bast
Bundesanstalt für Straßenwesen

„Wie kann die PKI die Authentizität und Integrität sicherstellen? “

KOTAM Workshop

Safety & Security im Kontext von C-ITS-Diensten

30.11.2023 | Hamburg

Überblick

- C-ITS Zertifikate
- PKI - „Public Key Infrastructure“
- Gemeinsame Regeln
- Zusammenfassung

Überblick

- C-ITS Zertifikate
  - Was, wie und wozu?
- PKI - „Public Key Infrastructure“
  - Was ist das, welche Aufgaben gibt es und wie läuft das ab?
- Gemeinsame Regeln
  - Wozu dienen die (eur.) Regelwerke/Policies?
- Zusammenfassung

Zertifikate

- Was ist ein digitales Zertifikat?
  - Wikipedia:
    Ein digitales Zertifikat ist ein digitaler Datensatz, meist nach Standards der ITU-T oder der IETF, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten. Das Zertifikat wird ausgestellt durch eine Zertifizierungsstelle, die Certification Authority (CA).
- Viele relevante Punkte, nachfolgend kurz angerissen

C-ITS Zertifikate

- Wie sehen die Zertifikate aus?
- „Digitaler Datensatz“
- Standardisierte Struktur – ETSI TS 103 097
  - Gültigkeitszeitraum
  - Berechtigungen (SSPs)
  - Public Key – der „öffentliche“ Schlüssel
  - Name der ausstellenden CA
  - Signatur der austellenden CA
  - …

```
value EtsiTs103097Certificate ::= {
  version 3,
  type explicit,
  issuer self : sha384,
  toBeSigned {
    id name : "EU-TLM_L0",
    cracaId '000000'H,
    crlSeries 0,
    validityPeriod {
      start 548114403,
      duration years : 4
    },
    appPermissions {
      {
        psid 624,
        ssp bitmapSsp : '01C8'H
      }
    },
    verifyKeyIndicator verificationKey : ecdsaBrainpoolP384r1 : compressed-y-1 :
'50F275F27AB3A08F9DCDCF6822DBB53348C520FD8CC1F20AB9CD3FA4C6F31774AE1814'H -- truncated --
  },
  signature ecdsaBrainpoolP384r1Signature : {
    rSig x-only : '0D90C99B4F275AB7BB53C5F9D8D4E4D6C352A4D636299B0CCD93EEE60B370DBC954FA4'H --
truncated --,
    sSig '5A7CE1D63B851EEA6F967CA208A0486F5A19494BE4F7C95701284E24777706578D1333'H -- truncated --
  }
}
```

C-ITS Zertifikate

- Wozu werden die Zertifikate genutzt?
  - Wikipedia:

    - Eigenschaften von Personen / Objekten bestätigen

      SSPs: Dienstespezifisch für Einsatzfahrzeuge (DENM),

      Lichtsignalanlagen (SPAT/SSEM), ÖPNV (SREM), private PKW…

    - *Authentizität* und *Integrität*

      durch *kryptographische Verfahren* sicherstellen

- Was bedeutet das genau?

Kryptographischer Hintergrund – Teil 1

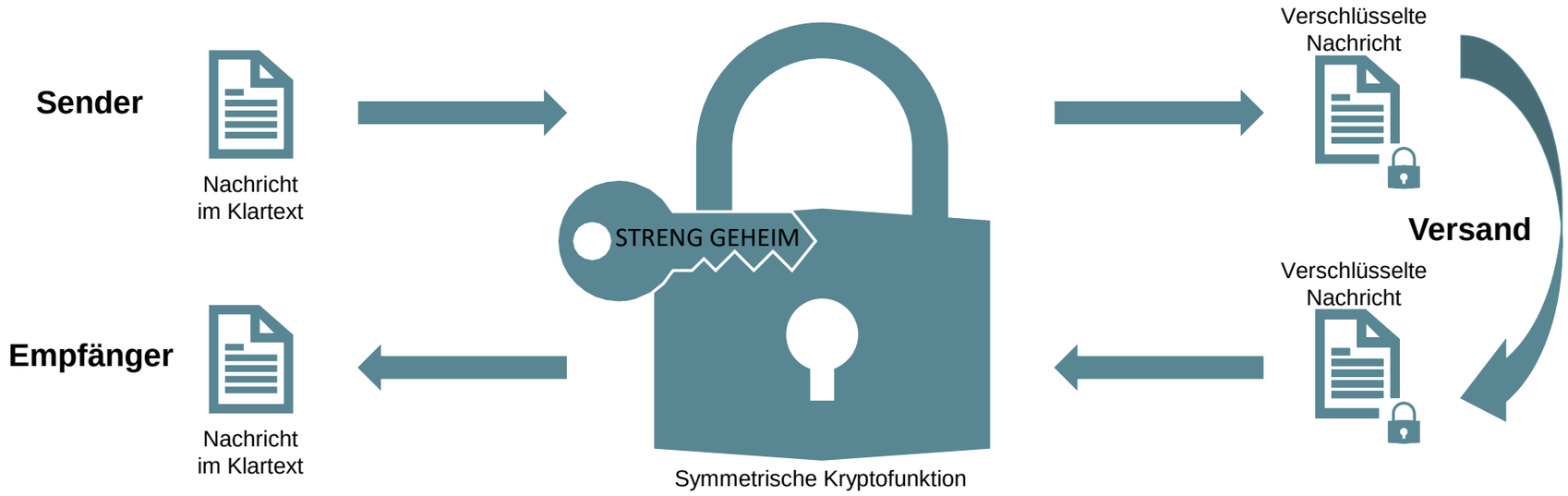
- *Symmetrische* Kryptografie: ein *gemeinsamer geheimer Schlüssel*
- Verschlüsselung zwischen Sender / Empfänger → Ziel: „Vertraulichkeit“

Beispiel: Cäsar-Chiffre

Quelle: https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung

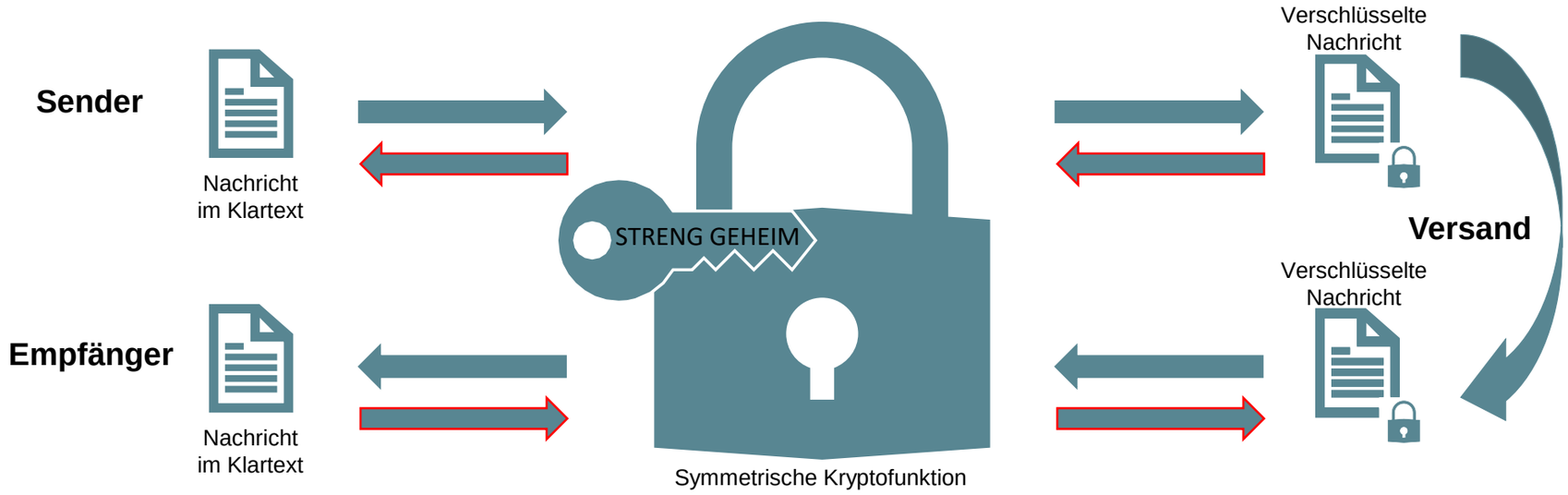
Kryptographischer Hintergrund – Teil 1

- *Symmetrische* Kryptografie: ein *gemeinsamer geheimer Schlüssel*
- Verschlüsselung zwischen Sender / Empfänger → Ziel: „Vertraulichkeit“



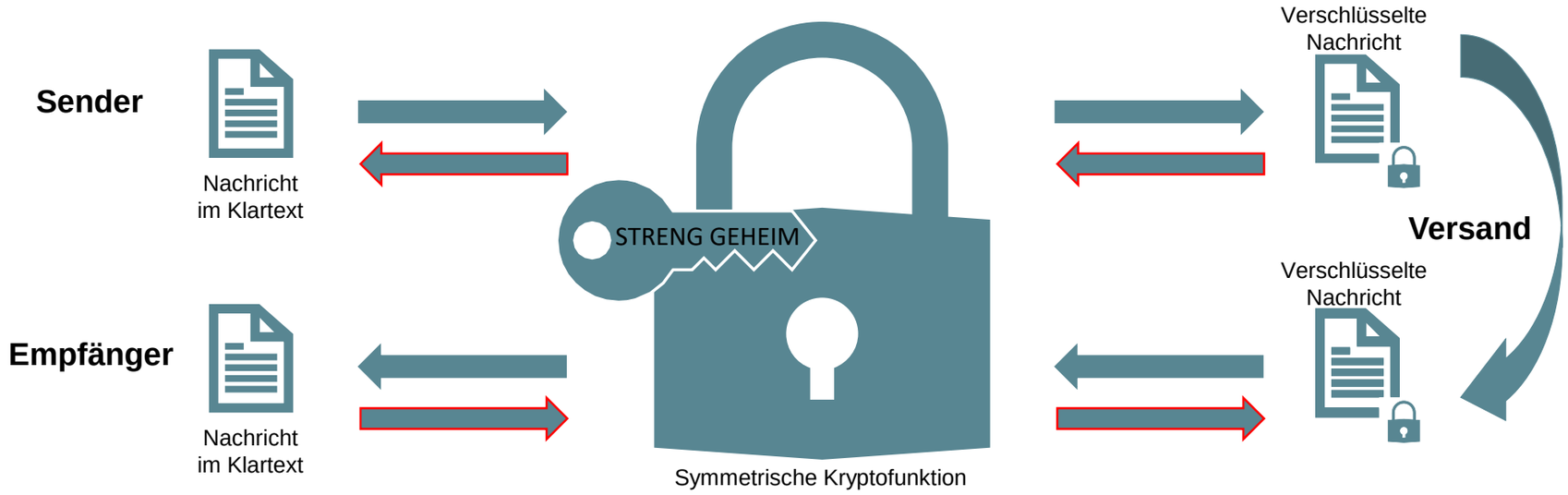
Kryptographischer Hintergrund – Teil 1

- *Symmetrische* Kryptografie: ein *gemeinsamer geheimer Schlüssel*
- Verschlüsselung zwischen Sender / Empfänger → Ziel: „Vertraulichkeit“
- Versand über unsicheren Kanal möglich, solange der Schlüssel geheim bleibt



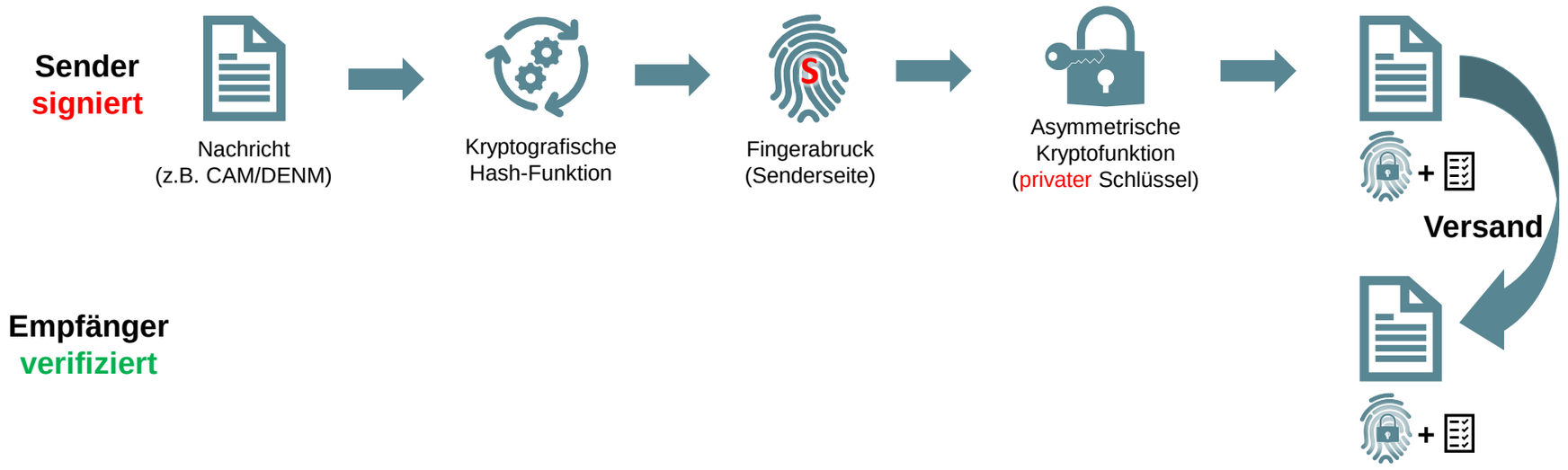
Kryptographischer Hintergrund – Teil 1

- *Symmetrische* Kryptografie: ein *gemeinsamer geheimer Schlüssel*
- Verschlüsselung zwischen Sender / Empfänger → Ziel: „Vertraulichkeit“
- Versand über unsicheren Kanal möglich, solange der Schlüssel geheim bleibt
- Wie verteilt man den Schlüssel auf sichere Weise?



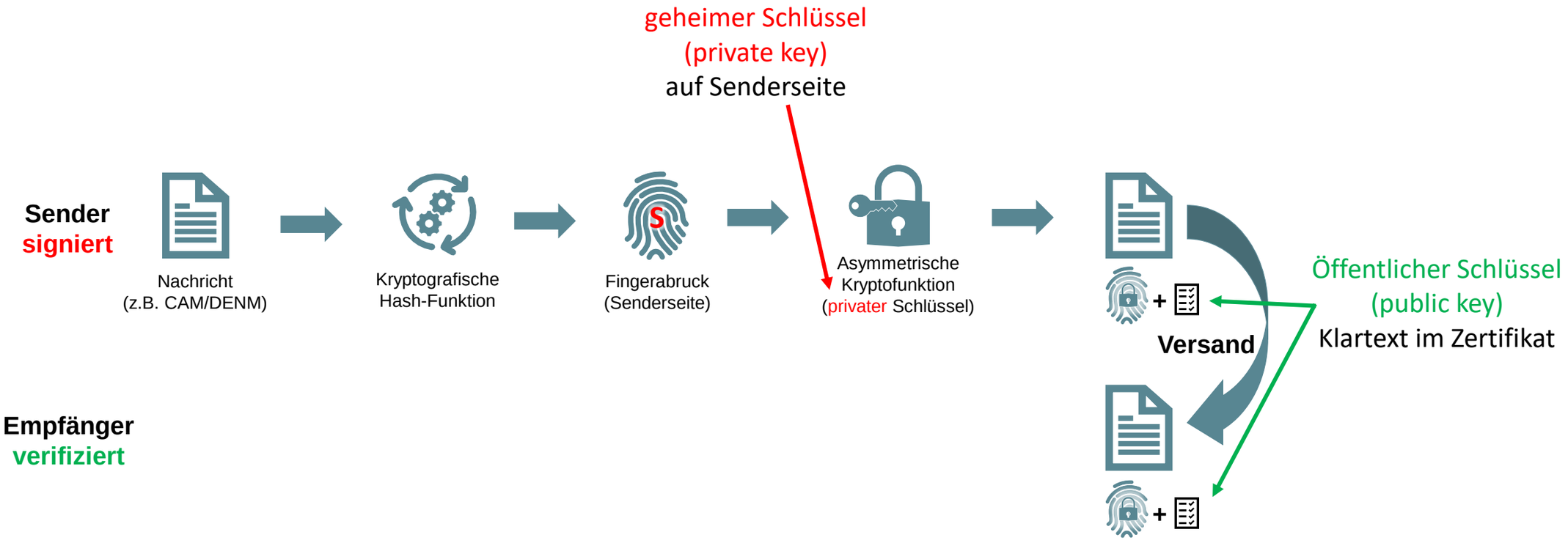
Kryptographischer Hintergrund – Teil 2

- Zertifkatsbasierte, *asymmetrische* Kryptografie nutzt *unterschiedliche Schlüssel*



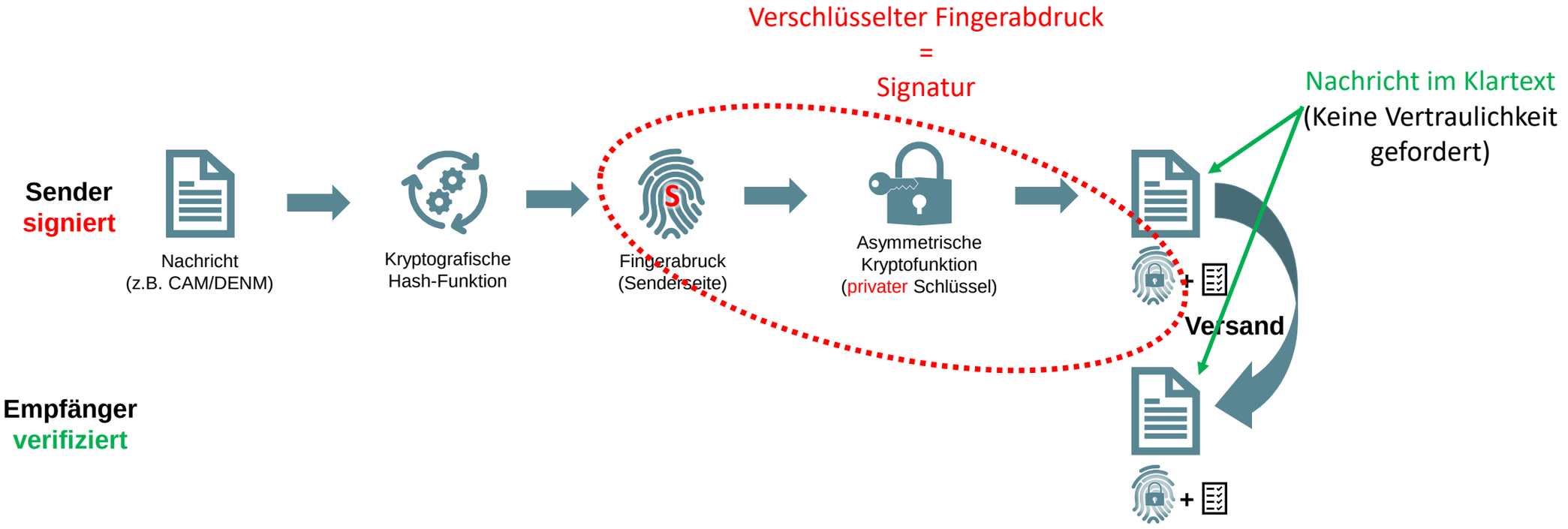
Kryptographischer Hintergrund – Teil 2

- Zertifkatsbasierte, *asymmetrische* Kryptografie nutzt *unterschiedliche Schlüssel*



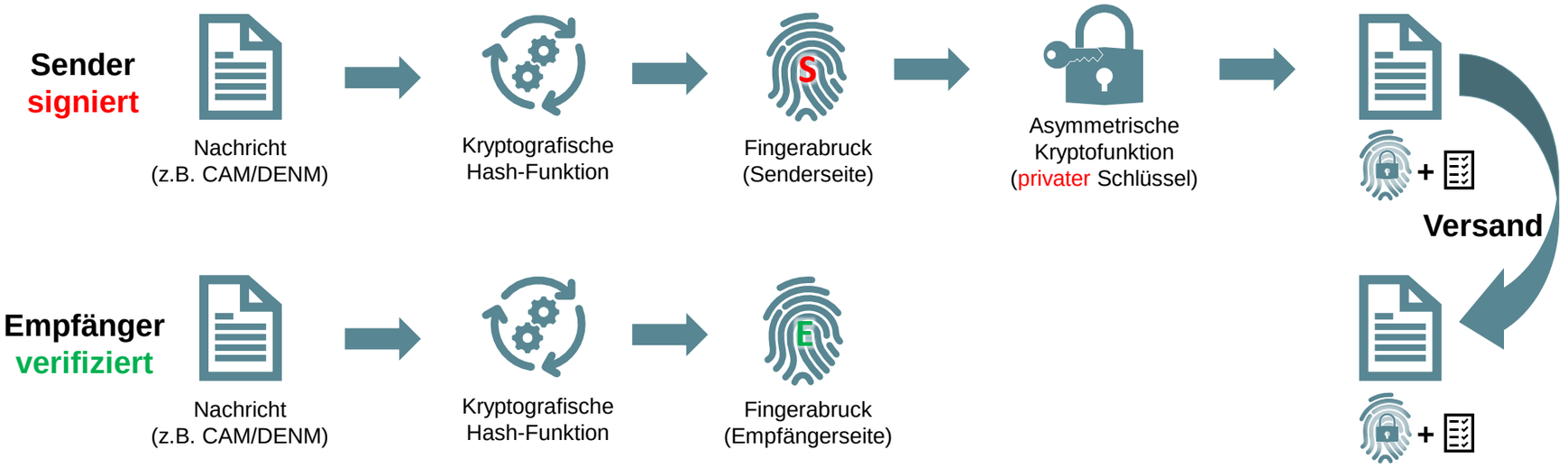
Kryptographischer Hintergrund – Teil 2

- Zertifkatsbasierte, *asymmetrische* Kryptografie nutzt *unterschiedliche Schlüssel*
- Für C-ITS Nachrichten: Schutz von Authentizität & Integrität angestrebt



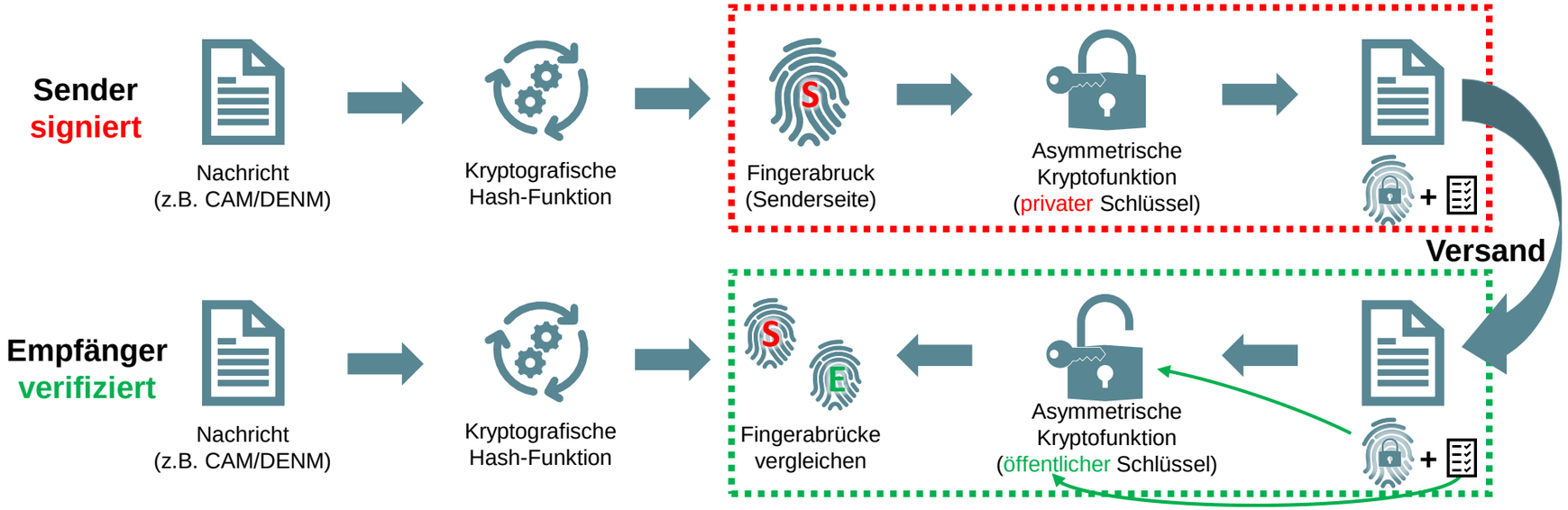
Kryptographischer Hintergrund – Teil 2

- Zertifkatsbasierte, *asymmetrische* Kryptografie nutzt *unterschiedliche Schlüssel*
- Für C-ITS Nachrichten: Schutz von Authentizität & Integrität angestrebt



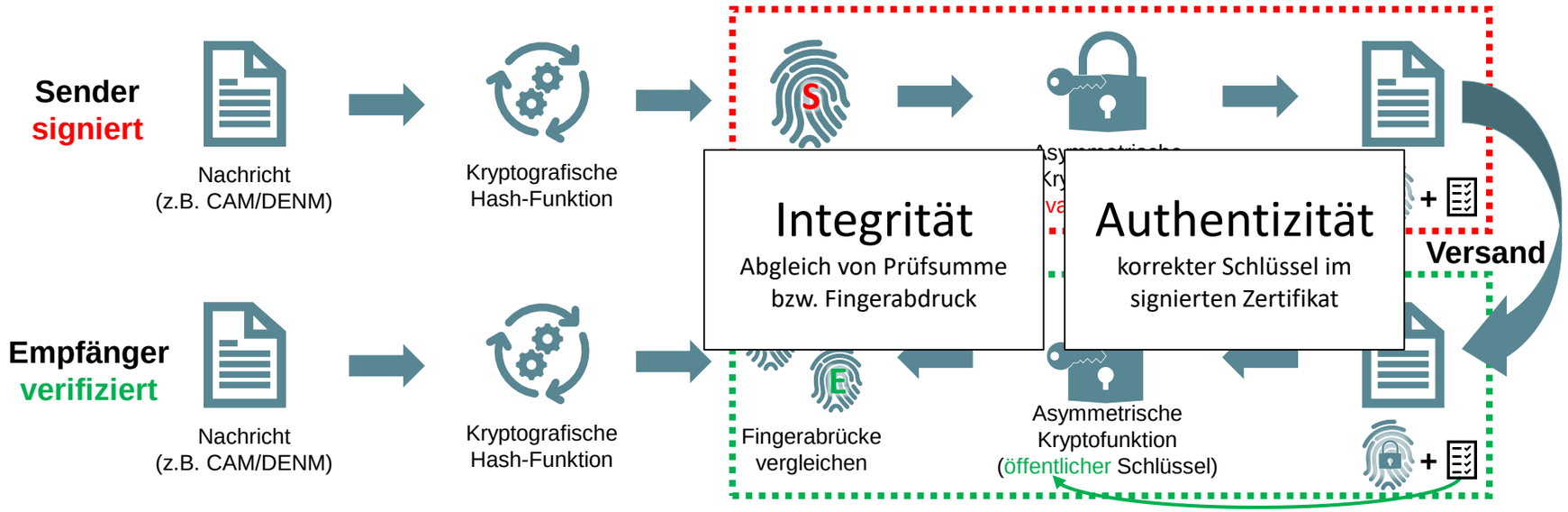
Kryptographischer Hintergrund – Teil 2

- Zertifkatsbasierte, *asymmetrische* Kryptografie nutzt *unterschiedliche Schlüssel*
- Für C-ITS Nachrichten: Schutz von Authentizität & Integrität angestrebt



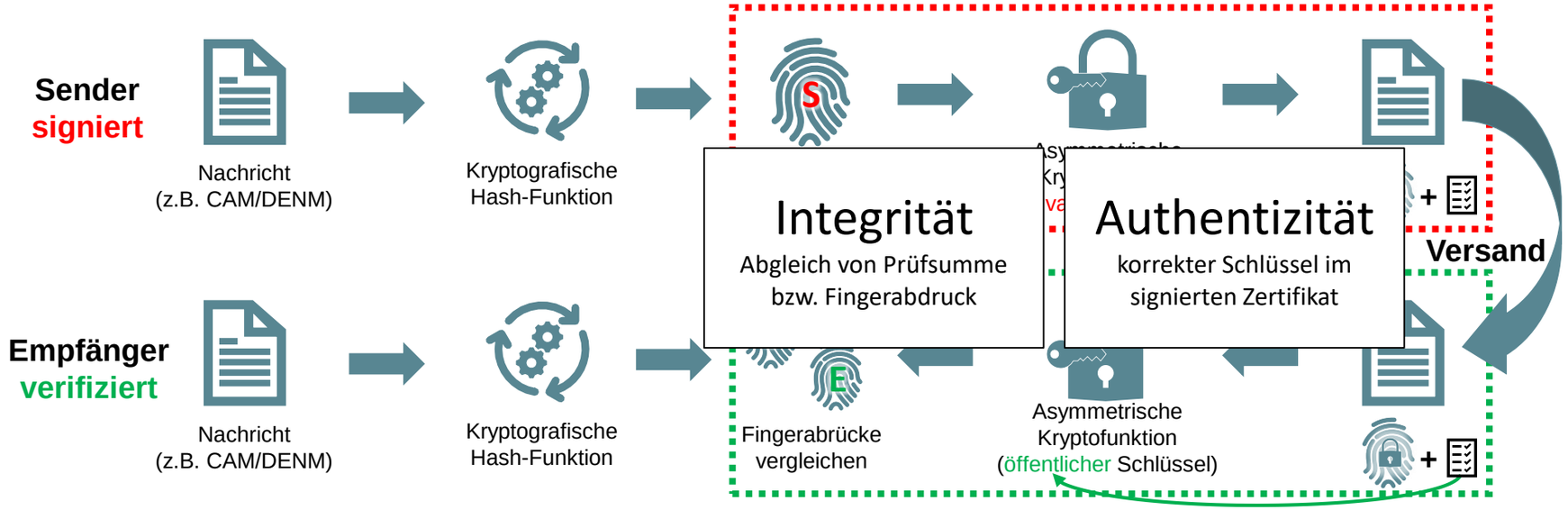
Kryptographischer Hintergrund – Teil 2

- Zertifkatsbasierte, *asymmetrische* Kryptografie nutzt *unterschiedliche Schlüssel*
- Für C-ITS Nachrichten: Schutz von Authentizität & Integrität angestrebt



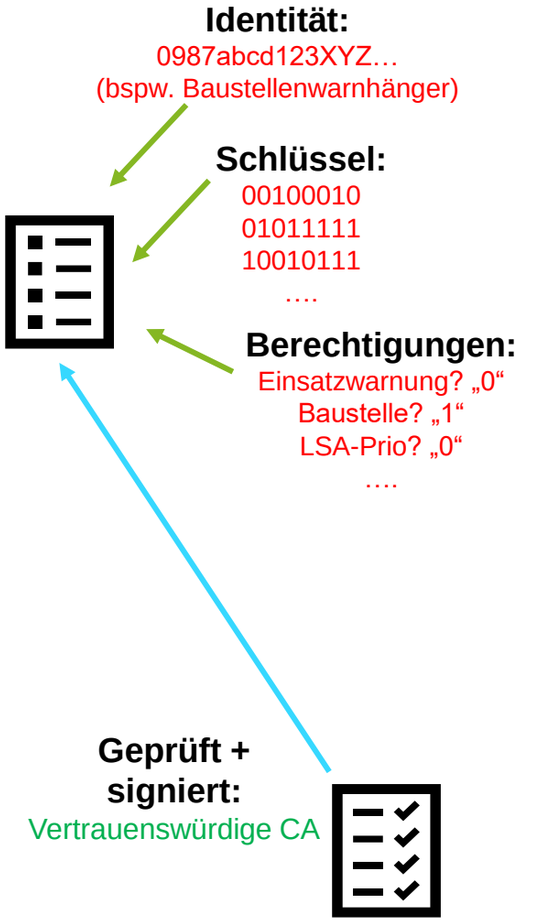
Kryptographischer Hintergrund – Teil 2

- Zertifkatsbasierte, *asymmetrische* Kryptografie nutzt *unterschiedliche Schlüssel*
- Für C-ITS Nachrichten: Schutz von Authentizität & Integrität angestrebt
- Vertrauen in Identitäten/Eigenschaften durch Zertifikate, doch wie verteilt man diese Zertifikate → Vertrauensanker PKI



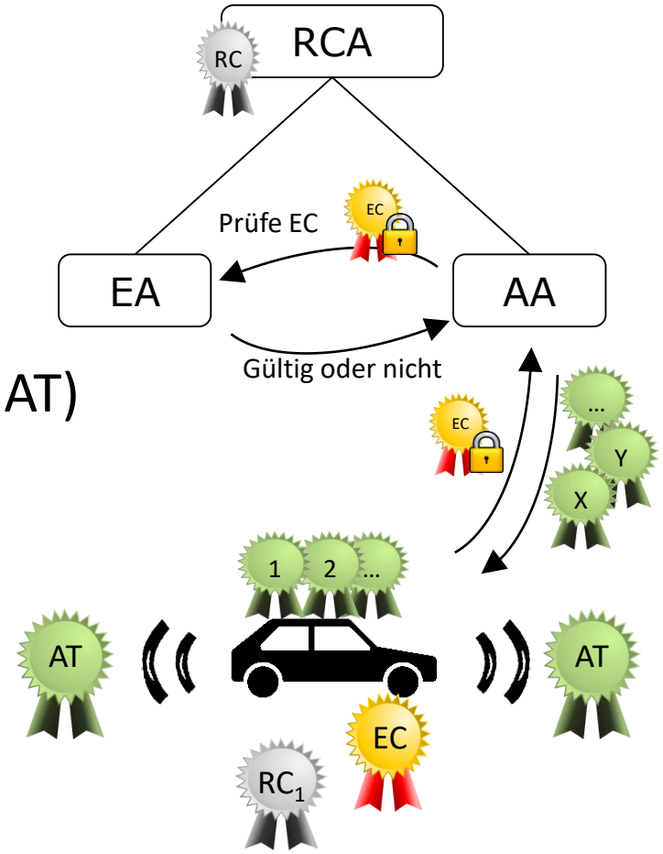
PKI – Public Key Infrastructure

- Zertifikate werden von einer CA herausgegeben/signiert
  - Zertifikate verknüpfen (öffentliche) Schlüssel mit Identitäten
  - Zertifikate können weitere Informationen enthalten
  - Zertifikate existieren in verschiedenen Formaten
- PKI = (kryptografisches) System mit einheitlichen Regeln
  - Zertifikate ausstellen – durch CAs
  - Zertifikate verteilen – Server / Repositories
  - Zertifikate prüfen ggf. revozieren – Zertifikatslisten
- Technische Maßnahmen und deren Umsetzung
- Auch organisatorische Maßnahmen erforderlich



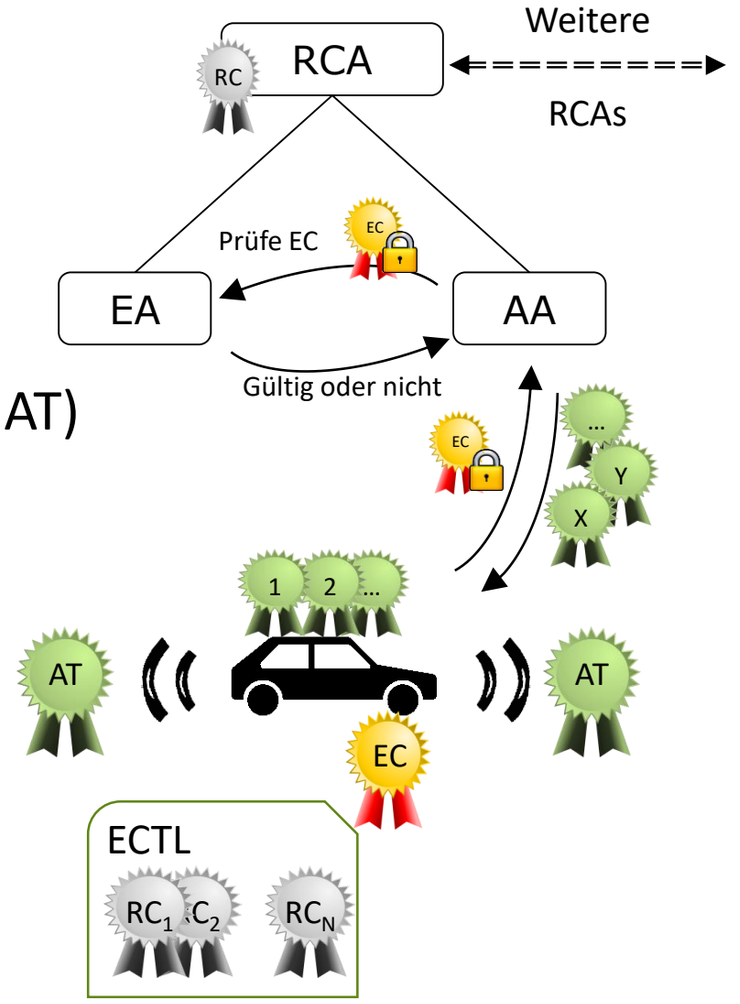
C-ITS PKI – ein verteiltes System

- Root Certificate Authority (RCA)
  - Gibt der PKI Rahmenbedingungen (Policy) (Algorithmus, Zertifikate, Schlüssel…)
  - Sicherheit durch RCA Policy definiert
- Pseudonyme Kurzzeit-Zertifikate (Authorisation Tickets AT)
  - Ausgestellt von der Authorisation Authority (AA)
  - „Ausweis“ gegenüber anderen Fahrzeugen
  - Kurze Gültigkeit, mehrere verfügbar
- Langzeit-Zertifikate (Enrolment Credentials EC)
  - Ausgestellt von Enrolment Authority (EA)
  - „Ausweis“ für Erhalt neuer ATs von AA
  - Gültigkeit nur durch EA überprüfbar



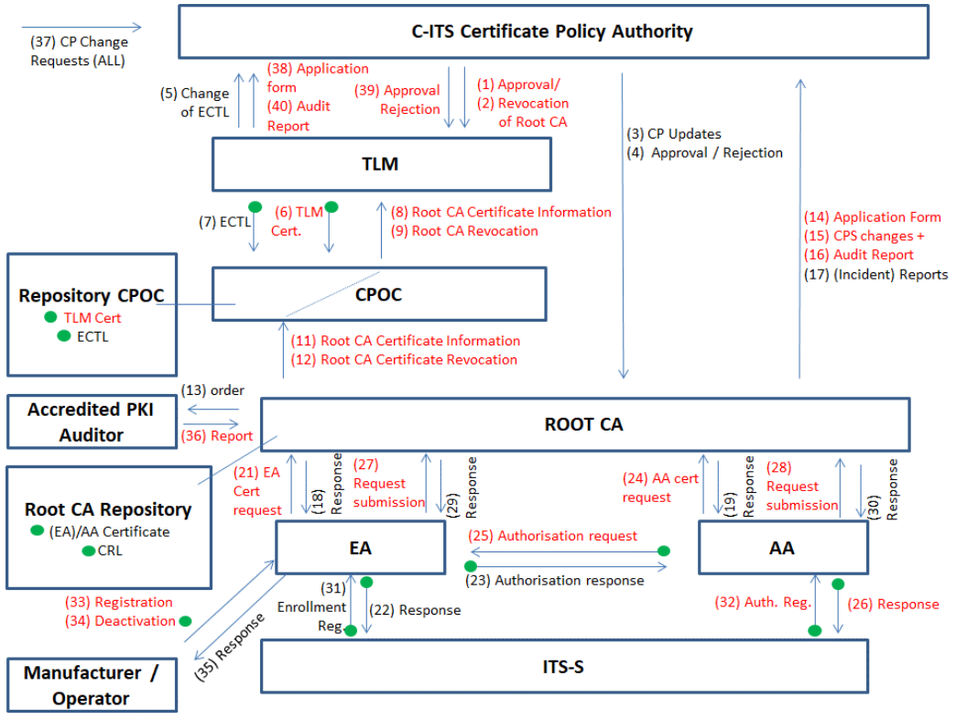
C-ITS PKI – ein verteiltes System

- Root Certificate Authority (RCA)
  - Gibt der PKI Rahmenbedingungen (Policy) (Algorithmus, Zertifikate, Schlüssel…)
  - Sicherheit durch RCA Policy definiert
  - „Cross-Certification“ möglich – gemeinsame Regeln
- Pseudonyme Kurzzeit-Zertifikate (Authorisation Tickets AT)
  - Ausgestellt von der Authorisation Authority (AA)
  - „Ausweis“ gegenüber anderen Fahrzeugen
  - Kurze Gültigkeit, mehrere verfügbar
- Langzeit-Zertifikate (Enrolment Credentials EC)
  - Ausgestellt von Enrolment Authority (EA)
  - „Ausweis“ für Erhalt neuer ATs von AA
  - Gültigkeit nur durch EA überprüfbar



C-ITS Trust Model – europäischer PKI-Verbund

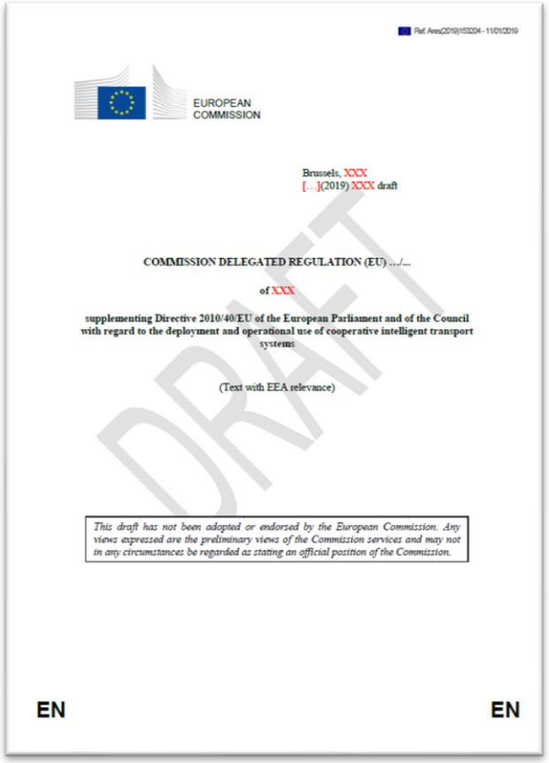
- Certificate Policy (Regeln für PKI) und Security Policy (Regeln für Stationen & Betreiber)
  - Ursprünglich Anhänge zur del. VO
  - Fortschreibung in Expert Group E01941
    - SP Update 2022/2023
    - CPOC Protocol Update 2023
    - CP Update in Arbeit
  - Point of Contact @ JRC der EU KOM: https://cpoc.jrc.ec.europa.eu/
- Policies schaffen gemeinsame Vertrauensgrundlage
  - Grundlegende Prozesse, Regeln & Anforderungen
  - CPA – Certificate Policy Authority (alle Akteure)
  - TLM – Trust List Manager (stellt die EU KOM)
  - ECTL – European Certificate Trust List (Tool)



Quelle: https://cpoc.jrc.ec.europa.eu/

Profile im Entwurf der Delegierten VO zu C-ITS

- Rahmen zur Einführung koop. Systeme (ergänzend zu 2010/40/EU)
- Zielsetzung der del. VO: Interoperabilität und rechtlicher Rahmen
- Harmonisierte Profile im Anhang (C-Roads für I2V, Car2Car für V2V/V2I)


EUROPEAN COMMISSION

Brussels, XXX
[...](2019) XXX draft

COMMISSION DELEGATED REGULATION (EU) .../...

of XXX

supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems

(Text with EEA relevance)

DRAFT

This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.

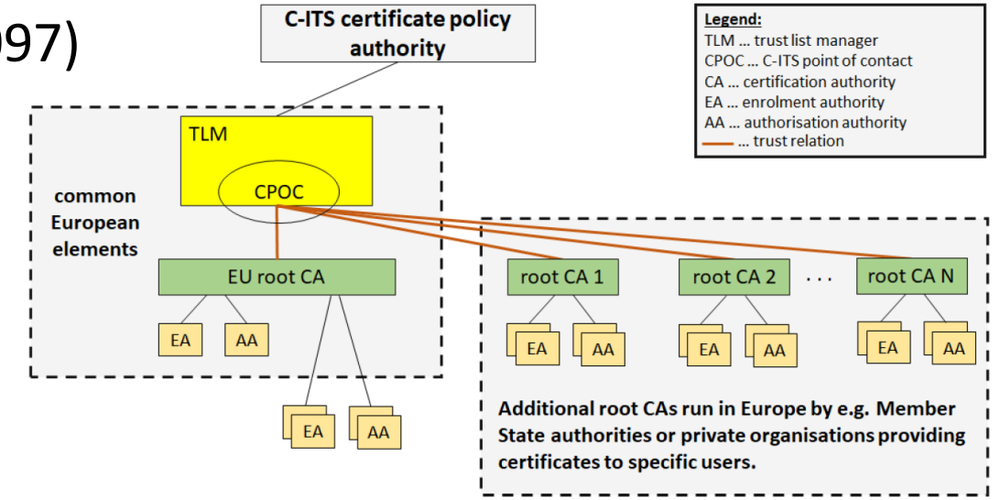
EN EN

- <u>Historie</u>
  - Delegierte VO von EU KOM vorgelegt (13.03.2019)
  - Durch EP angenommen (Widerspruch ohne Mehrheit, 17.04.2019)
  - Durch eur. Rat abgelehnt (04.07.2019)

- Keine rechtliche Grundlage, aber nach wie vor gemeinsame* Arbeitsgrundlage
  - *vgl. http://c-its-deployment-group.eu/

C-ITS Trust Model – europäischer PKI-Verbund

- Hierarchische, verteilte PKI-Systeme auf eur. Ebene
  - Trust Model in Policy Dokumenten niedergeschrieben
  - EU KOM betriebt zentralen Vertrauensanker
- Zertifikatsbasiert, inkl. Berechtigungen (ETSI TS 103 097)
  - Dienstespezifisch (z.B. Polizei vs privater PKW)
  - Chain of Trust muss geprüft werden
- Funktionale Interoperabilität nicht zu vergessen
  - IT-Sicherheit ist kein Selbstzweck („signed garbage“)
- Auch Anforderungen an Komponenten wichtig
  - CC-zertifiziertes HSM für Schlüsselmaterial – für PKI und Stationen (RSU/OBU)
  - CC-zertifizierte Kommunikationseinheiten
- DE: BSI-Anforderungen („Guidance“ TR-03164, auf Policies aufsetzend)



Quelle: https://cpoc.jrc.ec.europa.eu/

Zusammenfassung

- Zertifikate bestätigen Authentizität (Eigenschaften / Identitäten)
  → Standardisierte kryptographische Systeme sichern dieses Vertrauen ab
  → Gesprächspartner „authentisch“ (wenn auch unbekannt/pseudonym)
- Signaturen sichern inhaltliche Integrität ab
  → Integrität jeder einzelnen Nachricht erforderlich
  → Veränderungen und Übertragungsfehler werden erkannt
- Eine PKI ist erforderlich, um Zertifikate zu managen
  → Erstellung, Verteilung, Prüfung, Revokation
  → Verteilte Systeme sind flexibel und leistungsfähig
- Gemeinsame Regeln sind erforderlich
  → Policies und Mechanismen (TLM, ECTL…) sichern Interoperabilität
  → Mindestanforderungen für alle Betreiber

bast
Bundesanstalt für Straßenwesen

→ Gemeinsame Diskussion