Bundesamt
für Sicherheit in der
Informationstechnik

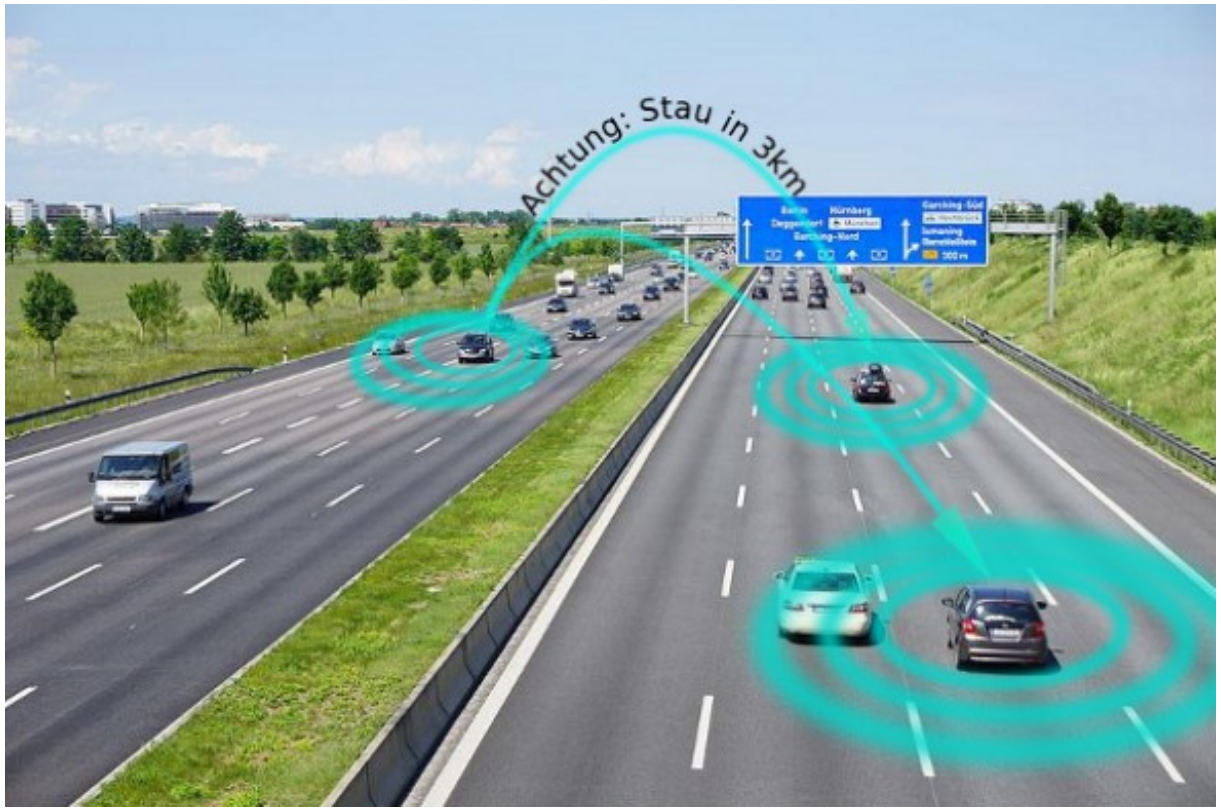
IT-Sicherheit für das vernetzte Fahren

Automotive 2017, 31.5.2017, Stuttgart

Fahrzeug-zu-X-Kommunikation

Anwendungen für den “Tag 1”

- Warnung vor langsamen/stehenden Fahrzeugen
- Warnung vor sich nähernden Einsatzfahrzeugen
- Verkehrszeichen im Fahrzeug
- Missachtung von Ampeln
- Geschwindigkeitsbegrenzung im Fahrzeug
- Geschwindigkeitsempfehlung für Grüne Welle
- Abfederung von Staustoßwellen
- usw.



Quelle:Wikimedia

Strategie der Bundesregierung

Ziele

- Erhöhung der Verkehrssicherheit
- Verringerung des Ressourcenverbrauchs
- Leitanbieter bleiben, Leitmarkt werden
  - Automatisiertes und vernetztes Fahren rechtlich ermöglichen

Handlungsfelder

- Digitale Infrastruktur
- Innovation
- **IT-Sicherheit und Datenschutz**

Der C-ITS-Korridor

- 2013 initiiertes internationales Projekt (AT, D, NL)
- Autobahnkorridor von Rotterdam bis Wien wird mit ITS-Anwendung ausgestattet
- Leitung in D beim BMVI, Koordinierung durch die BaSt
- Unterstützung durch BSI: Pilot-PKI

Quelle: BMVI

Bundesministerium für Verkehr und digitale Infrastruktur

bast

Ministry of Infrastructure and the Environment of the Netherlands

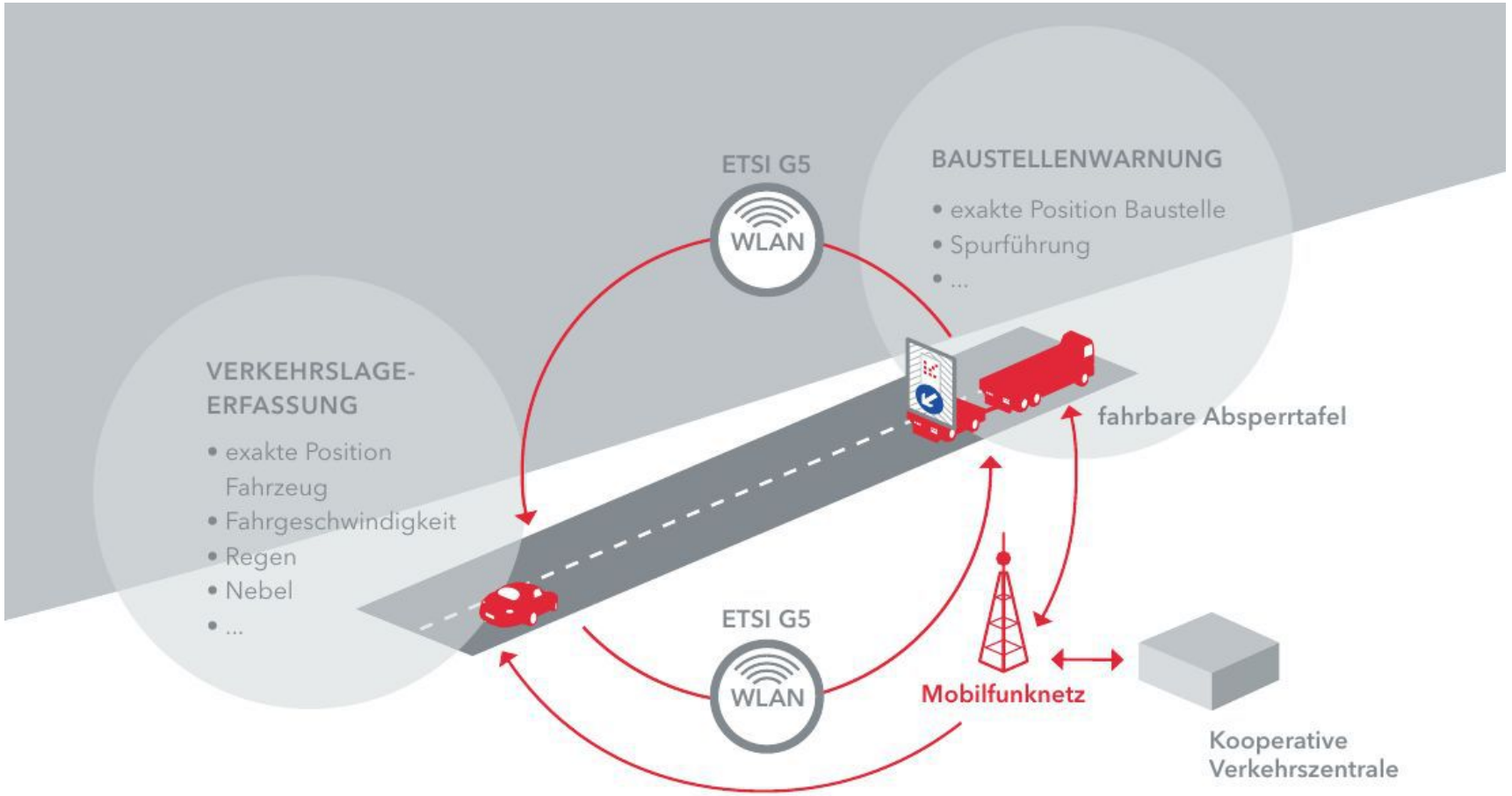
bmvit
Bundesministerium für Verkehr, Innovation und Technologie

Hessen Mobil
Straßen- und Verkehrsmanagement

HESSEN

Bundesamt für Sicherheit in der Informationstechnik

Anwendungen im C-ITS-Korridor



Quellen: BMVI, Hessen Mobil Straßen- und Verkehrsmanagement

Nachrichtenformate

- Cooperative Awareness Messages (CAMs)
  - Daten über (aktuellen) Zustand des Fahrzeugs (Geschwindigkeit, Richtung, Maße, Pfadhistorie, ...)
  - Regelmäßiger Broadcast mit bis zu 10 Hz
  - „Single hop“
- Decentralized Environmental Notification Messages (DENMs)
  - Daten über besondere Verkehrssituationen (Schlechtes Wetter, langsames Fahrzeug, Baustelle, ...)
  - Broadcast bei Bedarf
  - „Multi hop“

Beispiel: CAM

High Frequency Container

Heading
Speed
Drive direction
Vehicle length
Vehicle width
Longitudinal acceleration
Curvature
Yaw rate
Acceleration control (optional)
Lane position (optional)
Steering wheel angle (optional)
Lateral acceleration (optional)
Vertical acceleration (optional)
Performance class (optional)
CenDsrcTollingZone (optional)

Low Frequency Container

Vehicle role
Exterior lights
Path history

Special vehicle Container

Public Transport Container
Special Transport Container
Dangerous Goods Container
Road Works Container
Rescue Container
Emergency Container
Safety Car Container

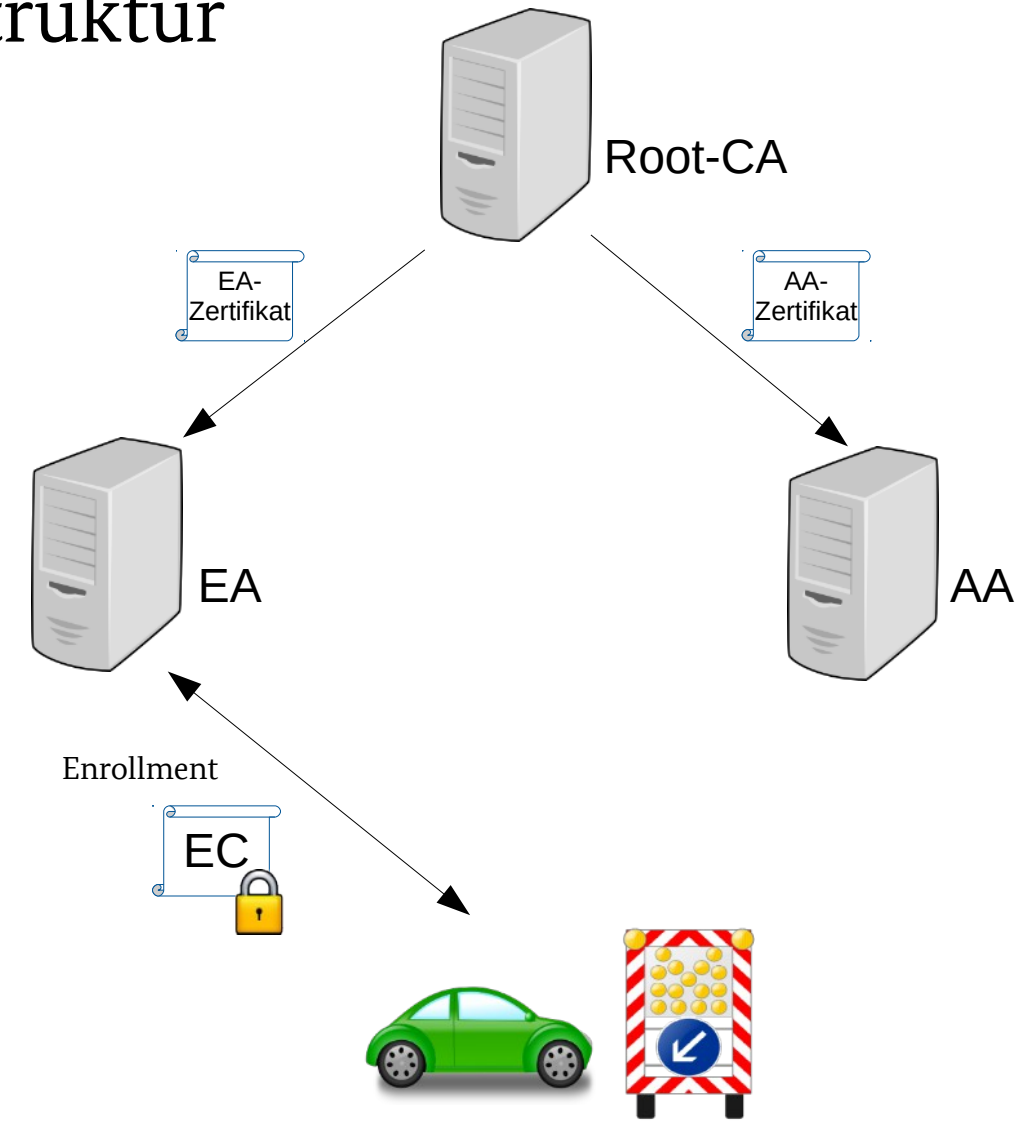
IT-Sicherheit

- Grundlage: Sicherheitskonzept des
  Car-to-Car Communication Consortium (C2C-CC), ETSI-Spezifikationen
  - CAMs und DENMs werden digital signiert (keine Verschlüsselung)
  - Signatur mit ECDSA
  - Zur Zeit: elliptische Kurve NIST P-256, später auch Brainpool-Kurven
  - Eigenes Zertifikatsformat
  - Pseudonymkonzept
- Technische Randbedinungen: Hohes Nachrichtenaufkommen, begrenzte Kanalkapazität
- BSI: Anpassung des Konzepts für die Verkehrsinfrastrukturseite, Aufbau der Pilot-PKI
- Baustellenwarner-Gateway: 2000 Sig.-Verifikationen/Sek. möglich

Paketstruktur gesicherter CAMs/DENMs

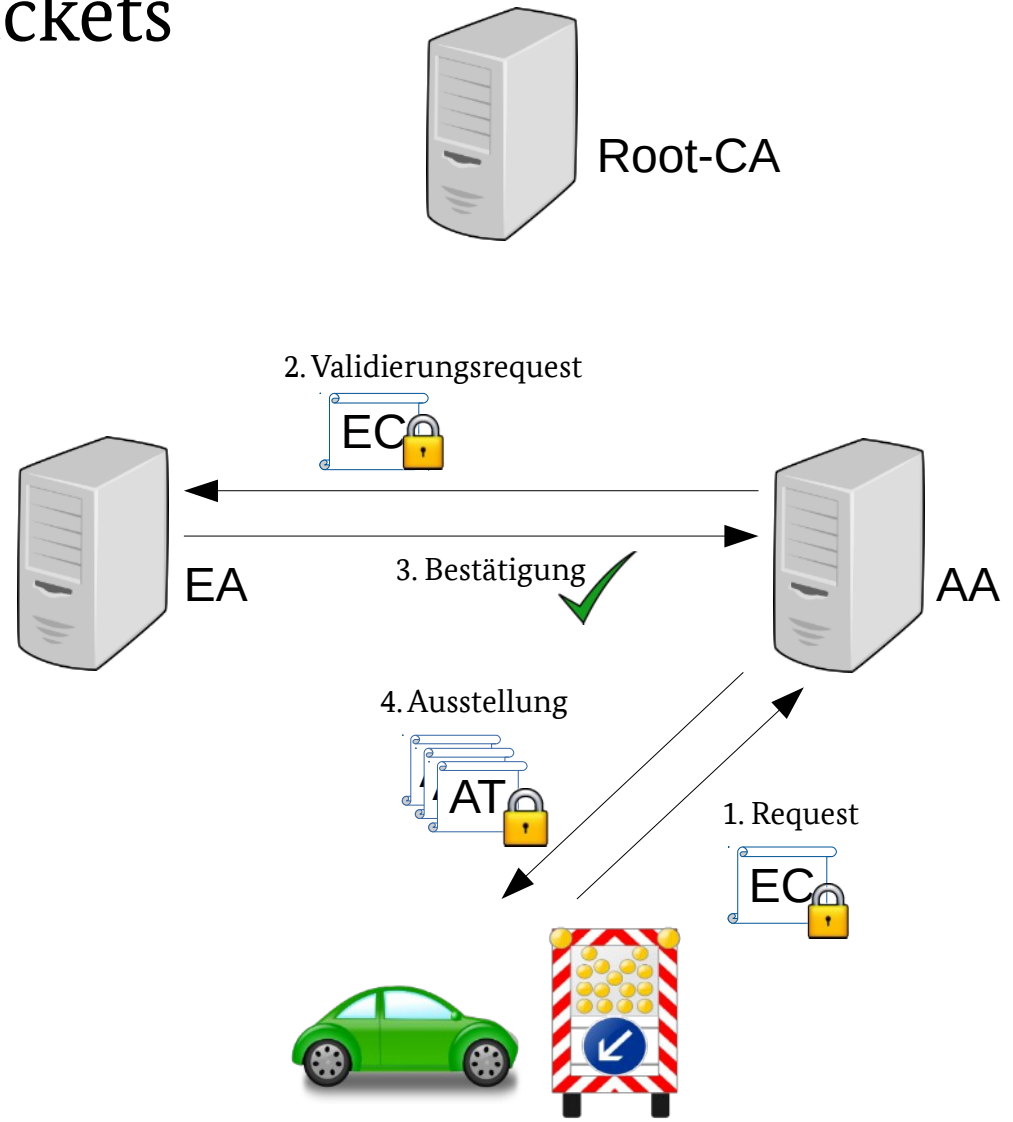
IT-Sicherheit: Public-Key-Infrastruktur

- Root-CA: Wurzelzertifizierungsstelle
- EA: „Enrollment Authority“
  - Stellt Langzeitzertifikate (EC) aus
- AA: „Authorization Authority“
  - Stellt Kurzzeitzertifikate (ATs) aus
  - Für Fahrzeuge pseudonym
  - Werden an CAMs, DENMs angehägt
- Revokation von CA-Zertifikaten und Langzeitzertifikaten möglich
- Separate Systeme für Fahrzeuge und RSUs



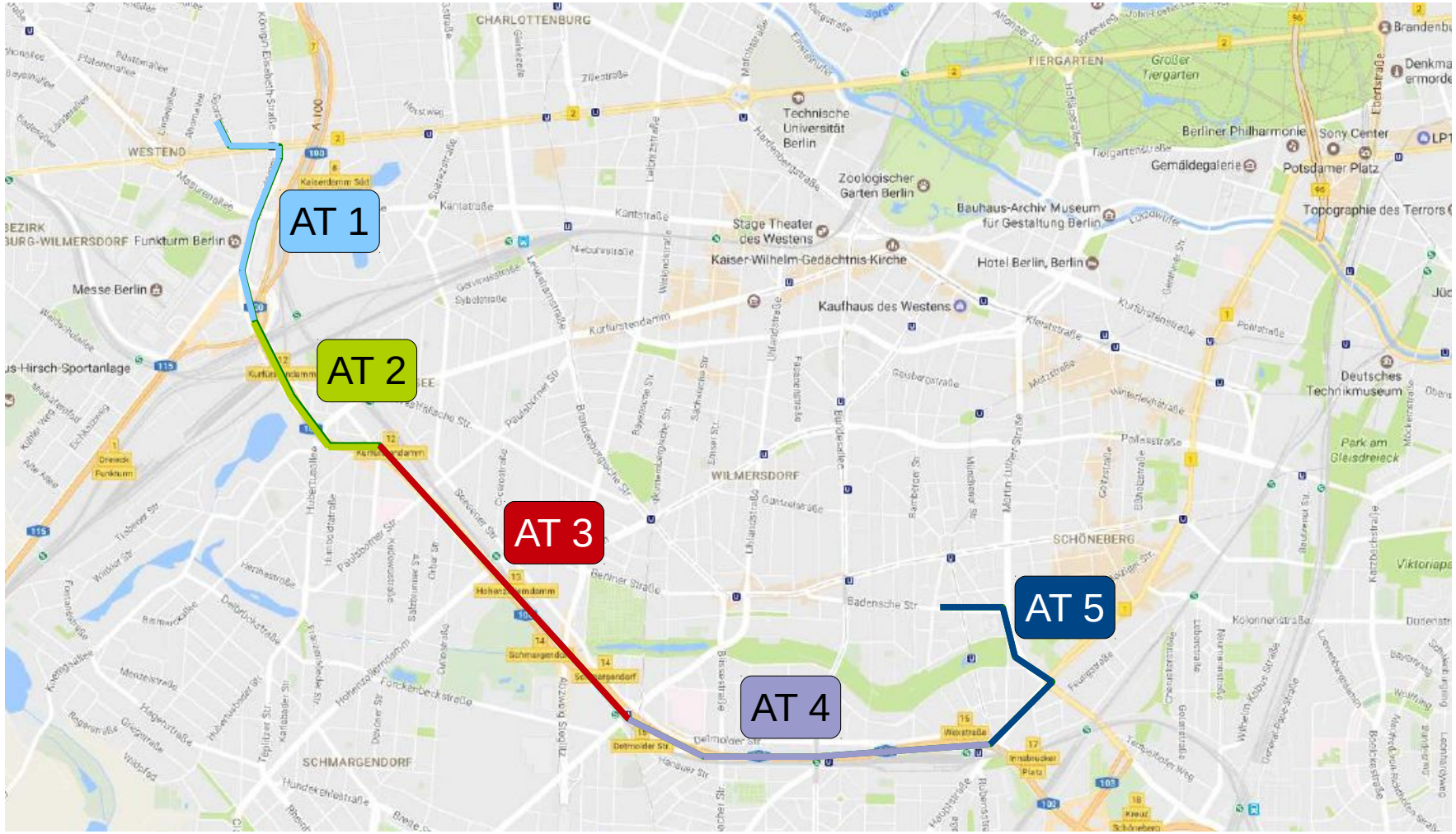
Ausstellung von Authorization Tickets (ATs)

- Authorization Ticket: Zertifikat mit kurzer Gültigkeit zur Signierung von CAMs, DENMs
- Anonyme Ausstellung (bei Fahrzeugen)
- „Verteilte“ Prüfung des Requests bei EA und AA erschwert Zuordnung von Identitäten



C-ITS: Location Privacy

- Fahrstrecken sollen nicht “global” nachvollziehbar sein
- Inbesondere Start und Ende einer Strecke sollen nicht verknüpfbar sein
- Daher: Regelmäßiger Wechsel der ATs
- Genaue Wechsel-Strategie?
  - Nach x m
  - Nach y Min.
- Wiederverwendung von ATs?



Kartendaten (c) 2017, GeoBasis-DE/BKG ((c) 2009), Google

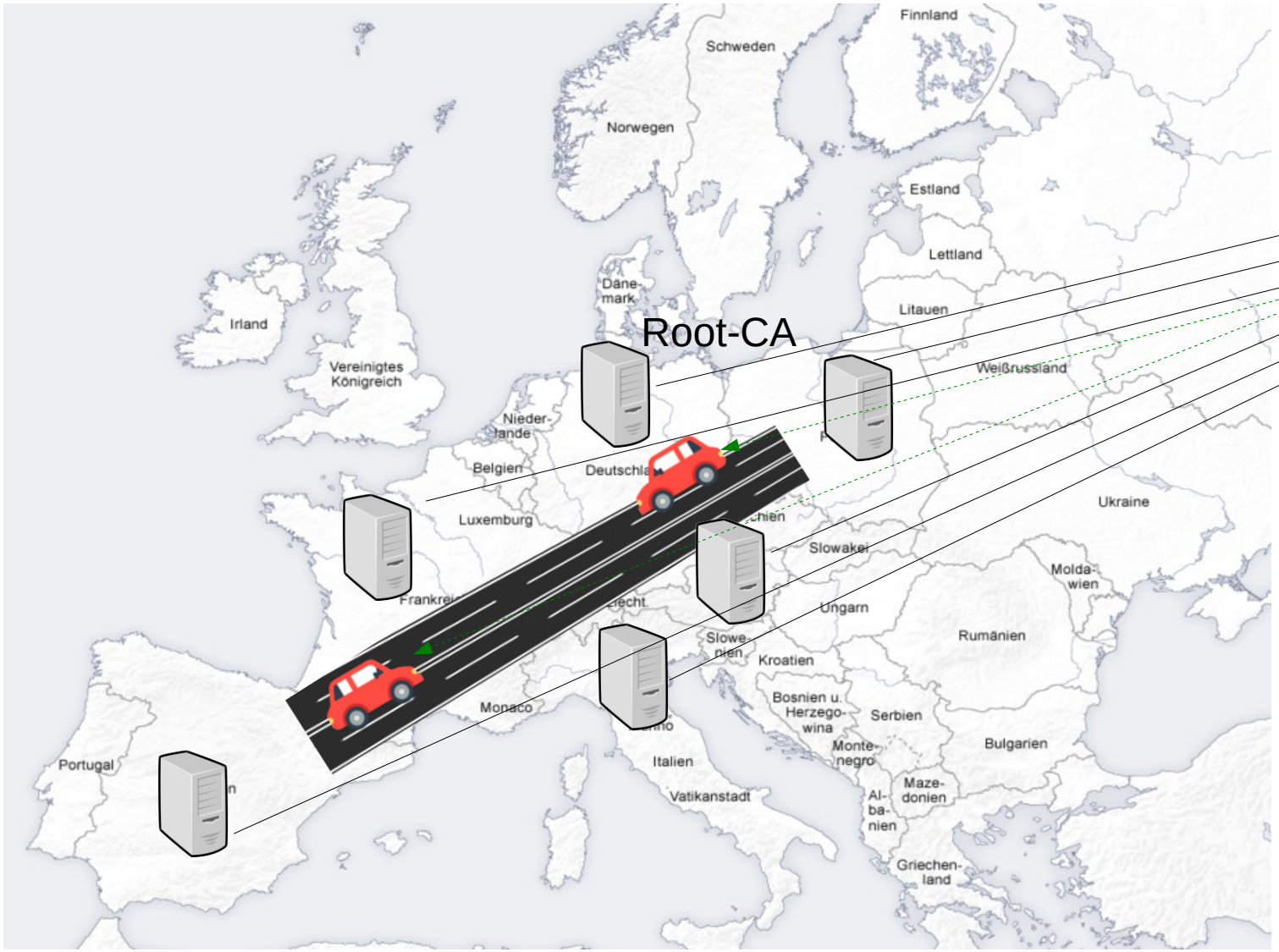
C-ITS: Location Privacy

- Zertifikate (ATs) als Identifikator (fester Public Key) → Tracking bei festem AT möglich
- Ansatz: Regelmäßiger Wechsel der Zertifikate
  - Fahrzeug beantragt regelmäßig (großen) Pool an ATs
  - Fahrzeug verwendet ATs im Wechsel
- Grenzen
  - Anzahl der Zertifikate begrenzt (Fahrzeuge nicht immer online)
  - langfristige Beobachtung möglich
  - Tracking aufgrund des umfangreichen Datensatzes in CAMs (insb. GPS-Position)
- Technische Lösung schwierig
  - Verschlüsselung?
  - CAM-Gebrauch einschränken?

Die C-ITS-Plattform

- EU-Kommission (DG MOVE): C-ITS-Plattform seit 2015
- Technische und rechtliche Fragestellungen in Bezug auf Interoperabilität
- Empfehlungen an Kommission und andere relevante Akteure
- Working Groups: Compliance Assessment, **Data Protection and Privacy**, Digital and Physical Road Infrastructure, Enhanced Traffic Management, **Security**, ...
- Regulierung via delegiertem Rechtsakt basierend auf EU-Direktive 2010/40/EU
- IT-Sicherheit: Policy für europaweite PKI

Eine europäische Public-Key-Infrastruktur



Karte Quelle: Wikimedia, San Jose

European Commission

Trust List Manager

European Root

Bundesamt für Sicherheit in der Informationstechnik

C-ITS Certificate Policy

- Vorgaben zu
  - Gesamtarchitektur PKI
  - Genehmigung (Approval) des CA-Betriebs (Roots, Sub-CAs...)
  - Erst-/Folgeausstellung von Zertifikaten
  - Laufzeiten von Zertifikaten
  - Revokation
  - Vergabe von Service Specific Permissions
- Enge Abstimmung mit ETSI (z.B. Listenformate ECTL, CRL)
- Erste Version wird in 2017 als Guideline veröffentlicht

Externe Schnittstellen des Fahrzeugs

WLAN

Digitalradio

Mobilfunk/Internet

Bluetooth

Car-to-X

Sensoren

TPMS

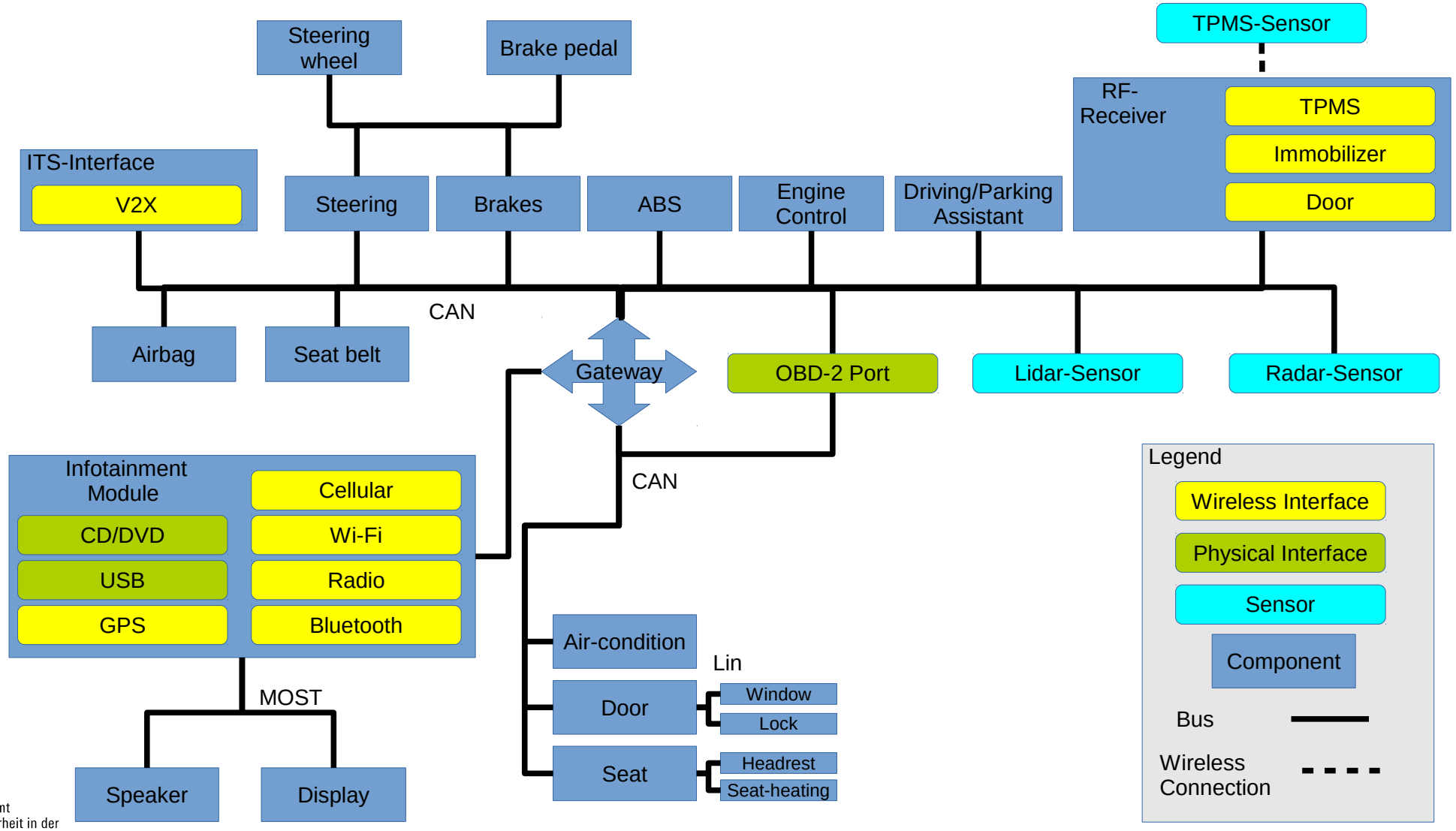
USB

OBD-2

Türschloss/Wegfahrsperre

Quelle: Wikimedia, SurfAst

Fahrzeuginterne Netzwerke



Bundesamt für Sicherheit in der Informationstechnik

IT-Angriffe auf Fahrzeuge

Typische Schwachstellen

- Identisches Schlüsselmaterial auf allen Instanzen
- Fehlende Authentisierung
- Unsignierte Soft-/Firmwareupdates
- Lückenhaft/un-gesicherte Backendverbindungen
- (Schwache kryptographische Verfahren)
- (Schreibender Zugriff auf CAN-Bus über OBD-2 möglich)

Automotive Security

- Handlungsbedarf wird auf pol. Ebene gesehen
- Strategie Automatisiertes und Vernetztes Fahren:
  - Erarbeitung von Grundsätzen bei der UNECE, Working Group ITS/AD
  - Vorgaben für (Typ-)Zulassung von Fahrzeugen
- Mögliche Management-Maßnahmen:
  - Zertifizierung von Komponenten/Produkten mit Sicherheitsfunktionalität?
  - Meldewesen für IT-Sicherheitsvorfälle,-schwachstellen?
  - Soft-/Firmwarepatches, Regelmäßige Prüfung?

Zertifizierung von Komponenten

- Schutzprofil nach Common Criteria
  - Beispiel: Digitaler Tachograph
  - Reguliert nach EU-Verordnung (1360/2002, 561/2006)

  - Baustellenwarner-Gateway (laufend)

- Zukünftige Zertifizierung?
  - Kommunikationsschnittstellen (V2X-Unit)?
  - Datenspeicher (StVG)?
  - …

§ 63a Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion

(1) Kraftfahrzeuge mit hoch- oder vollautomatisierter Fahrfunktion gemäß § 1a zeichnen nach dem Stand der Technik entsprechend der internationalen Vorgaben jeweils auf, ob das Kraftfahrzeug durch den Fahrzeugführer oder mittels hoch- oder vollautomatisierter Fahrfunktionen gesteuert wird. Wird der Fahrzeugführer durch das hoch- oder vollautoma-

Änderung Straßenverkehrsgesetz

Ausblick Automotive Security

- Standardisierung und Regulierung, z.B.
  - ISO (TC22) „Automotive Security Engineering“
  - ISO (TC204) „Intelligent Transport Systems – Cooperative ITS – Common Approaches to Security“
  - UNECE WP.29 Harmonization of Vehicle Regulations, Working Group ITS/AD
  - Guideline Certificate Policy, Security Policy der C-ITS-Plattform
- Wechselwirkungen mit automatisiertem Fahren?
- Privatsphäre und Datenschutz
  - *Transparenz gegenüber Fahrer erforderlich*
  - *Wahlfreiheit des Fahrers sicherstellen*

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Christian Wieschebrink
christian.wieschebrink@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik
Referat D 33 - Cyber-Sicherheit für die Digitalisierung
in Verkehr und Industrie 4.0
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik