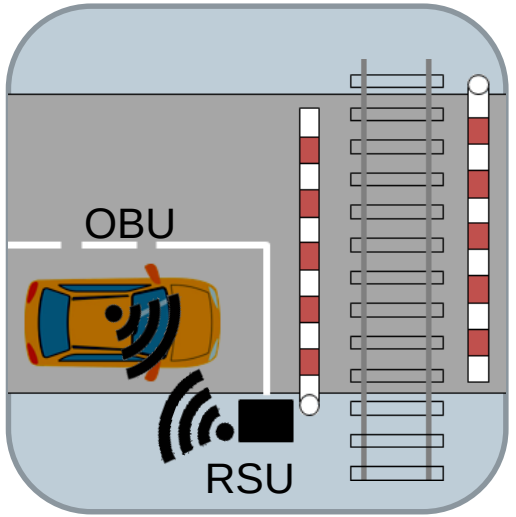
1: Service und Diagnose



Datenaustausch
Infrastruktur ↔ Zug

→ preiswerte Datenerfassung
→ effizientere Instandhaltung

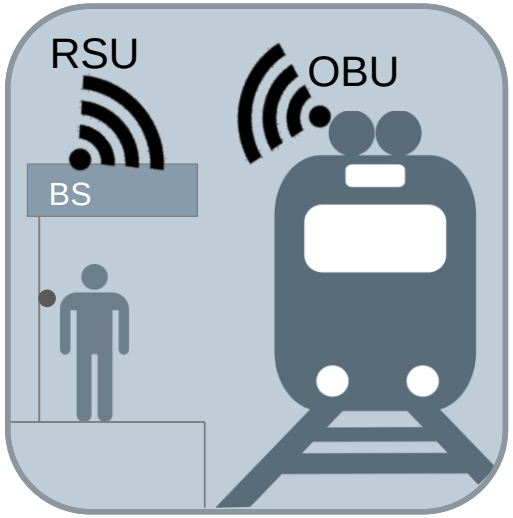
2: Anrufschranke



Informationsaustausch
Kfz ↔ Bahnübergang

→ erhöhte Sicherheit
→ verbesserter Komfort

3: Bedarfshalt



Informationsaustausch
Zug ↔ Station

→ preiswerte Kommunikation
→ effizienterer Regionalverkehr

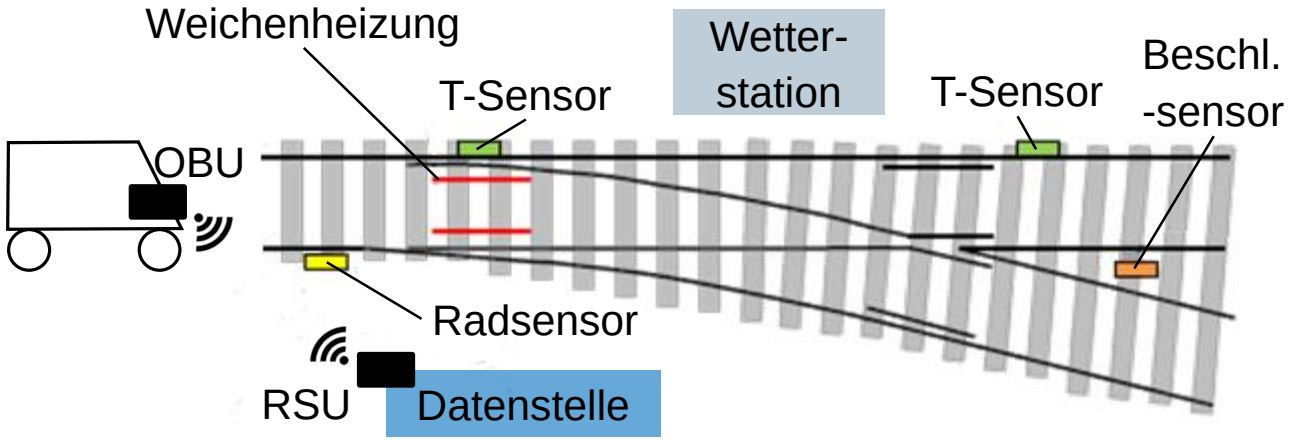
Daten können kostengünstig gesammelt und zentral analysiert werden

Use Case 1: Service und Diagnose

- Sammeln von (Sensor)daten an wichtigen Infrastrukturpunkten (z. B. Weichen)
- Einsammeln der Daten durch vorbeifahrende Züge mit Rail2X
- Weitergabe der Daten an zentrale Server z. B. im Depot
- Speicherung und Analyse der Daten an zentraler Stelle

→ preiswerte Datenerfassung ohne dauerhafte Kommunikationsverbindung

→ effizientere Instandhaltung



Konzept der Anrufschranke bleibt erhalten durch effizientere An- und Abmeldung

SIEMENS
Ingenuity for life

Use Case 2: Anrufschranke

- Anrufschranke:
  normalerweise geschlossen, öffnet bei Anmeldung (wenn sicher)
- Verkehrsteilnehmer ohne Vehicle2X:
  manuelle An- und Abmeldung wie gehabt
- Verkehrsteilnehmer mit Vehicle2X:
  automatische An- und Abmeldung durch Kommunikation mit Bahnübergang; Anzeige der Rückmeldung

→ verbesserter Komfort
→ verkürzte Wartezeiten
→ erhöhte Sicherheit

Regionalverkehr wird effizient durch preiswerte und komfortable Bedarfshalte

SIEMENS
Ingenuity for life

Use Case 3: Bedarfshalt

- Bedarfshalt:
  Zug hält nur bei Haltewunsch eines Passagiers im Zug oder an Haltestelle
- Übertragung Haltewunsch an Haltestelle → Zug durch Rail2X
- Übertragung ‚Zug hält' von Zug an Haltestelle durch Rail2X

→ verbesserter Komfort
→ preiswerte Kommunikation
→ effizienterer Regionalverkehr

Eine Hopping-Station erweitert die Kommunikationsreichweite

SIEMENS
Ingenuity for life

Hopping-Station

- Hopping-Station:
  leitet Rail2X-Nachrichten weiter
- Platzierung z. B. in Kurven ohne Sichtverbindung

→ erhöhte Kommunikationsreichweite

Daten sollen gesammelt, analysiert und u. a. für bessere Instandhaltung verwendet werden

SIEMENS
Ingenuity for life

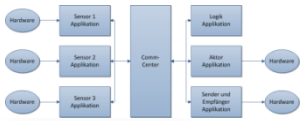
Systemumgebung mit Datenserver

Infrastruktur-sensoren

Messzüge

Ursachen
(beschreibende Parameter)

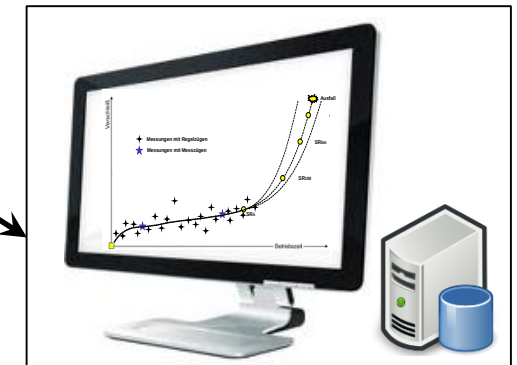
Sensorsysteme auf Regelzügen



Datenmanagement

Rail2X Use Cases

Visualisierung und Analyse



Zustandsprognose und Instandhaltungsplanung

Sensoren → Daten → Algorithmen

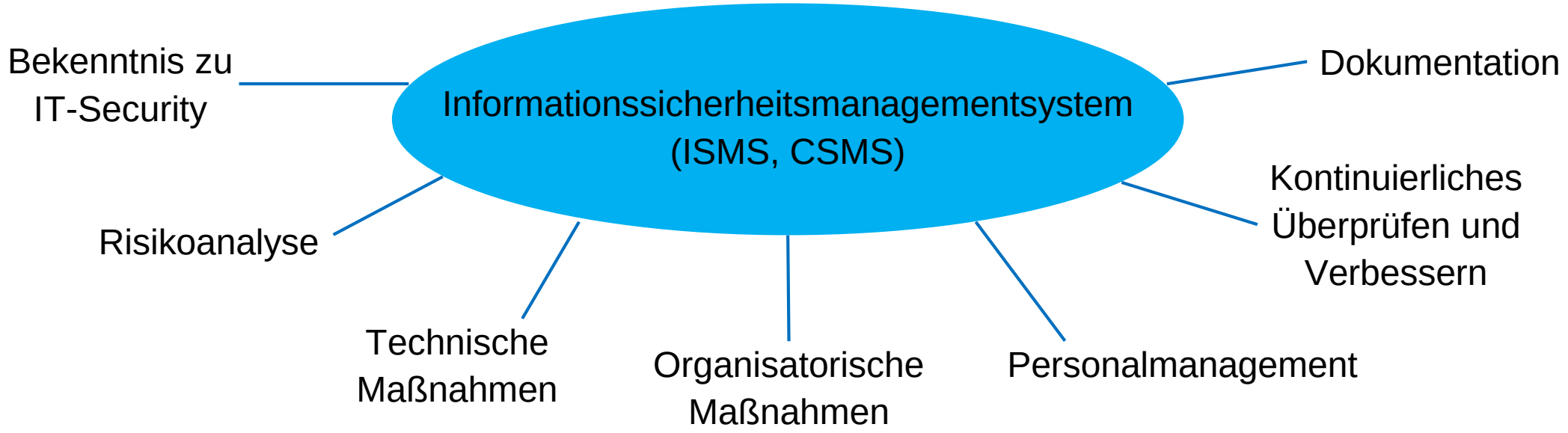
IT-Security Standards

Allgemeines

Ein ISMS umfasst alle Tätigkeiten, um IT-Security einzuführen und am Laufen zu halten

SIEMENS
Ingenuity for life

Informationssicherheitsmanagementsystem (ISMS)



In Standards: IEC 62443-2-1, ISO/IEC 27001, BSI-Standard 200-1

SIEMENS
Ingenuity for life

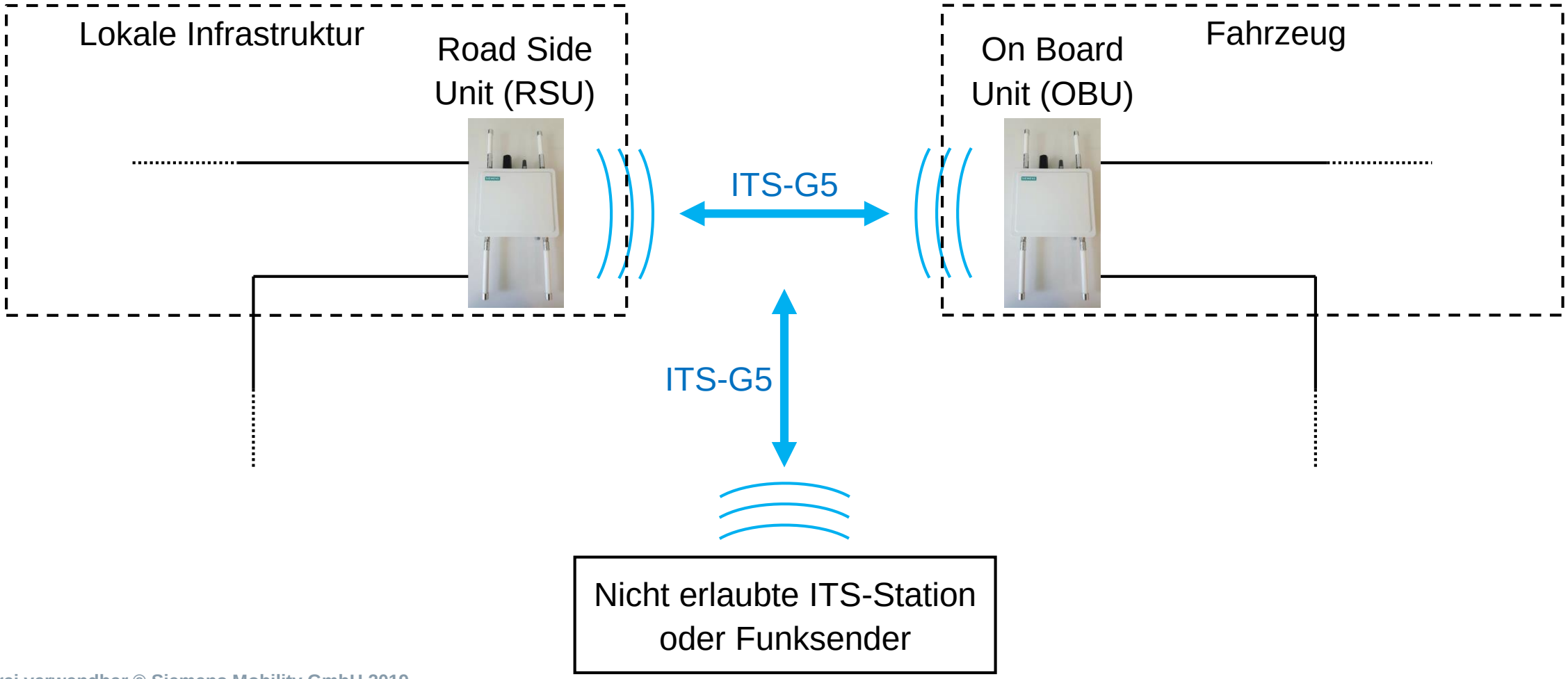
ITS-G5 Security

Allgemeines

Wie sicher ist ein ITS-Kommunikationssystem?

SIEMENS
Ingenuity for life

ITS-Kommunikationssystem



Ein besonderes Risiko ist eine falsche Abmeldung vom Bahnübergang, da sie zu einer gefährlichen Schließung führen kann

SIEMENS
Ingenuity for life

Rail2X-spezifische Risiken

	Risiko	Auswirkungen	Bemerkungen
UC 1	Angreifer verhindert Senden von Diagnosedaten oder verfälscht diese	Service findet nicht rechtzeitig statt oder rückt fälschlicherweise aus	
UC 2	Angreifer meldet fälschlicherweise Fahrzeug am Bahnübergang an	Bahnübergang wird unnötig geöffnet	keine Gefahr für Safety
UC 2	Angreifer meldet fälschlicherweise, Fahrzeug hat Bahnübergang verlassen (bei indirektem Abmelden über Position muss Angreifer falsche Position senden und wahre Positionsmeldungen unterdrücken)	Bahnübergang schließt mit oder ohne vorherige Warnung, selbst wenn Fahrzeug Gefahrenbereich noch nicht verlassen hat	ohne Warnung besteht Gefahr für Safety; mit Warnung selbe Gefahr wie für nicht ITS-Teilnehmer
UC 3	Angreifer meldet fälschlicherweise Haltewunsch oder verhindert das Senden desjenigen	Zug hält unnötig an oder fährt an Station vorbei ohne zu halten	Vorbeifahren, obwohl Fahrgäste mitfahren wollen, ist ein gravierender Service-Mangel

Es existieren verschiedene Arten von ITS-Nachrichten, die verschiedene Schutzziele erfüllen müssen

SIEMENS
Ingenuity for life

Nachrichten Modelle

Individual Public Messages (broadcast)

Authentifikation, Autorisierung, Integrität → All

Authentifikation, Autorisierung, Integrität, Privatsphäre → All

Individual Private Messages or Security Associations (unicast)

Authentifikation, Autorisierung, Integrität, Vertraulichkeit, (Privatsphäre) → Specific recipient

Security Association:
- Aufbau eines sicheren Kommunikationskanals
- Vertrauliche Kommunikation

SIEMENS
Ingenuity for life

ITS-G5 PKI

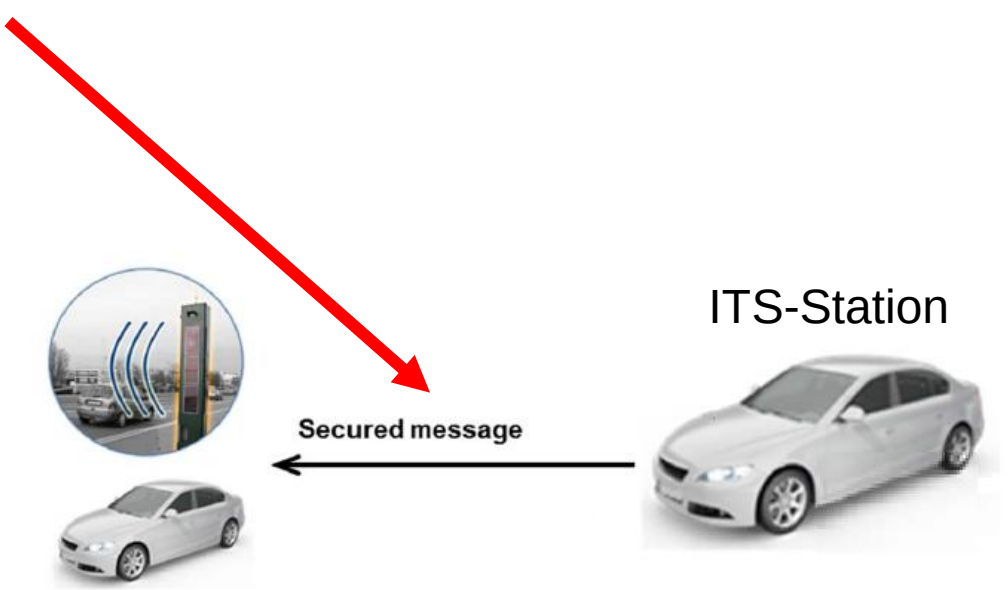
Sicherheitsarchitektur der Vehicle2X Kommunikation

Wie stellt man eine sichere Kommunikation zwischen ITS-Stationen her?

SIEMENS
Ingenuity for life

PKI Architektur / C-ITS Trust Model

Wie stellt man eine sichere Kommunikation zwischen ITS-Stationen her?

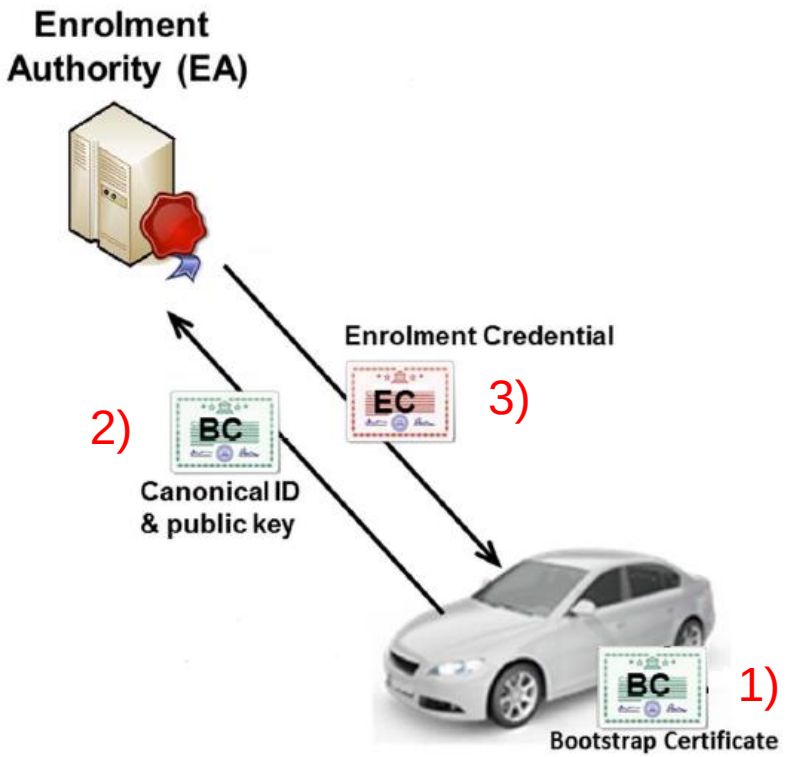


Zuerst meldet sich die ITS-Station mit ihrem vorgegebenen Profil bei der EA an, um Teilnahmeberechtigung zu erhalten

SIEMENS
Ingenuity for life

PKI Architektur / C-ITS Trust Model

1) ITS-Station erhält ID, Schlüssel und Profil vom Hersteller oder Betreiber, z. B. in Form von BC
2) ITS-Station erfragt Teilnahme-berechtigung bei EA mit BC
3) Nach Prüfung erteilt EA generelle Berechtigung zur Teilnahme an ITS in Form von EC

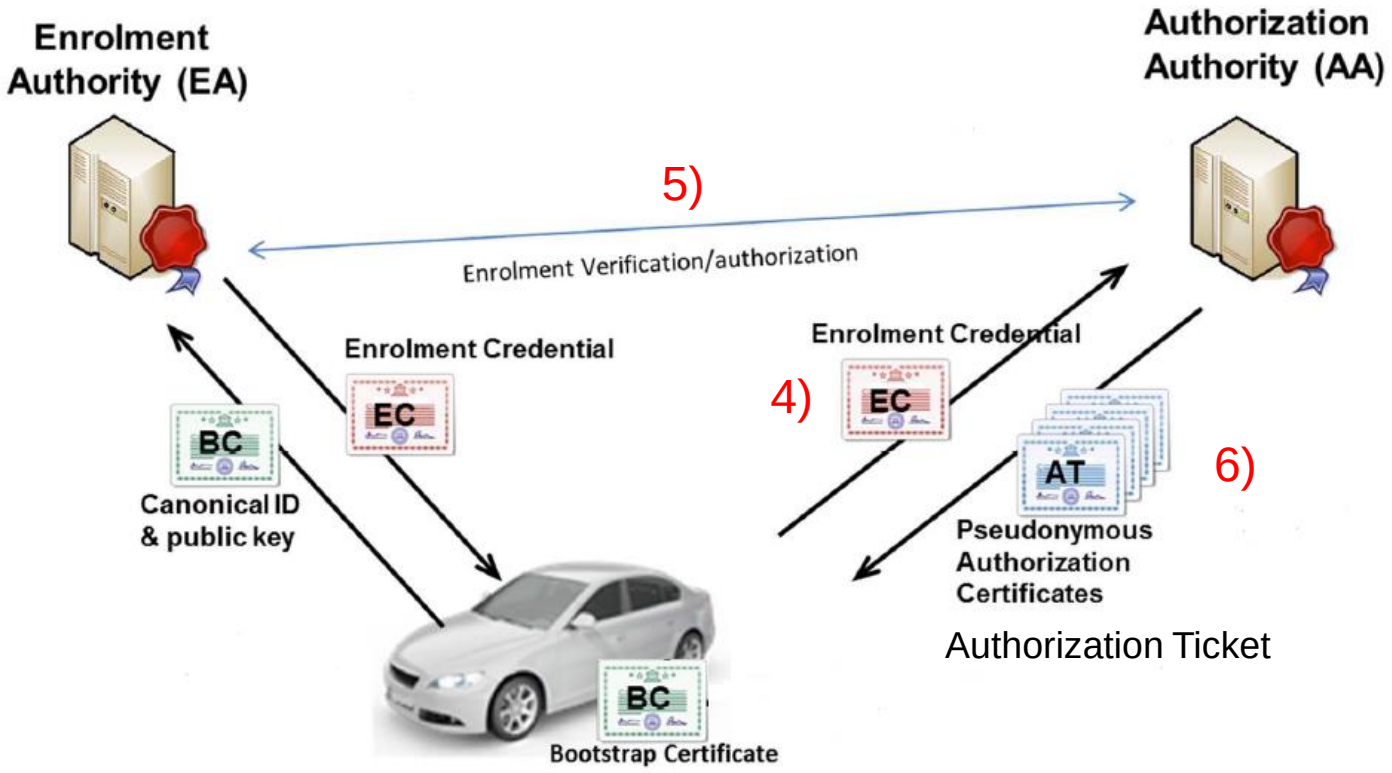


Dann erfragt die ITS-Station von der AA konkrete, pseudonymisierte Autorisierungen

SIEMENS
Ingenuity for life

PKI Architektur / C-ITS Trust Model

4) ITS-Station erfragt konkrete Autorisierungen bei AA mit EC
5) AA überprüft EC durch Rücksprache mit EA
(AA erhält die wahre Identität der ITS-Station nicht)
6) AA erteilt Autorisierungen in Form von ATs
(mit der EA unbekannten Daten)

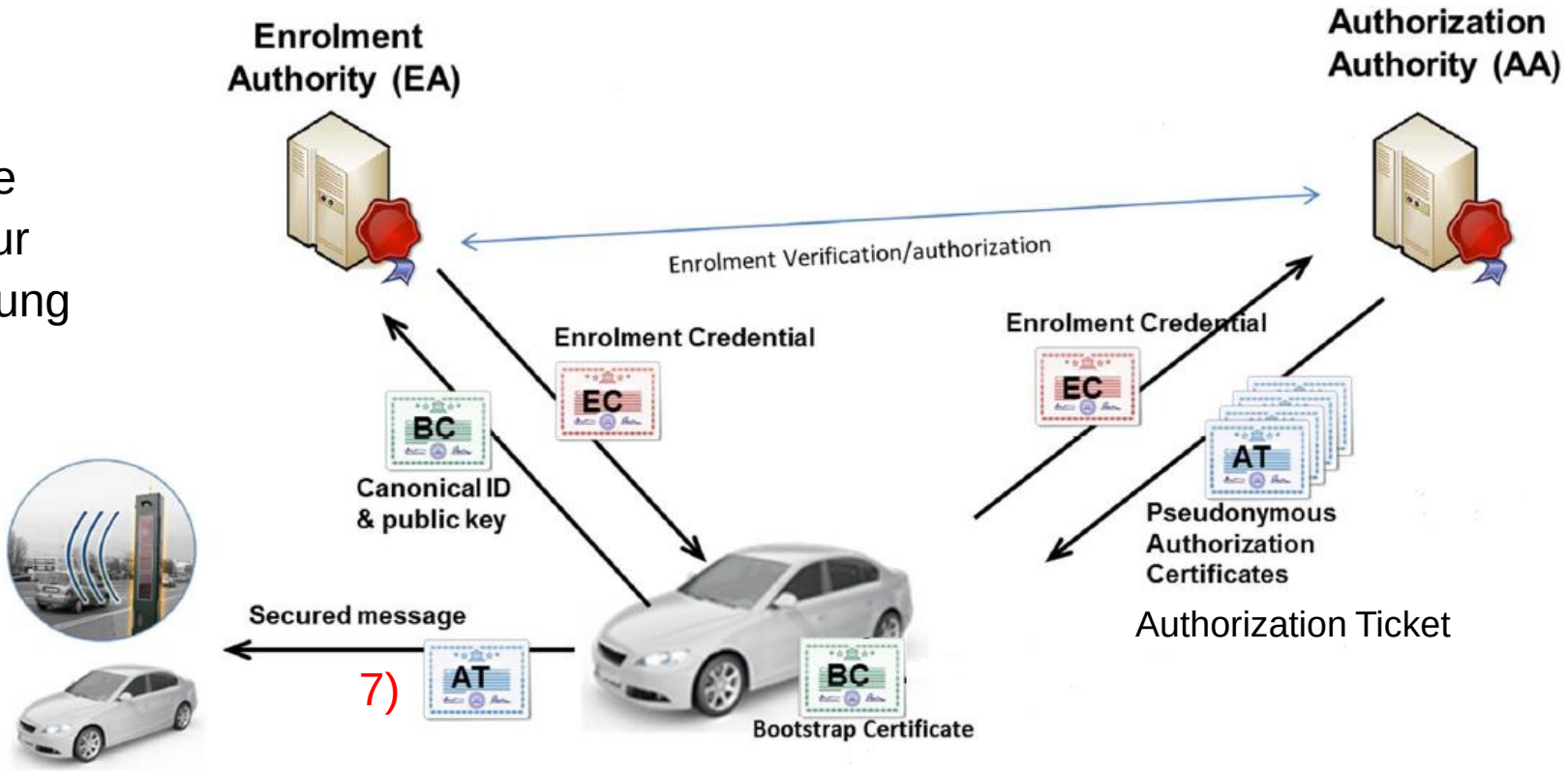


Mit Autorisierungen kann kommuniziert werden, unter Einhaltung der Prinzipien Authentifikation, Autorisierung, Privatsphäre

SIEMENS
Ingenuity for life

PKI Architektur / C-ITS Trust Model

7) ITS-Station versendet signierte Nachricht mit passender AT zur Authentifikation und Autorisierung



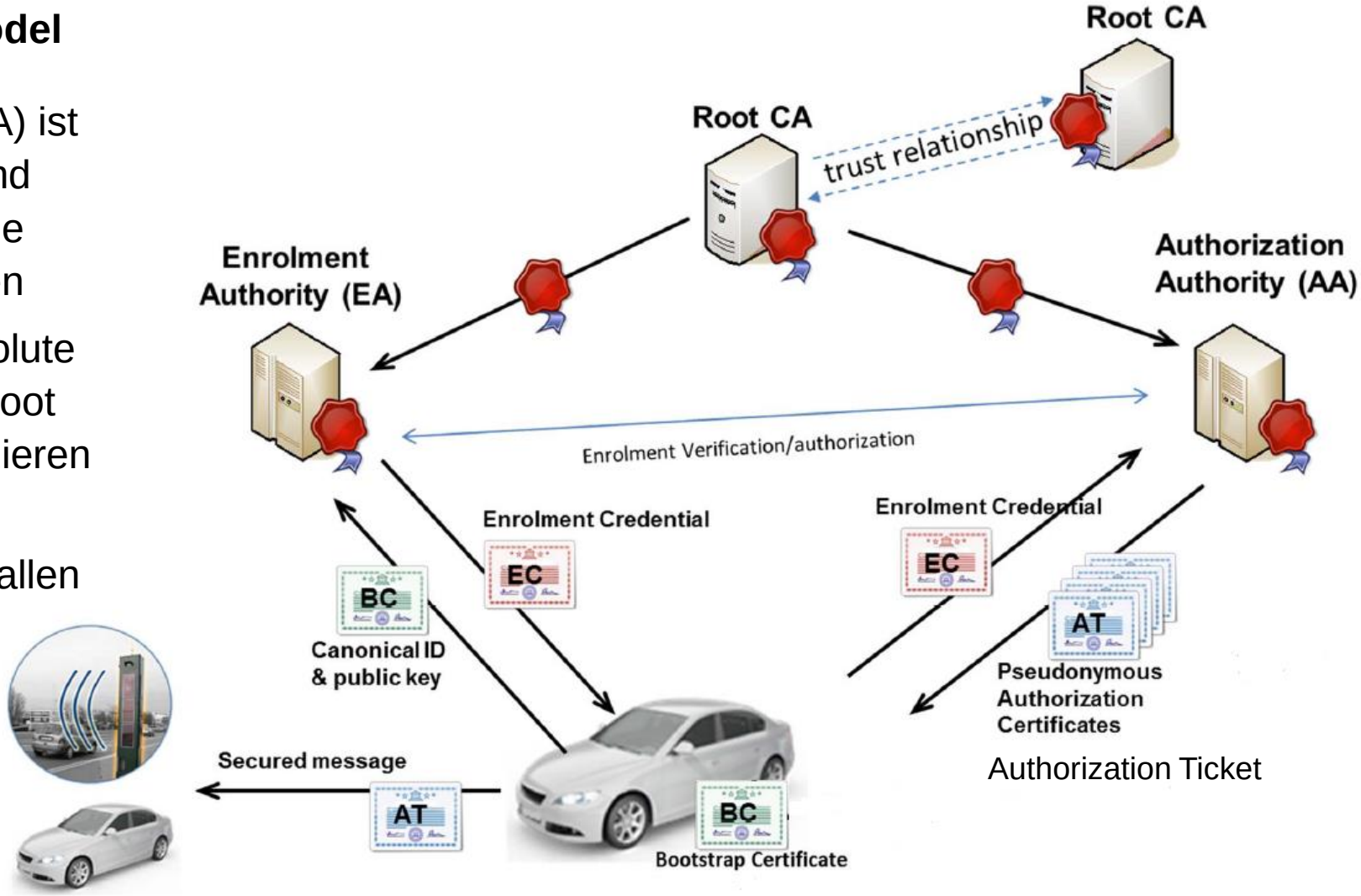
EAs und AAs erhalten Erlaubnis zur Vergabe von Zertifikaten von einer Root Certification Authority

SIEMENS
Ingenuity for life

PKI Architektur / C-ITS Trust Model

- Root Certification Authority (CA) ist höchste Zertifizierungsstelle und bestätigt EAs und AAs, dass sie ECs bzw. ATs ausstellen dürfen
- Es kann eine Root CA als absolute Instanz geben oder mehrere Root CA, die sich gegenseitig verifizieren
- Konkret: Menge an Root CA Zertifikaten ist vorhanden und allen bekannt. Man kann sich um Zertifikat bewerben.

Aus Standard:
ETSI TS 102 940



SIEMENS
Ingenuity for life

ITS-G5 Security

Sicherheitsaspekte der Vehicle2X Kommunikation

Security Services arbeiten innerhalb der Schichten der Kommunikationsarchitektur, sowie übergreifend im Management

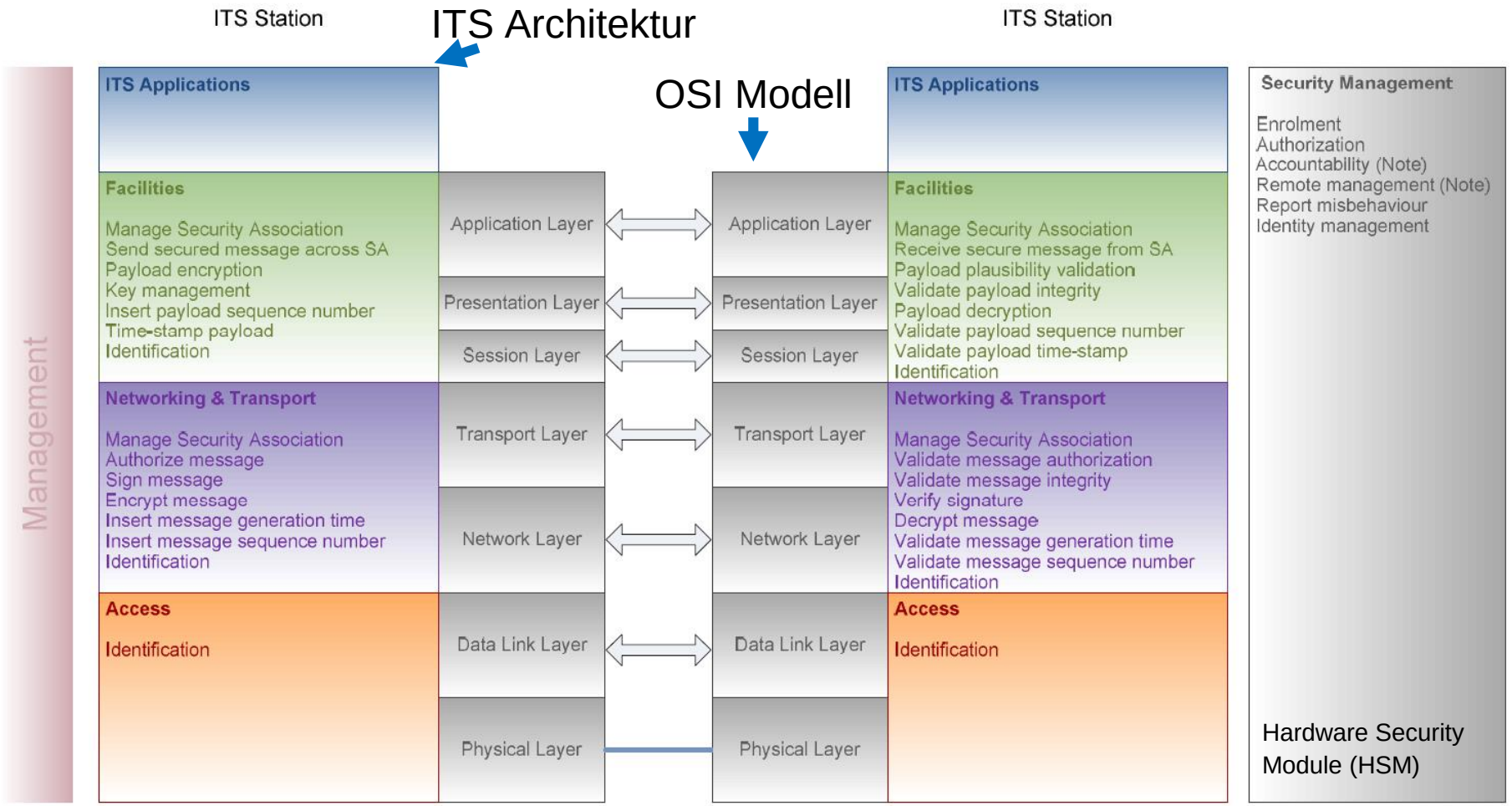
SIEMENS
Ingenuity for life

ITS Security in Kommunikationsarchitektur

Security Services bieten

- Authentifikation
- Autorisierung
- Rechenschaft (Accountability)
- Integrität
- Vertraulichkeit (Confidentiality)
- Privatsphäre
- Verfügbarkeit (Availability)

Aus Standard:
ETSI TS 102 940



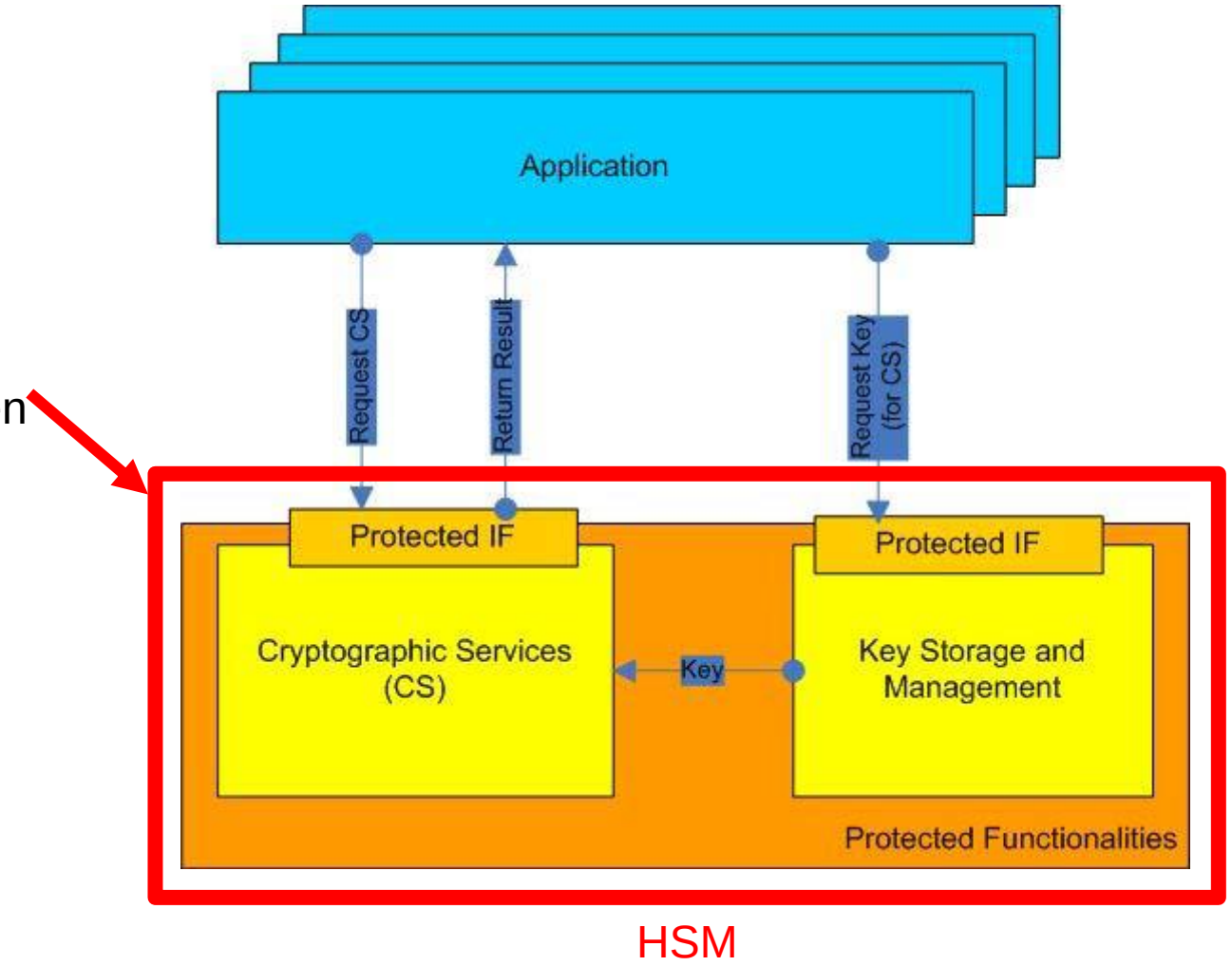
Das HSM ist für Kommunikationsverschlüsselung und PKI Handling zuständig

SIEMENS
Ingenuity for life

Hardware Security Modul (HSM)

HSM:

- Sicheres Speichern von privaten Schlüsseln
- Sicheres Ausführen kryptographischer Funktionen
- Zugang zu sensiblen Daten / Schlüsseln nur mit expliziter Genehmigung und über geschützte Schnittstellen
- Siemens ESCoS RSU besitzt ein HSM



Aus Standard: ETSI TS 102 940

Schienen-ITS-PKI

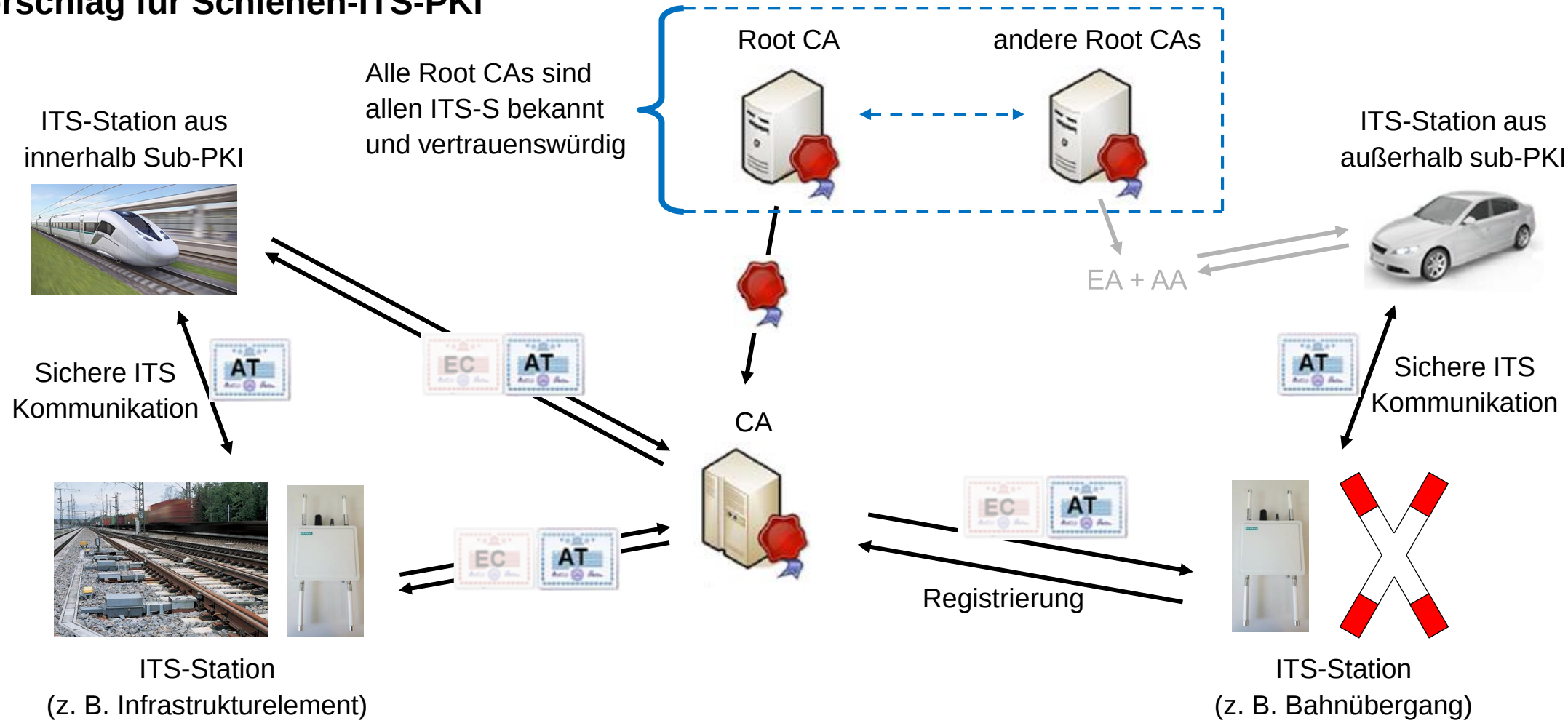
Aufbau einer PKI für bahnspezifische ITS-Anwendungen

www.siemens.com/mobility

Eine bahnspezifische Sub-PKI als Teil der gesamten ITS-PKI ist denkbar

SIEMENS
Ingenuity for life

Vorschlag für Schienen-ITS-PKI



Danke für die Aufmerksamkeit.

Fragen?

Kontakte

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

Telefon: +49 174 2634873
E-Mail: slawa.lang@siemens.com

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

Telefon: +49 173 6062831
E-Mail: jens.braband@siemens.com

Ingo Schwarzer
DB Systel

Telefon: +49 30 29716370
E-Mail: ingo.schwarzer@deutschebahn.com