IT-Sicherheit in der Car-to-X Kommunikation

Secure and Privacy Aware Wireless Car-to-X Communication

Norbert Bißmeyer

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

IHK Offenbach

29.11.2012

CASED

Fraunhofer SIT

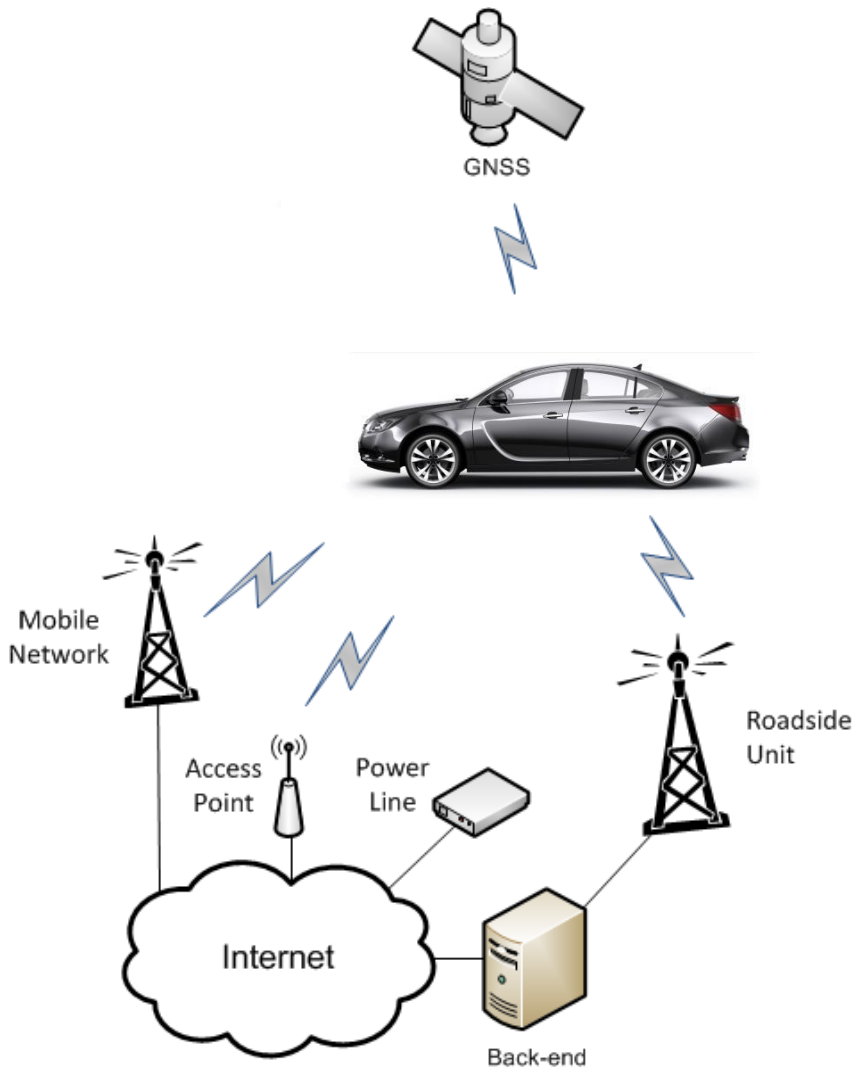
Inhalt

- Motivation
- Das Projekt sim^{TD}
- C2X Kommunikation
- IT-Sicherheit und Privatsphärenschutz in der C2X Kommunikation
- Evaluierungsstrategie bezüglich IT-Sicherheit und Privatsphärenschutz
- Zusammenfassung und Ausblick

Motivation

Vision der C2X Kommunikation

- Verkehrshindernisse wahrnehmen, bevor man sie sieht.
- Gefahren erkennen, bevor sie zur Bedrohung werden.
- Schnell, sicher und entspannt ans Ziel kommen.
- Rechtzeitig auf akute Verkehrssituationen reagieren.
- Just-in-time Kommunikation zwischen Fahrzeugen untereinander sowie Verkehrs-teilnehmern und den Verkehrszentralen nutzen.
- Verkehrsmanagement durch hochaktuelle Ist-Verkehrsdaten optimieren.



Motivation | Ziele

Verkehr

Erfassung der Verkehrslage und ergänzender Informationen / Basisdienste

- Infrastrukturseitige Datenerfassung
- Fahrzeugseitige Datenerfassung
- Ermittlung der Verkehrswetterlage
- Ermittlung der Verkehrslage
- Identifikation Verkehrsereignisse

Verkehrs(fluss)-Information und Navigation

- Straßenvorausschau
- Baustelleninformationssystem
- Erweiterte Navigation

Verkehrs(fluss)-Steuerung

- Umleitungsmanagement
- Lichtsignalanlagen Netzsteuerung
- Lokale verkehrsabhängige Lichtsignalanlagensteuerung

Fahren und Sicherheit

Lokale Gefahrenwarnung

- Hinderniswarnung
- Stauendewarnung
- Straßenwetterwarnung
- Einsatzfahrzeugwarnung

Fahrerassistenz

- Verkehrszeichen-Assistent/-Warnung
- Ampel-Phasen-Assistent/-Warnung
- Längsführungsassistent
- Kreuzungs-/Querverkehrsassistent

Ergänzende Dienste

Internetzugang und lokale Informationsdienste

- Internetbasierte Dienstnutzung
- Standortinformationsdienste

Mission | Zeitplan

Projekt-Phase 1

Anforderungen

Spezifikation der Funktionen und der Architektur

Prototypische Implementierung ITS Vehicle Station (IVS), ITS Roadside Station (IRS)

Projekt-Phase 2

Forschungsfahrzeuge ausgestattet, Systemtests

Produktion der ITS Vehicle Stations (IVS) und ITS Roadside Stations (IRS)

Schrittweiser Ausbau von Versuchsflotte und Versuchsgebiet

Start des Feldversuchs

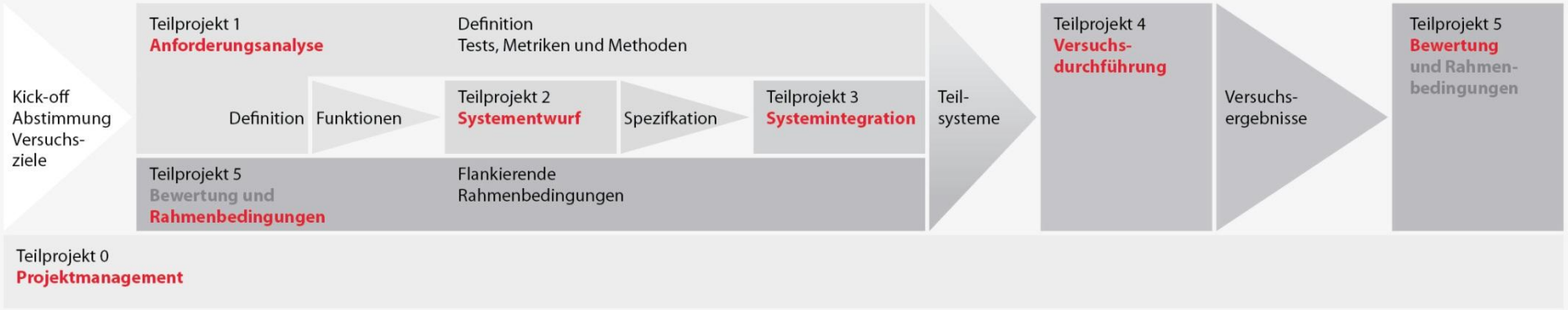
Projekt-Phase 3

Versuchsgebiet ausgestattet

Mehrere hundert Fahrzeuge und ITS Roadside Stations (IRS) einsatzbereit

Großversuch

Dokumentation, Auswertung und Bewertung



Konsortium

simTD : Partner

Automobilhersteller

Audi

BMW

DAIMLER

Ford

OPEL

VOLKSWAGEN
AKTIENGESELLSCHAFT

Zulieferer

BOSCH

Continental

Netzbetreiber

Deutsche Telekom

Wissenschaft

Fraunhofer

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH

TU berlin

Technische Universität München
Lehrstuhl für Verkehrstechnik

Hochschule für Technik und Wirtschaft des Saarlandes
University of Applied Sciences

HTW

IZVW

Öffentliche Einrichtungen

HESSEN

Unsere Kompetenz Ihre Mobilität
Hessisches Landesamt für Straßen- und Verkehrswesen

Stadt Frankfurt am Main

simTD : Förderer

Bundesministerien

Bundesministerium für Wirtschaft und Technologie

Bundesministerium für Bildung und Forschung

Bundesministerium für Verkehr, Bau und Stadtentwicklung

Unterstützer

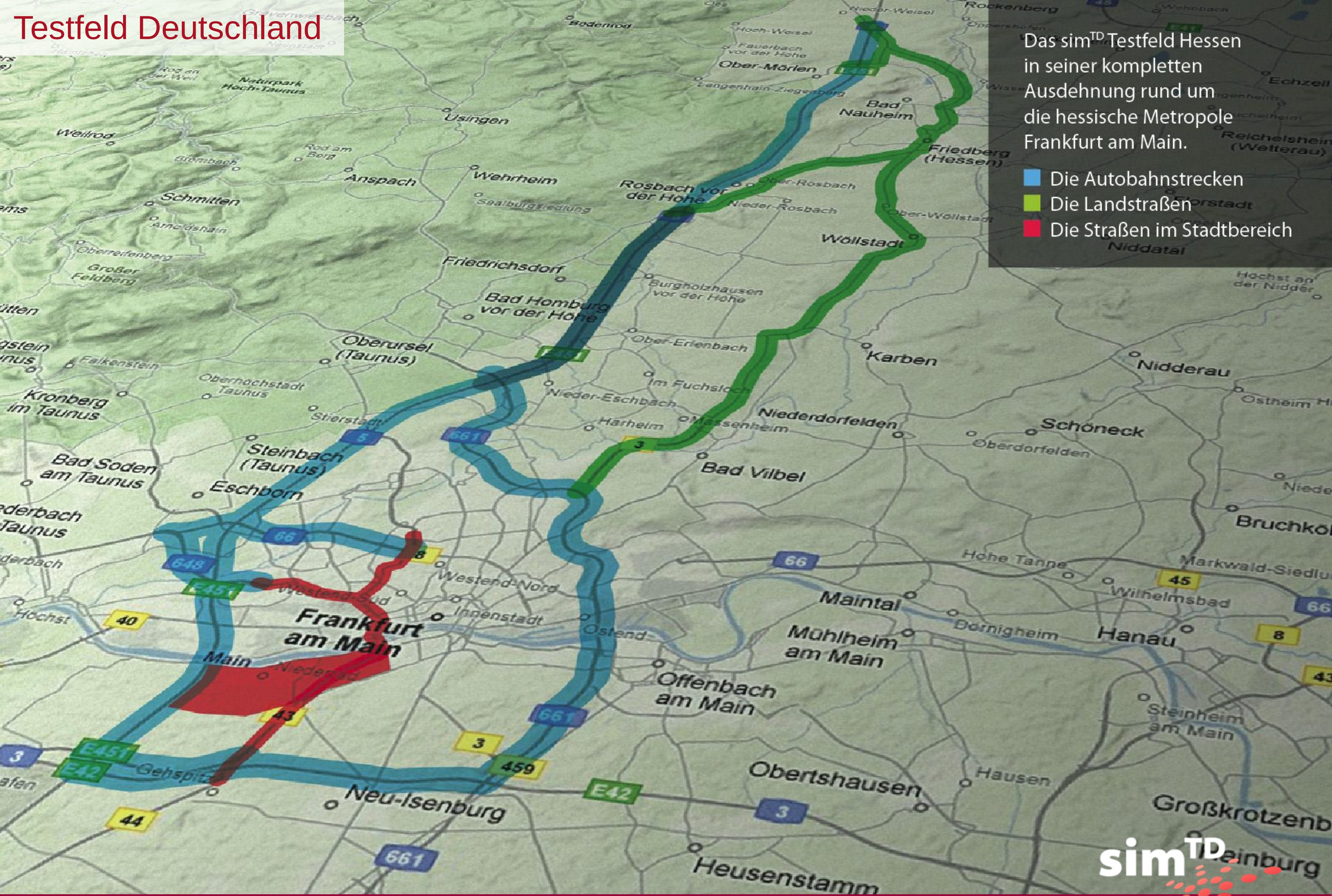
HESSEN

VDA Verband der Automobilindustrie

Testfeld Deutschland

Das sim^{TD} Testfeld Hessen in seiner kompletten Ausdehnung rund um die hessische Metropole Frankfurt am Main.

- Die Autobahnstrecken
- Die Landstraßen
- Die Straßen im Stadtbereich



sim^{TD}

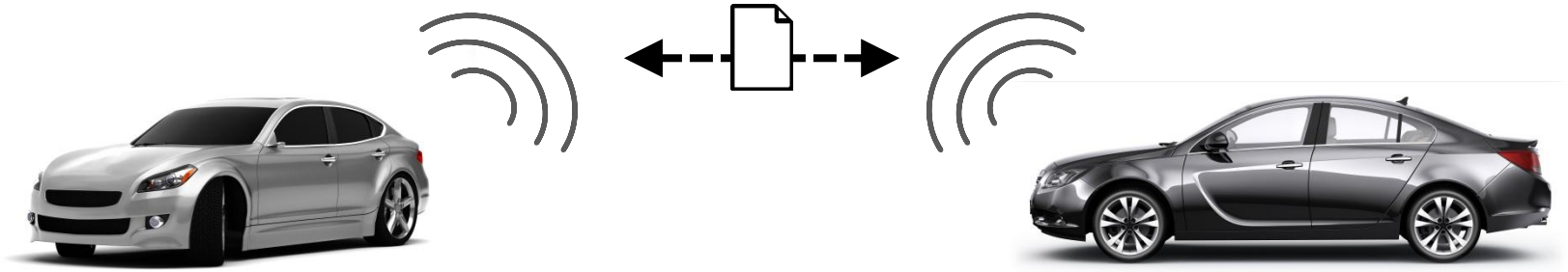
Herausforderungen in der C2X Kommunikation

- Technische Herausforderungen
  - Unter Umständen keine Sichtverbindung zwischen Kommunikationspartnern
  - Hohe Genauigkeit der Positionsdaten und Zeit
  - Niedrige Latenz zwischen Kommunikationspartnern
  - Regelmäßiger Wechsel der Netzwerktopologie durch hohe Bewegung der Kommunikationspartner
  - Keine regelmäßige Verbindung zur Infrastruktur
  - Anzahl von Kommunikationspartnern
- Nicht technische Herausforderungen
  - Preisdruck
  - IT-Sicherheit und Privatsphärenschutz

Herausforderungen in der C2X Kommunikation

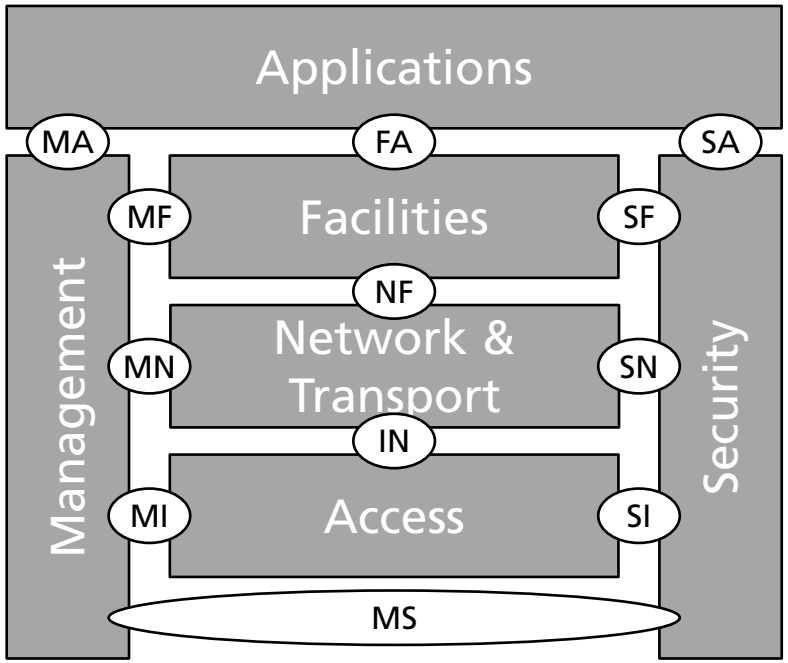
IT-Sicherheit und Privatsphärenschutz

- Authentisierung und Autorisierung der Sender von Nachrichten.
- Nachrichten- und Datenintegrität muss sicher gestellt werden.
- Nachrichten- und Datenvertraulichkeit wird bei einzelnen Anwendungen benötigt.
- Systemintegrität ist notwendig um die Sender-Authentisierung sicher zu stellen.
- Daten- und Privatsphärenschutz wird benötigt.



C2X Kommunikation

Intelligent Transportation System Architektur (1 / 6)



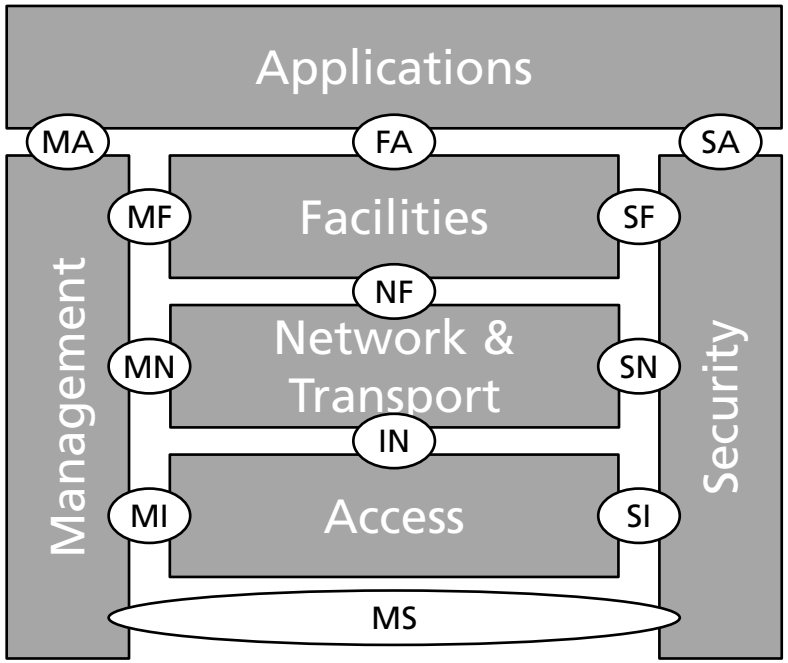
Access

- ITS G5A (5.875GHz – 5.905 GHz)
  - 1 x Control Channel
  - 2 x Service Channel
- ITS G5B (5.855GHz – 5.9875 GHz)
  - 2 x Service Channel
- WLAN

ETSI EN 302 665, v1.1.1 (2010-09)

C2X Kommunikation

Intelligent Transportation System Architektur (2 / 6)



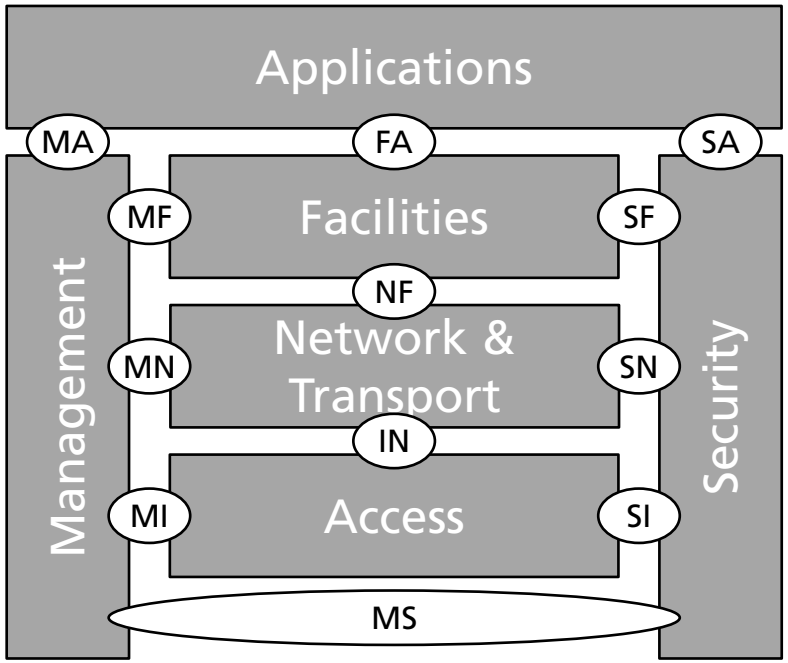
Network & Transport

- Multi-hop Routing
- Quality of Service
- Nachrichtenabsicherung

ETSI EN 302 665, v1.1.1 (2010-09)

C2X Kommunikation

Intelligent Transportation System Architektur (3 / 6)



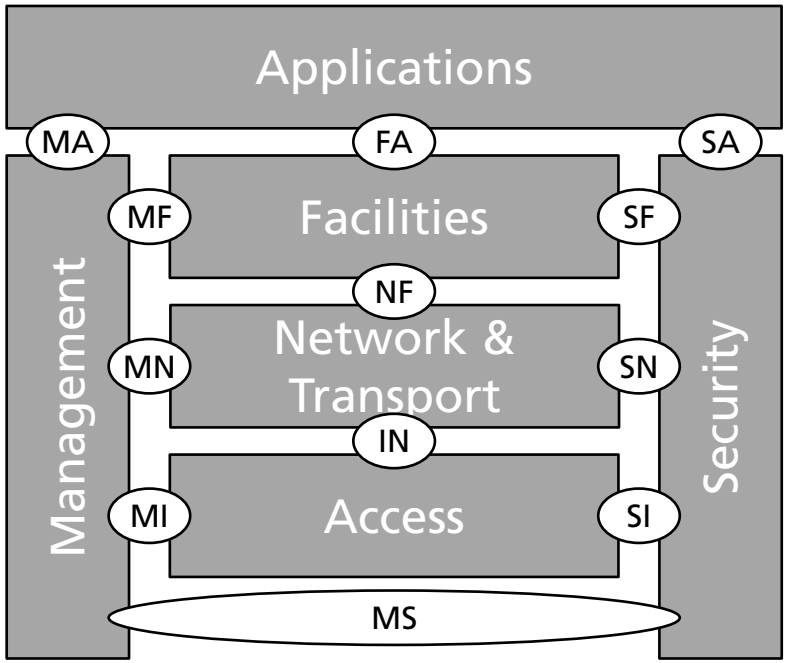
Facilities

- Generierung von Systemnachrichten, z.B. **Cooperative Awareness Message (CAM)**
- Verarbeitung von Systemnachrichten
- Bereitstellung von Systeminformationen
  - Ego-Fahrzeugdaten (z.B. GPS Position)
  - Umfeldtabelle
- Nachrichtenabsicherung

ETSI EN 302 665, v1.1.1 (2010-09)

C2X Kommunikation

Intelligent Transportation System Architektur (4 / 6)



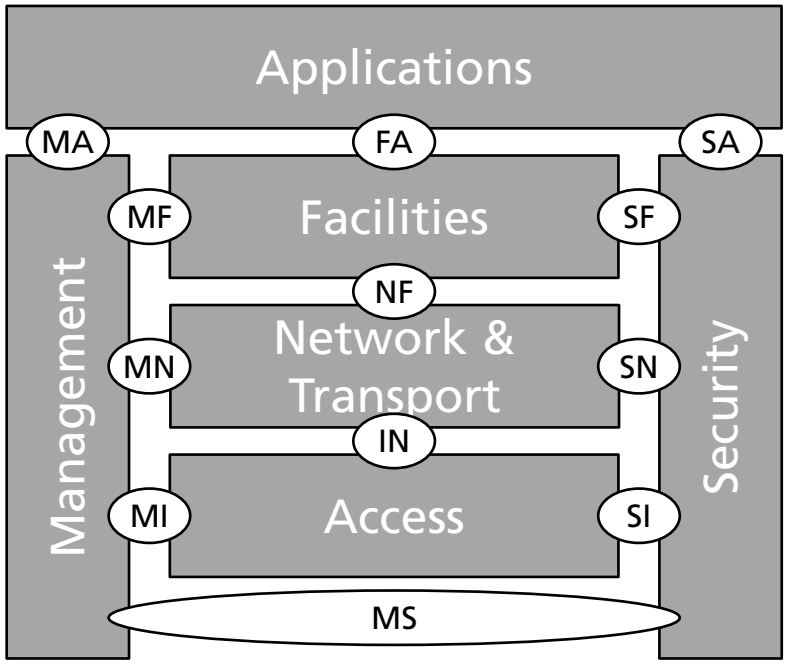
Application

- Generierung anwendungsorientierter Nachrichten, z.B. **Decentralized Environmental Notification Message (DENM)**
- Verarbeitung anwendungsorientierter Nachrichten
- Anwendungsorientierte Reaktion, z.B. Ausgabe von Warnungen

ETSI EN 302 665, v1.1.1 (2010-09)

C2X Kommunikation

Intelligent Transportation System Architektur (5 / 6)



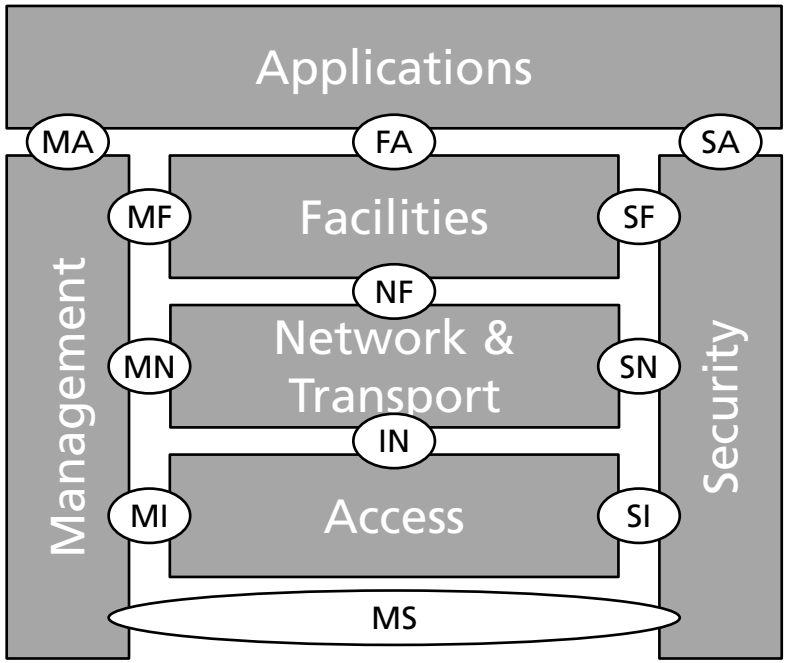
Management

- Konfiguration, Steuerung und Verwaltung des Systems

ETSI EN 302 665, v1.1.1 (2010-09)

C2X Kommunikation

Intelligent Transportation System Architektur (6 / 6)



Security

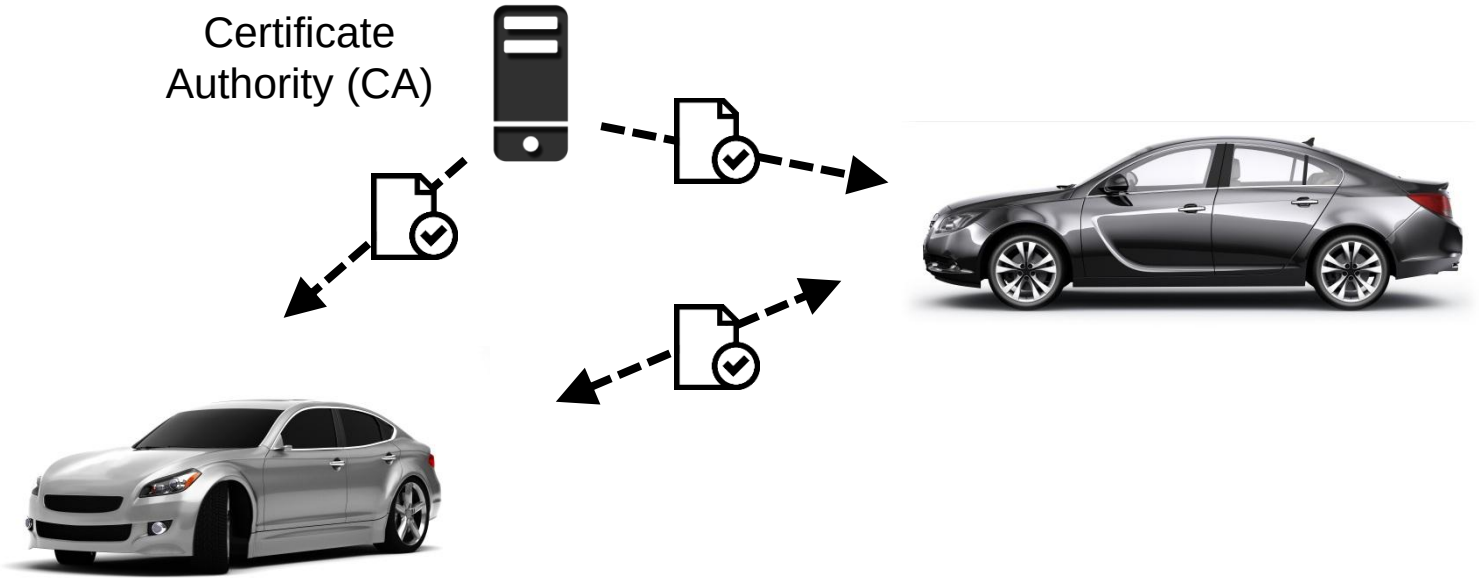
- Absicherung der Nachrichten
  - Authentizität
  - Integrität
  - Vertraulichkeit
- Schutz der Privatsphäre
  - Pseudonymität
  - Wechsel der Pseudonyme
- Absicherung des Systems

ETSI EN 302 665, v1.1.1 (2010-09)

IT-Sicherheit in der C2X Kommunikation

PKI – Motivation und Anforderungen

- Identifikation gültiger Sender → **Zentrale PKI als Vertrauensanker**
- PKI Design muss die Privatsphäre der Fahrzeughalter / Fahrer schützen
- Eine permanente Kommunikationsverbindung mit der zentralen Autorität kann nicht angenommen werden



Security Solution for C2X Communication

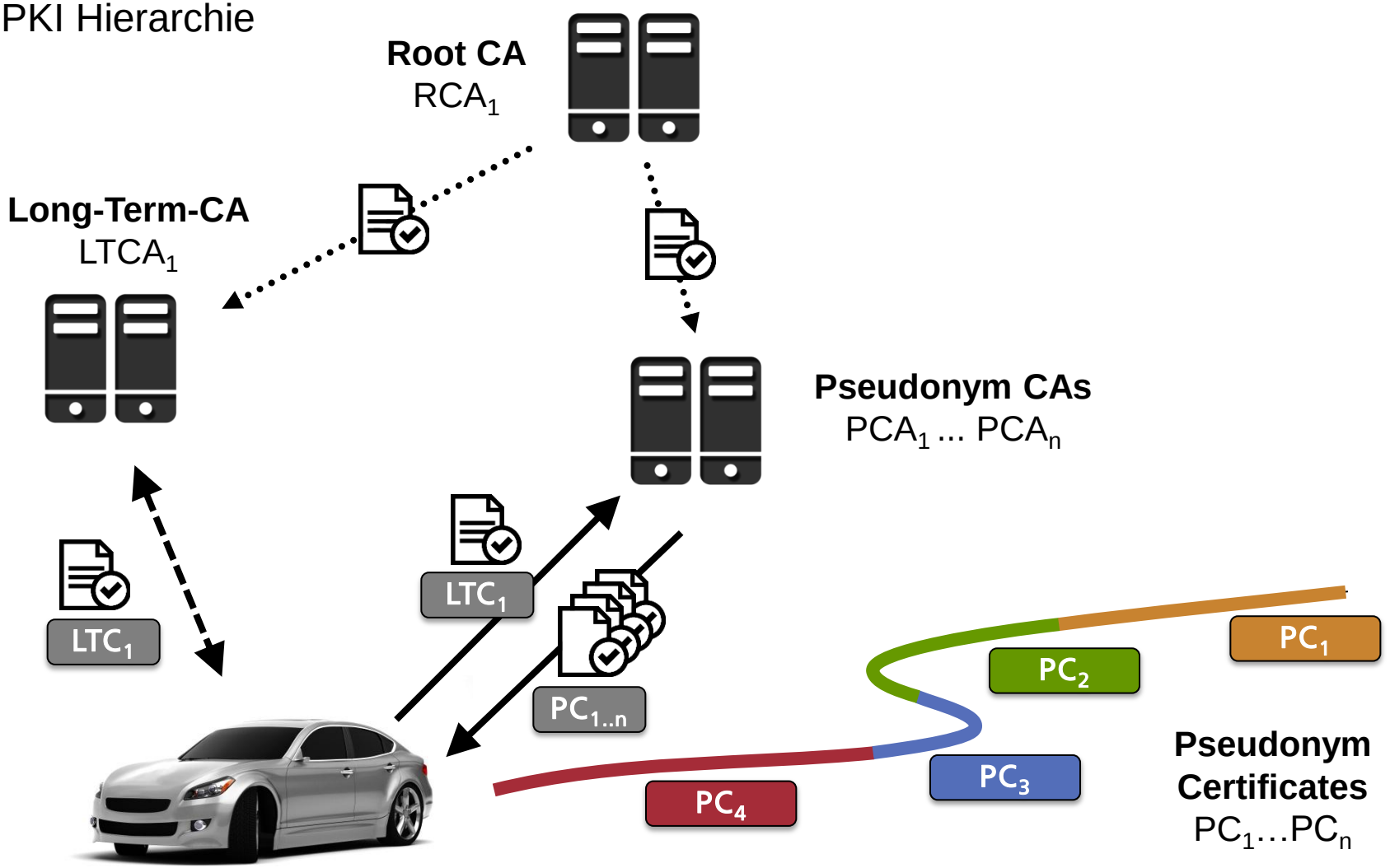
PKI Solution – Certification

Long-term Certificate (LTC)	Short-term, Pseudonym Certificates (PCs)
• Authentifiziert Stationen innerhalb der PKI, z.B., zum Abruf neuer PCs, wird immer Verschlüsselt übertragen	• Authentifiziert Stationen in der C2X Kommunikation, Ermöglicht Autorisierung, Signierung und Verschlüsselung
• Kann gesperrt werden wenn Missbrauch festgestellt wurde	• Durch kurze Gültigkeitsdauer ist Revokation nicht notwendig → Erspart den Transfer von Revokationslisten zu den Fahrzeugen
• Beinhaltet Berechtigungen und kann identifizierende Informationen speichern	• Inhalte sind reduziert auf ein Minimum → Daten- und Privatsphärenschutz

Car-2-Car Communication Consortium, Public Key Infrastructure Memo

Security Solution for C2X Communication

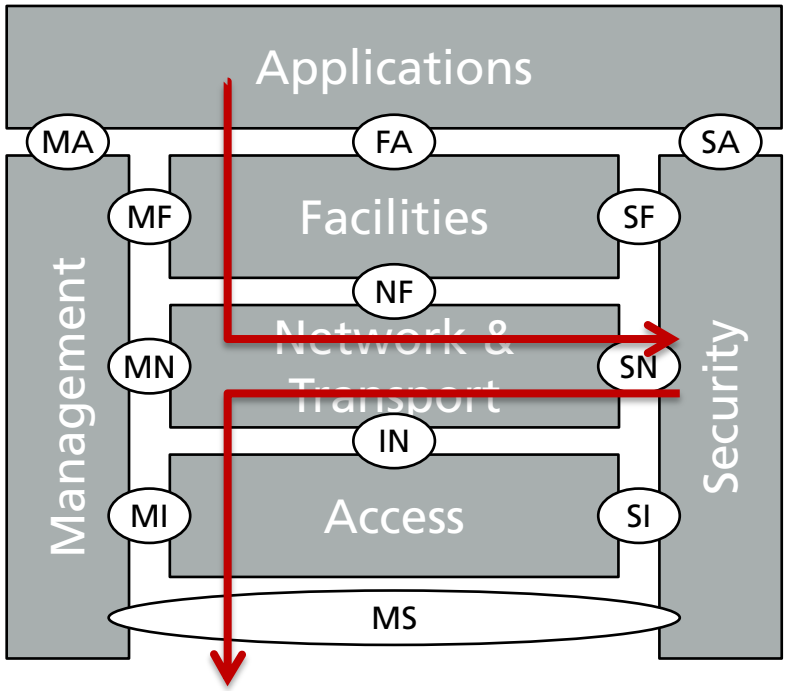
PKI Hierarchie



Car-2-Car Communication Consortium, Public Key Infrastructure Memo

IT-Sicherheit in der C2X Kommunikation

Integration der IT-Sicherheitsmaßnahmen



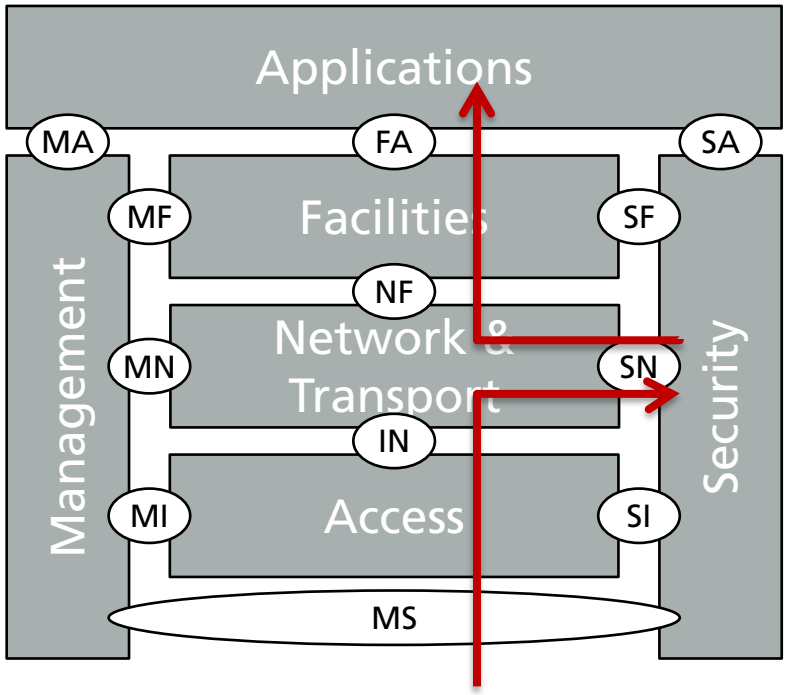
Senden

- Generierung durch Anwendung oder Facilities-Funktion
- Signierung / Verschlüsselung durch die Security
- Versand per ITS G5

ETSI EN 302 665, v1.1.1 (2010-09)

IT-Sicherheit in der C2X Kommunikation

Integration der IT-Sicherheitsmaßnahmen



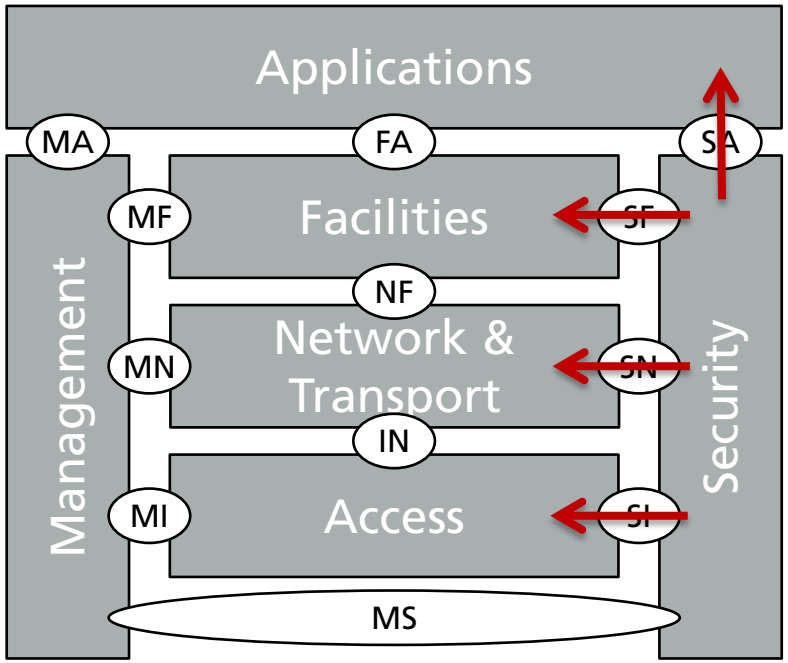
Empfang

- Empfang per ITS G5
- Verifikation / Entschlüsselung durch die Security
- Plausibilitätsprüfung durch die Security
- Verarbeitung durch Anwendung oder Facilities-Funktion

ETSI EN 302 665, v1.1.1 (2010-09)

IT-Sicherheit in der C2X Kommunikation

Integration des Privatsphärenschutz in der Kommunikation



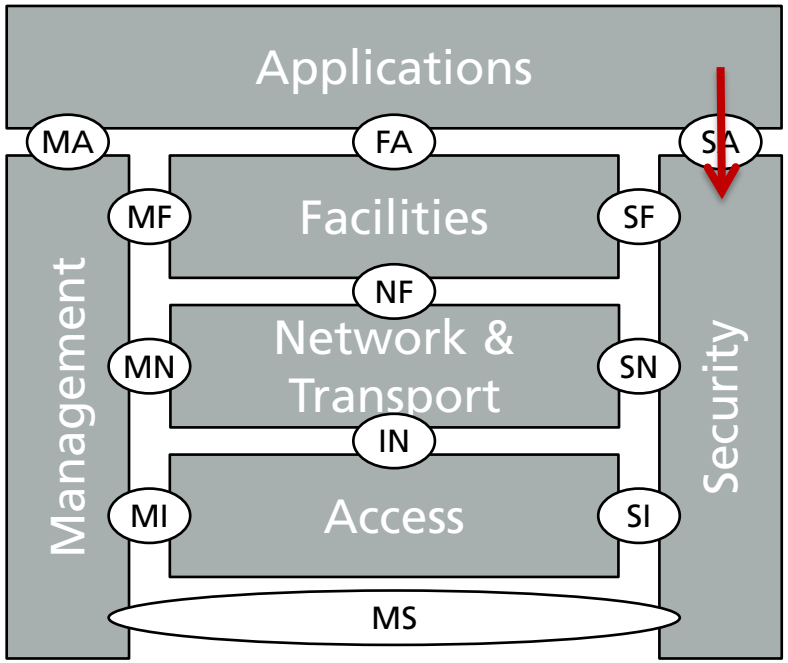
Pseudonymwechsel

- Steuerung durch die Security oder das Management
- Synchronisierter Wechsel der ID auf allen Schichten
- Ableitung der ID vom Pseudonym-Zertifikat (optional)

ETSI EN 302 665, v1.1.1 (2010-09)

IT-Sicherheit in der C2X Kommunikation

Integration des Privatsphärenschutz in der Kommunikation



Sperre des Pseudonymwechsels

- Anwendungen können in kritischen Situationen, z.B. im Kreuzungsbereich, den Pseudonymwechsel blockieren.

  → Anwendungen anderer Fahrzeuge in Kommunikationsreichweiter werden nicht gestört.

ETSI EN 302 665, v1.1.1 (2010-09)

Evaluierung der IT-Sicherheit

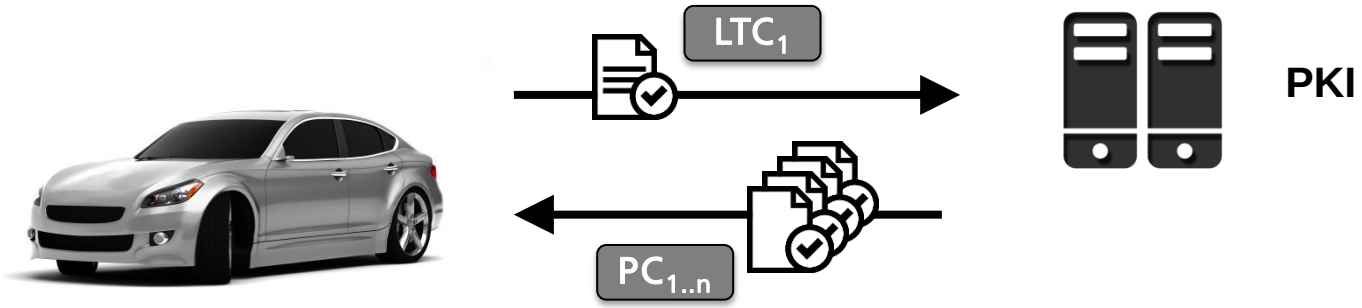
Zertifikatsabruf von der PKI

- Welche durchschnittliche Belastung ist für eine C2X-PKI zu erwarten?

  →Anzahl abgefragter Pseudonym-Zertifikate von der PKI
- Ist ein Update des Zertifikatpools während der Fahrt möglich?

  → Bearbeitungsdauer der Pseudonym-Zertifikatsanfragen bei der PKI
- Sind die Zertifikatsabfragen regelmäßig oder konzentriert?

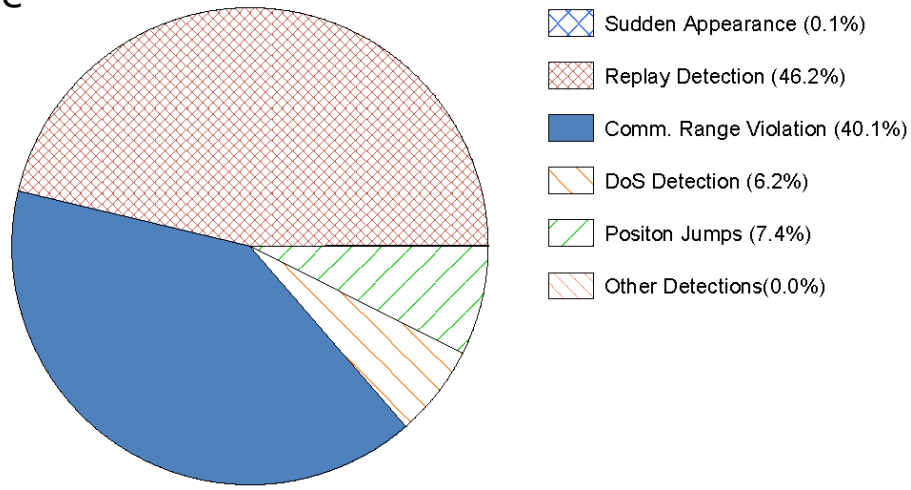
  →Verteilung der Anfragen über den Tag



Evaluierung der IT-Sicherheit

Plausibilitätsprüfung - Kategorien

- Keine Durchführung expliziter Angriffe
- Separate Betrachtung für…
  - Fahrzeuge und
  - Roadside Stationen.

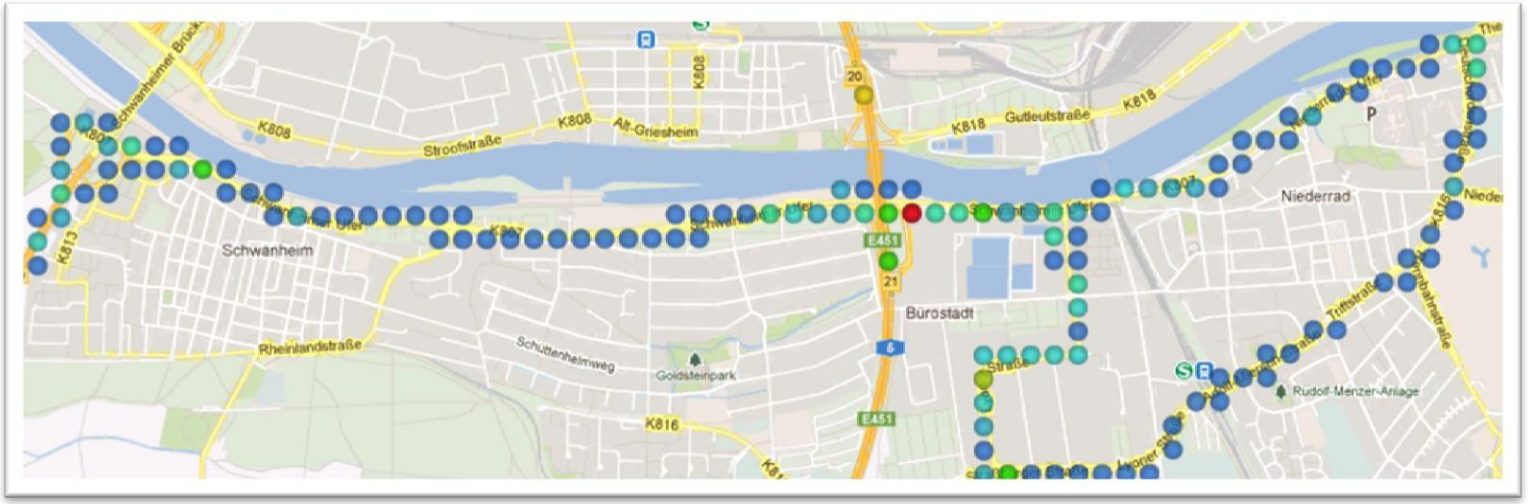


- Messung der Plausibilitätsprüfung
  - Zeitsynchronisation zwischen Stationen (Replay Attack Detection)
  - Dimension des Kommunikationsradius (Communication Range Violation)
  - Genauigkeit des Fahrzeug-Tracking (Position Jump Detection)
  - Unerwartetes Auftauchen neuer Stationen (Sudden Appearance)

Evaluierung der IT-Sicherheit

Plausibilitätsprüfung - Gebiete

- Ortsbezogene Auswertung von Plausibilitätsfehlern



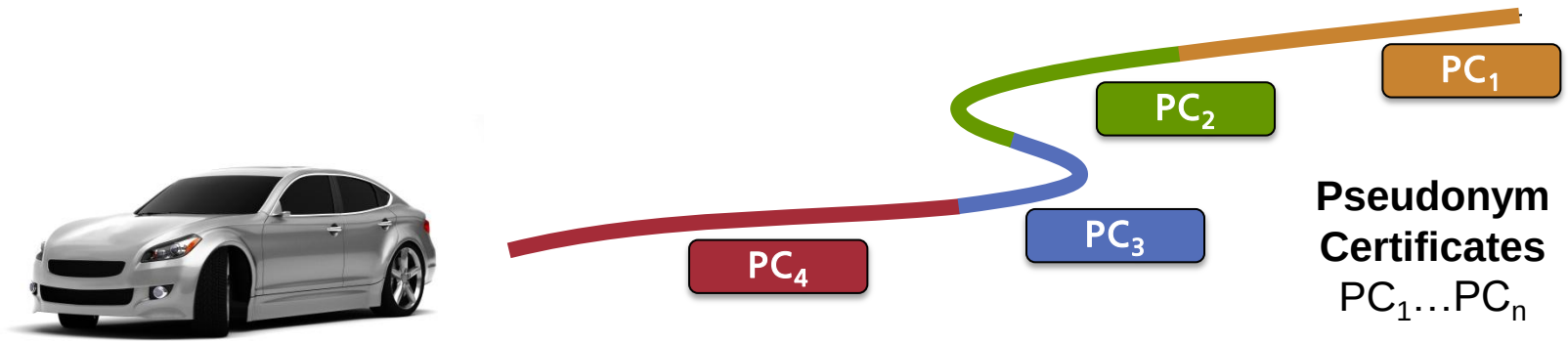
- Legende:

0% 0.25% 0.5% 0.75% >1%

Evaluierung der IT-Sicherheit

Pseudonymwechsel des eigenen Fahrzeugs

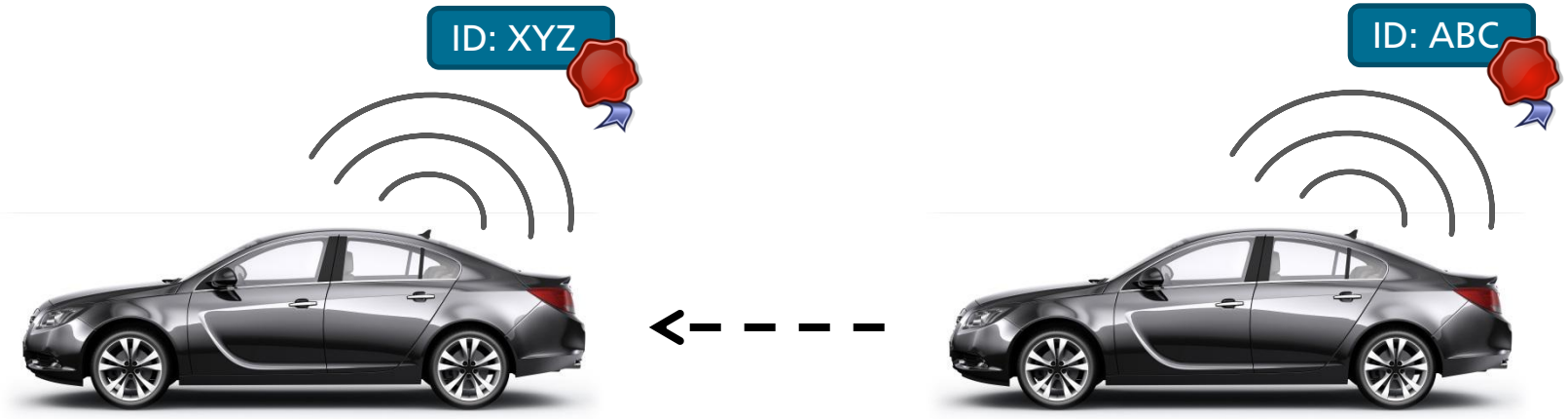
- Messung der zurückgelegten Strecke und Fahrtdauer
  - Pseudonymwechsel während der Fahrt
  - Pseudonymwechsel beim Fahrzeugstart
- Anzahl gültiger Pseudonym-Zertifikate im Speicher des Fahrzeugs beim Wechsel



Evaluierung der IT-Sicherheit

Pseudonymwechselerkennung bei fremden Fahrzeugen

- Erfolgreiche Erkennung von Pseudonymwechsel benachbarter Fahrzeuge
- Fehlerhaft erkannte Pseudonymwechsel (Falsch-Positiv)
- Nicht erkannte Pseudonymwechsel (Falsch-Negativ)



Zeitpunkt: $t0$

Zeitpunkt: $t1$

Evaluierung der IT-Sicherheit

Pseudonymwechselsperre

- Sperrung des Pseudonymwechsels auf dem eigenen Fahrzeug in kritischen Situationen durch verschiedene Anwendungen
  - Dauer der Sperre
  - Zurückgelegte Strecke mit aktiver Sperre

Zusammenfassung und Ausblick

- Durch die Erforschung und Erprobung der C2X-Kommunikation werden die Grundlagen zur
  - Steigerung der Verkehrseffizienz und zur
  - Erhöhung der Sicherheit im Straßenverkehr geschaffen.
- Die C2X Protokolle sind optimiert für die drahtlose (ad-hoc) Fahrzeug-Fahrzeug Kommunikation sowie für die Fahrzeug-Infrastruktur Kommunikation.
- IT-Sicherheitsmaßnahmen werden benötigt um Angriffe zu verhindern.
- Privacy- und Datenschutzmaßnahmen sind erforderlich um die Privatsphäre der Fahrer und Fahrzeughalter zu schützen.

- sim^{TD} erlaubt eine umfangreiche Evaluierung der Mechanismen zum Schutz der Privatsphäre und der IT-Sicherheit.

Norbert Bißmeyer

E-Mail: norbert.bissmeyer@sit.fraunhofer.de

Fraunhofer-Institut für
Sichere Informationstechnologie (SIT)
Rheinstraße 75
64295 Darmstadt

www.fraunhofer.de
www.sit.fraunhofer.de