TeleTrusT
Pioneers in IT security.

Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 13.06.2013

Elektromobilität
- Sicher und überall tanken

Dipl. Inf. Harry Knechtel (FH), secunet

secunet Security Networks AG

Bereich Automotive Security

Elektromobilität - Sicher und überall tanken

Erfahrungen aus der ISO15118

Juni 2013

Premium IT-Sicherheit Made in Germany

- **secunet …**
  - Einer der führenden Spezialisten für innovative und anspruchsvolle IT-Sicherheit
- **Kunden …**
  - Über 500 nationale und internationale Referenzen aus dem öffentlichen Sektor, Großkonzernen und Mittelstand
  - Darunter viele DAX-Unternehmen und zahlreiche Bundes- und Landesministerien
- **Erfahrung …**
  - Erfahrung und Expertise aus über 5.000 namhaften, nationalen und internationalen Referenzprojekten über alle Branchen
- **Partnerschaften …**
  - Sicherheitspartner der Bundesrepublik Deutschland
  - Enge Kooperationen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesministerium des Innern (BMI)
  - Vertrautes und partnerschaftliches Verhältnis mit Anbietern / Herstellern als auch mit Einrichtungen für Forschung und Entwicklung

Standards im Umfeld e-Mobility

Derzeit existieren diverse Standards im Umfeld „e-Mobility“:

- **ISO 15118** (Part 2: V2G Charge Protocol – Message & Protocols)
- **ETSI TS 101 556-1** (Electric Vehicle Charging Spot Notification)
- **OCPP** (Open Charge Point Protocol)
- **OCHP** (Open Clearing House Protocol)
- E-Mobility-ID-Schemata_DRAFT_1.0
- ...

Historie secunet / ISO 15118

2009

- Erste Gespräche mit verschiedenen OEMs und EVUs
- Konzeption Förderprojekt „Clearing House“ zum Nachweis der Abrechenbarkeit (incl. Roaming) von Strom in der e-Mobility

2010

- Review / Sicherheitsanalyse eines Ladeprotokolls für einen deutschen EVU / OEM
- Aufnahme secunet in die PT5 der ISO/IEC JWG V2G (ISO 15118)
- Mitarbeit in der ISO 15118 (Sicherheitskonzept, Zertifikatsprofile, Algorithmenauswahl, …)

2011

- PT übergreifende Unterstützung der ISO/IEC JWG V2G (ISO 15118)
- OEM PoC Implementierung der EV, EVSE und SA Komponenten der ISO15118 für einen OEM

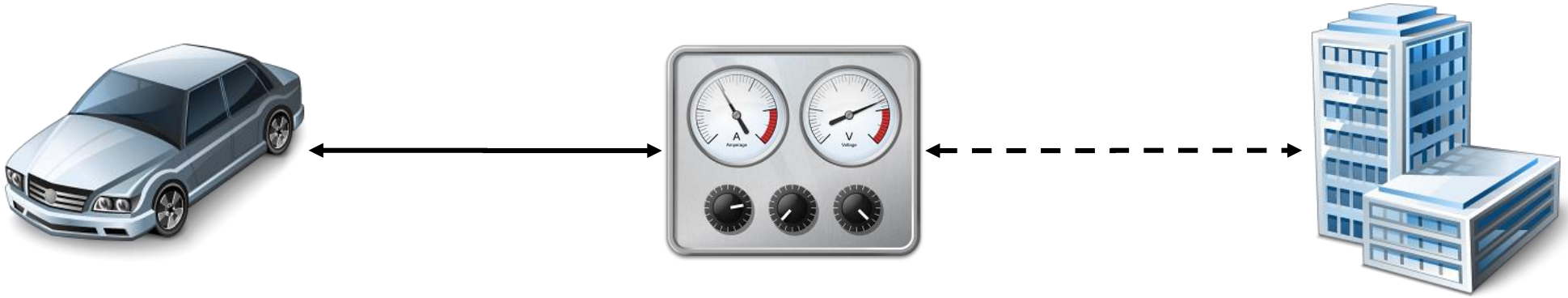
2012

- Konzept & Implementierung einer eMOB PKI für einen deutschen OEM
- Weiterentwicklung des OEM PoC zur Serienreife

2013

- Implementierung der weltweit ersten produktiven ISO 15118 Root CA

ISO 15118 – Sicher und überall tanken



Die ISO 15118 definiert die gesteuerte Ladekommunikation zwischen Fahrzeug und Ladeinfrastruktur.

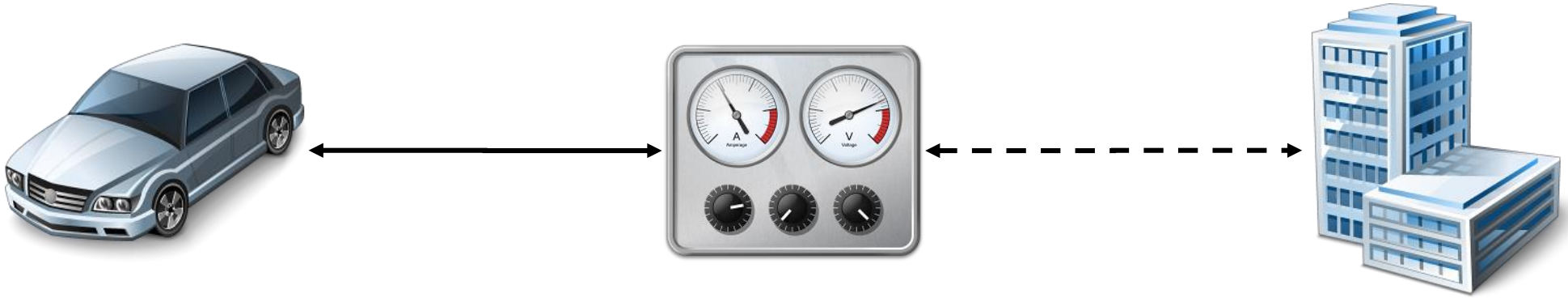
Der Ablauf gliedert sich grob in drei Schritte:

- Aufbau der Verbindung
- Auswahl der Dienstleistung
- Eigentlicher Ladevorgang

Die ISO 15118 deckt dabei verschiedene Einsatz-Szenarien ab:

- Gleichstrom- / Wechselstrom-Laden
- Laden an öffentlichen Orten (Ladestation) / in privater Umgebung (Wallbox)
- Bezahlen an der Ladestation oder automatisch am Fahrzeug (Plug‘n Charge)

Schutz-Ziele der ISO 15118



Schutz-Ziele der ISO 15118:

- Schutz von Fahrzeug und Infrastruktur vor Beschädigung
- Schutz vor Manipulation und Betrug
- Verfügbarkeit der Dienstleistung

Das Sicherheitskonzept der ISO 15118 basiert auf:

- Absicherung der Kommunikation zwischen Fahrzeug und Ladesäule
- Absicherung von Nutzdaten auf Applikations-Ebene
- Starker Authentisierung mittels PKI

Mögliche Angriffspunkte:

Endgeräte/Systeme:

Auto, Ladesäule, Backend…

Übertragung:

EV-EVSE, EVSE – Backend

secunet

Begriffserklärung

Schlüssel

Geheimer Anteil eines asymmetrischen
Schlüssel-Paares (privater Schlüssel) – oder ein symmetrischer Schlüssel

Zertifikat

Öffentlicher Anteil eines asymmetrischen Schlüssel-Paares
verbindlich bestätigt durch ein vertrauenswürdige Instanz

Key Pair

Kombination aus privatem Schlüssel und Zertifikat

Certification
Authority

Vertrauenswürdige Instanz die Schlüssel beglaubigt,
kann je nach Rolle ein „Root“ oder eine „normale“ CA sein

Begriffserklärung

PKI

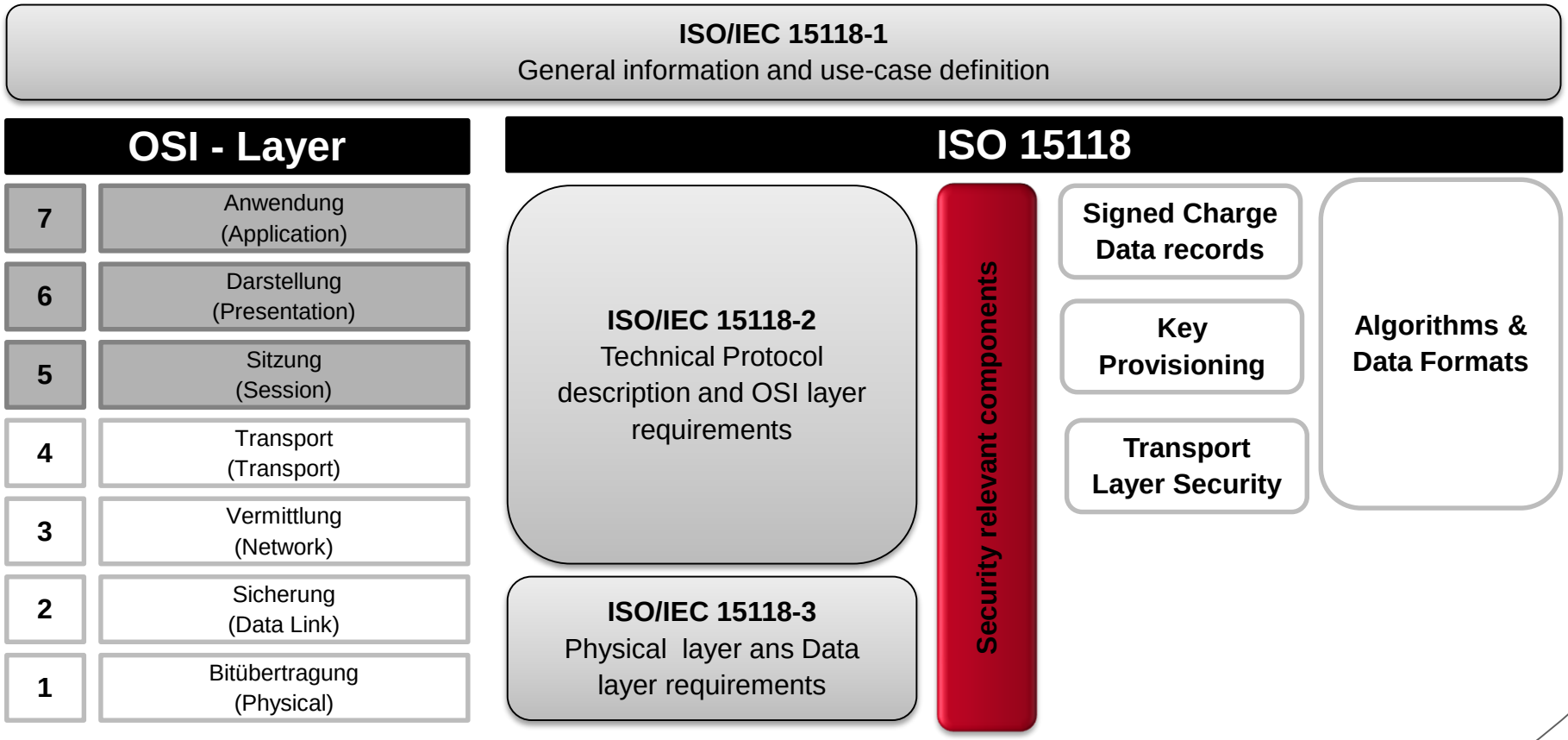
=

Public Key Infrastructure

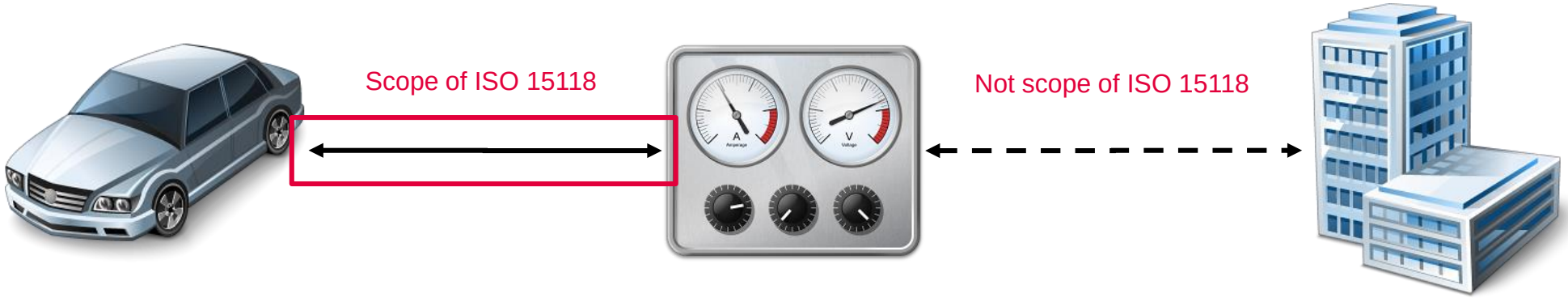
- Asymmetrische Kryptografie
- Schlüsselpaare / Key Pairs
- Öffentliche / Private Schlüssel
- Zertifikate

- Root, CA, RA, Trust Center
- Sperrlisten, CRL, OCSP, TSS
- Verzeichnisdienste / Directory
- Anwendung

Struktur der ISO 15118

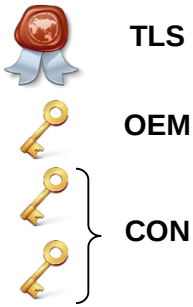


Wo spezifiziert die ISO 15118 ?



PT2 / PT5

- Einzusetzende Algorithmen und Schlüssel



TLS

OEM

CON

PT2 / PT3 / PT4

- Use Cases für AC und DC Charging
- Technische Details zu Physical, Data Link, Network, Session und Presentation Layer
- Network Layer: TLS
- Presentation Layer: XML/EXI

PT2 / PT5

- Einzusetzende Algorithmen und Schlüssel

CON

TLS

PT2

- Abstrakte Spezifikation der Nutzdaten (z.B. Tariftabelle)
- Keine technischen Vorgaben

PT2 / PT5

- Einzusetzende Algorithmen und Schlüssel

CON

OEM

PKI Rollen nach ISO 15118 (Arbeitsstand)

- **OEM**: Fahrzeughersteller
  Spielt Fahrzeug spezifische Provisioning Keys (incl. Zertifikat) ins Fahrzeug ein.
  Die Zertifikatskette der Provisioning Key Zertifikate wird vom Fahrzeug nicht geprüft.

- **Charge Point Operator (CPO)**: Betreiber der Ladeinfrastruktur
  Ladesäulen weisen sich via TLS Server Authentifizierung gegenüber dem Fahrzeug aus.
  Die TLS Zertifikate muss das Fahrzeug bis zu einer bekannten Root prüfen können.

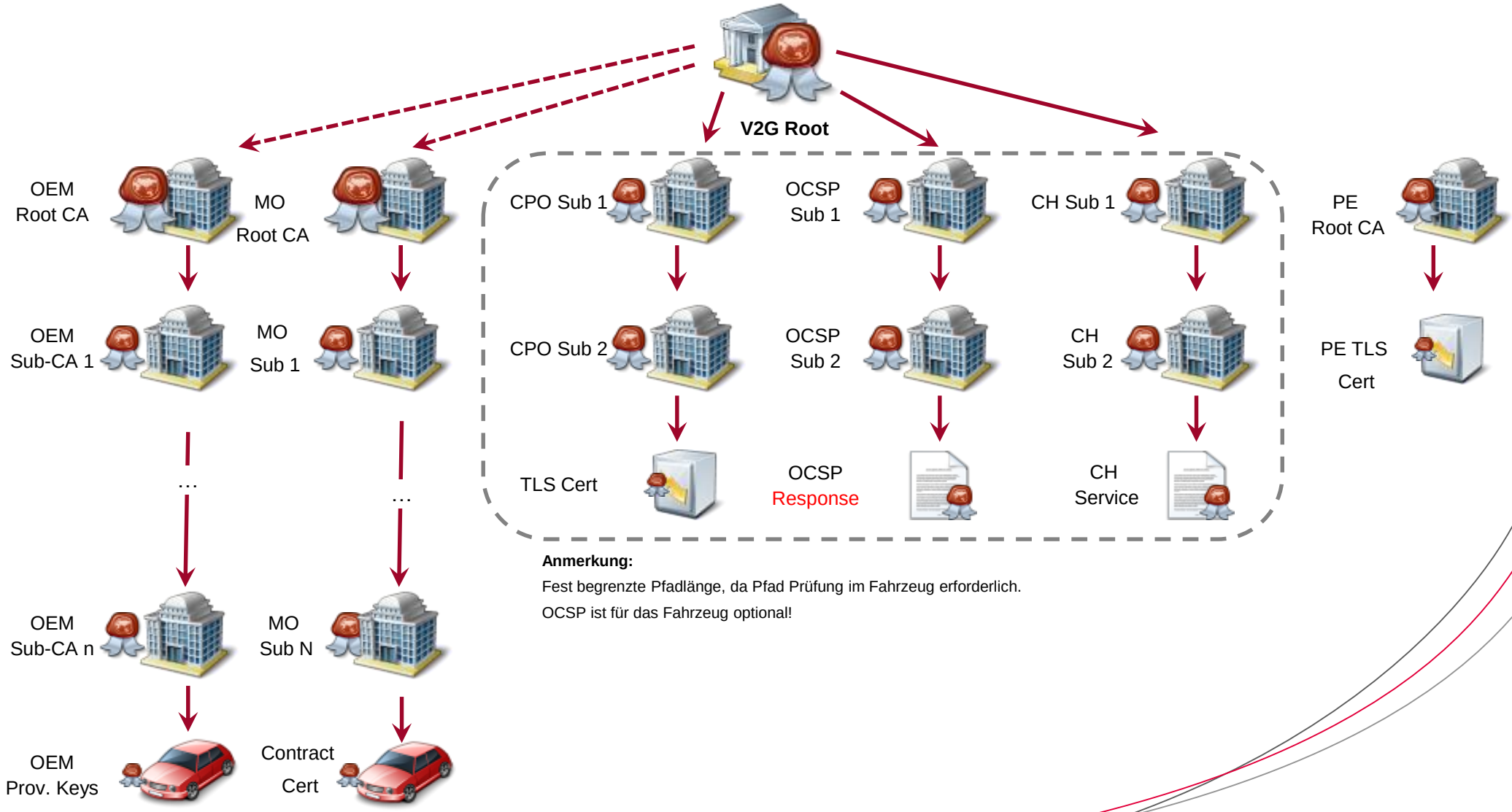
- **Mobility Operator (MO)**: Anbieter für Stromverträge
  Für jeden Stromvertrag wird ein Contract Key/Cert ins Fahrzeug eingespielt.
  Die Contract Zertifkate müssen nicht zwingend bis zu einer bekannten Root vom Fahrzeug geprüft werden. Auf Ladesäulenseite werden die Contract Zertifikate bis zu einer vertrauenswürdigen Root geprüft.

- **Clearing House (CH) / Roaming**: Dienstleister für das Verteilen von Contract Keys
  Bei Key Installation / Update wird vom Fahrzeug nicht der neue Contract Schlüssel bis zur Root geprüft, sondern die Signatur der einbringenden Stelle. D.h. eine Prüfung des CH Zertifikats bis zu einer bekannten Root muss möglich sein.

- **OCSP**: Bereitstellung von Sperrinformationen
  OCSP ist aus Sicht des Fahrzeugs optional, falls geprüft wird ist aber eine Prüfung bis zu einer bekannten Root erforderlich

- **Wallbox / Priv. Envir.(PE)**: Betreiber einer Wallbox im „private environment“.
  Sonderlösung für Wallbox Einsatz. Das „Private Operator Root Certificate“ wird z.B. vom Wallboxhersteller erzeugt.
  Dieses Root Zertifikat muss im Fahrzeug hinterlegt werden.
- *Anmerkung: Bestimmte Rollen können im operativen Betrieb zusammenfallen, z.B. CH und MO*

ISO15118 V2G PKI (Arbeitsstand)

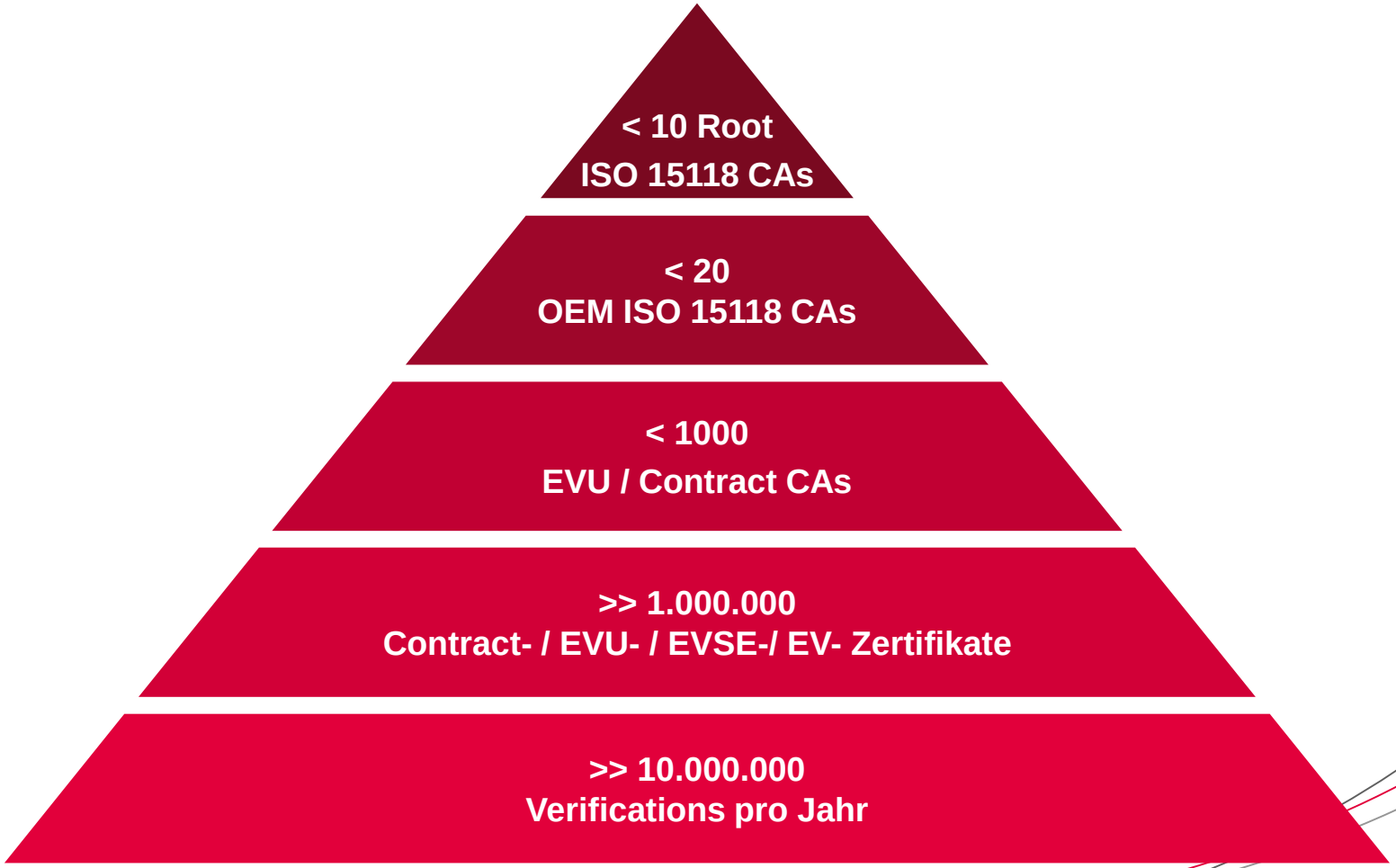


Anmerkung:

Fest begrenzte Pfadlänge, da Pfad Prüfung im Fahrzeug erforderlich.

OCSP ist für das Fahrzeug optional!

eMob PKI nach ISO 15118 – Mengenmodell



Was bedeutet ISO 15118 für den OEM?

- **Benötigte Kryptographie im Fahrzeug**
  - ECC Signing
  - ECC Verfication
  - ECC Key Exchange
  - AES
  - X.509 Certificate Handling → ASN.1, DER
- **Benötigte Protokolle**
  - TLS (EV – CP)
  - OCSP
  - XML, ISO 15118 Charge Protocol
  - XML, ISO 15118 Key Provisioning
- **Benötigte Infrastruktur**
  - CA / PKI for OEM Certificate Key Pair Generation
  - Personalisation / Key Distribution for OEM Certificates
- **Benötigte Prozesse**
  - Key Generation / Distribution
  - CA-Certification / Distribution
  - CA / OEM Key Revokation
  - Key / Zertifikate Update / Exchange

Was bedeutet ISO 15118 für den OEM?

- **Welche Schlüssel und Zertifikate werden im Fahrzeug benötigt?**
  - OEM Provisioning Keys

    - Private Key & Public Key Certificate
    - Public Key Certificate contains VIN7 within DN
    - Schlüssel müssen im Werk eingebracht werden

    - Beim SG Tausch müssen Schlüssel wieder eingebracht oder die neuen Schlüssel registriert werden (Fehleranfällig)
    - Schlüssel bzw. deren Public Key Zertifikate müssen zentral bei einem Clearing House registriert werden
  - Mobility Operator Contract Keys

    - Private Key & Public Key Certificate
    - Schlüssel müssen nach Vertragsabschluss eingebracht werden
    - Beim SG Tausch müssen Schlüssel wieder eingebracht werden oder die neuen Schlüssel registriert (Fehleranfällig)

    - Schlüssel bzw. das ganze Schlüsselpaar müssen sicher zentral bei einem Clearing House hinterlegt / registriert werden
  - Root Zertifikate

    - Root- und Sub CA Zertifikate zur Prüfung von Zertifikatsketten
    - Sicherer Rootschlüssel-Wechsel und Update erforderlich

Was bedeutet ISO 15118 für den OEM?

- **Detailbetrachtung OEM Provisioning Key – Fragestellungen**

  - Wo wird das Schlüsselpaar erzeugt?
    - Im Steuergerät – oder extern und der private Key dann ins SG übertragen ?
    - Beim OEM oder schon beim Zulieferer ?
  - Wann werden die Zertifikate erzeugt?
    - Da die VIN und der Public Key in das Zertifikat eingehen, kann das endgültige Zertifikat erst erzeugt werden wenn feststeht welcher private Key in welchem Fahrzeug verbaut wurde
  - Strategie für den SG-Tausch
    - Erneute Auslieferung bestehender Schlüssel (analog EWS)
    - Verwendung neuer Schlüssel mit entsprechender Rückdokumentation
  - Wie hoch ist der Schutzbedarf dieser Schlüssel ?
    - Was wären mögliche, sinnvolle Angriffe ?

Was bedeutet ISO 15118 für den CPO?

- **Benötigte Kryptographie im Charge Point (CP)**
  - ECC Signing
  - ECC Verfication
  - ECC Key Exchange
  - AES
  - X.509 Certificate Handling → ASN.1, DER
- **Benötigte Protokolle**
  - TLS (EV –CP, CP – Backend)
  - OCSP
  - XML, ISO 15118 Charge Protocol
  - XML, ISO 15118 Key Provisioning (nur durchreichen)
- **Benötigte Infrastruktur**
  - CA / PKI for CP Certificate Key Pair Generation
  - Personalisation / Key Distribution for CP Certificates
- **Benötigte Prozesse**
  - Key Generation / Distributtion
  - CA-Certification / Distribution
  - CA / CP Key Revokation
  - Key / Zertifikate Update / Exchange

Was bedeutet ISO 15118 für den Mobility Provider?

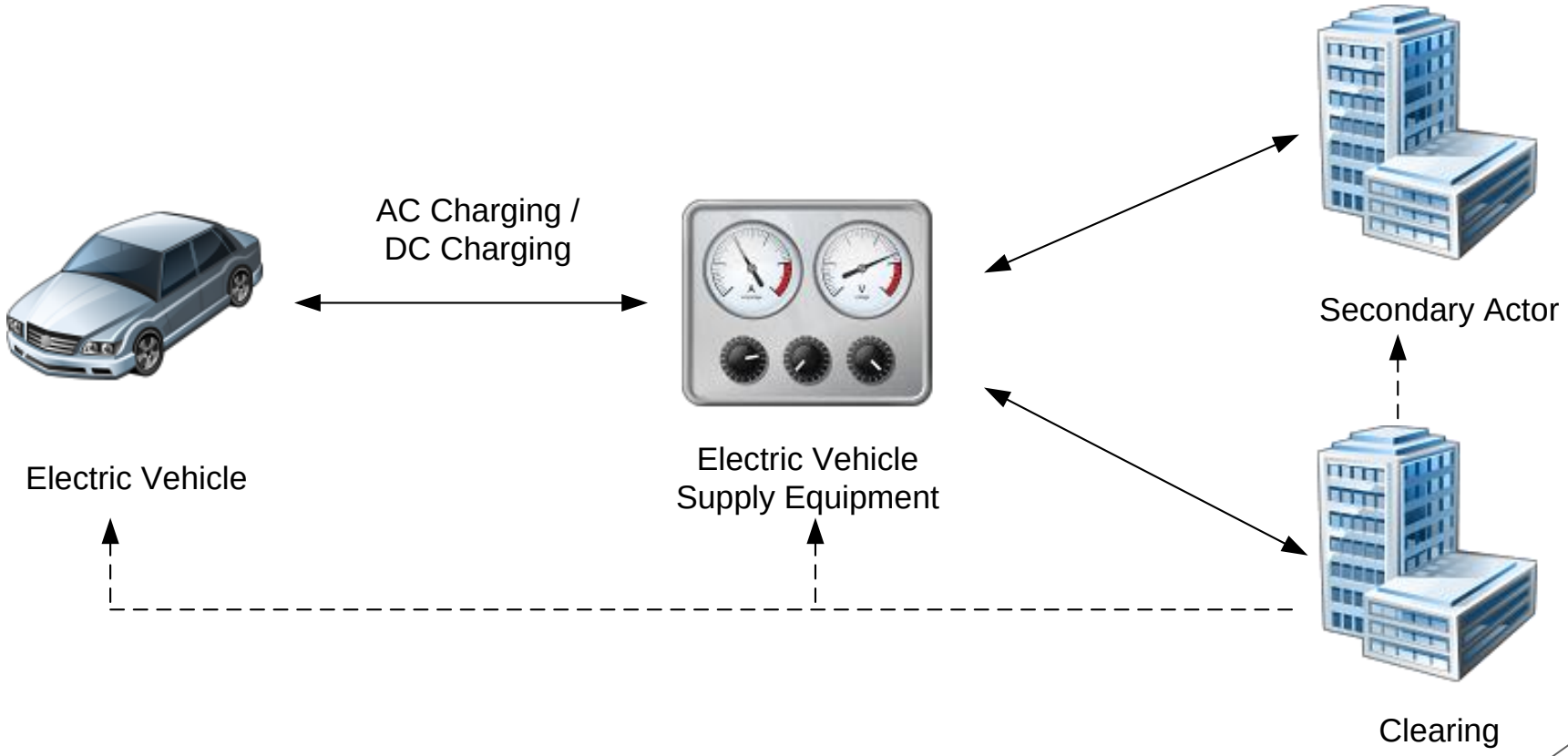
- **Benötigte Kryptographie im Backend**
  - ECC Signing
  - ECC Verfication
  - ECC Key Exchange
  - AES
  - X.509 Certificate Handling → ASN.1, DER
- **Benötigte Protokolle**
  - TLS (Backend - CP)
  - OCSP
  - XML, ISO 15118 Meter Receipts (Sub Set of Charge Protocol)
  - XML, ISO 15118 Key Provisioning
- **Benötigte Infrastruktur**
  - CA / PKI for Mobility Contract Certificate Key Pair Generation
  - Personalisation / Key Distribution for Mobility Contract Certificates
- **Benötigte Prozesse**
  - Key Generation / Distribution
  - CA-Certification / Distribution
  - CA / Mobility Contract Key Revokation
  - Key / Zertifikate Update / Exchange

Was bedeutet ISO 15118 für den Mobility Provider?

Alternative Verfahren zum Key Provisioning für Kundenverträge/Schlüssel betrachtet:

- **Ladeprotokoll ISO 15118: Über Ladesäule**
  - Anfrage Contract über VIN
- **Über Online Dienste im Fahrzeug**
  - OTA / Subscription Management
- **Über Speichermedien / Token**
  - Contactless Card
  - SD Card
  - USB Stick
- **Über Schnittstelle zum Smartphone**
  - Bluetooth
  - WiFi
  - NFC

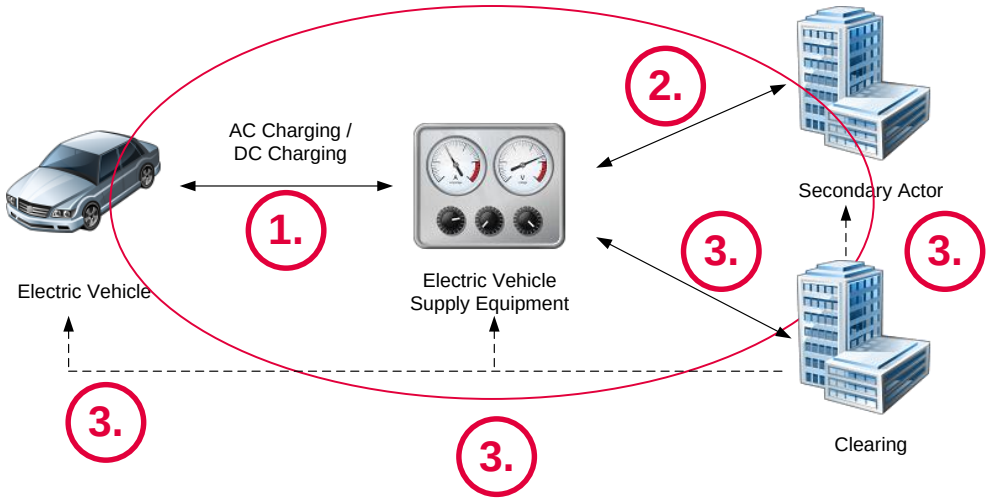
Umfang secunet Referenz-Plattform



Funktionale Abläufe auf Referenz-Plattform

1.Ladeprotokoll gemäß ISO 15118-2

- Initialisierung der Kommunikation und Auswahl des AC Charging Service
- Exemplarische Implementierung des AC-Charging Services (inkl. Austausch verschlüsselter Tarifinformationen und signierter Zählerstände)



2.Backend Kommunikation

- Secondary Actor stellt auf Anfrage verschlüsselte Tariftabellen für ein EV-Modul bereit, EVSE-Modul fungiert als Proxy
- EVSE überträgt signierte Zählerstände des EV an Secondary Actor

3.Kryptografischer Service Provider

- Clearing fungiert als oberste PKI Instanz (Root-CA)
- Clearing bietet Service zur Erstellung und Verteilung von Schlüsselmaterial und Zertifikaten für alle anderen Teilnehmer an
- Clearing bietet Service zur Verifikation signierter Zählerstände an

Module der Referenz-Plattform

Electric Vehicle

Electric Vehicle
Supply Equipment

Clearing /
Secondary Actor

Electric Vehicle Communication Controler (EVCC)

OPT: Presentation Layer

Business Layer

Data Layer | Communica-tion Layer

File-system | EXI/ XML

- Power delivery
- Meter Status
- etc.

Car_I

OnBoard Simulator

ISO 15118-2

Supply Equipment Communication Controler (SECC)

OPT: Presentation Layer

Business Layer

Data Layer | Communica-tion Layer

File-system | EXI/ XML

- Request contract-based Tariff-Table
- Request public Tariff-Table
- Send MeterReceipt

SA_I

- Verifiy MeterReceipt Signature
- Verifiy Contract-Certificate

TH_I

- Export Certificate as PKCS#7
- Export Certificate & Key as PKCS#12

FILE_OUT

Combined Clearing-/SA-Modul

OPT: Presentation Layer | PKI GUI

SA-Modul | Ticket-Handler | Certificate-Handler

Data Layer | Communica-tion Layer

Data-base | XML

ISO International Organization for Standardization

JAR

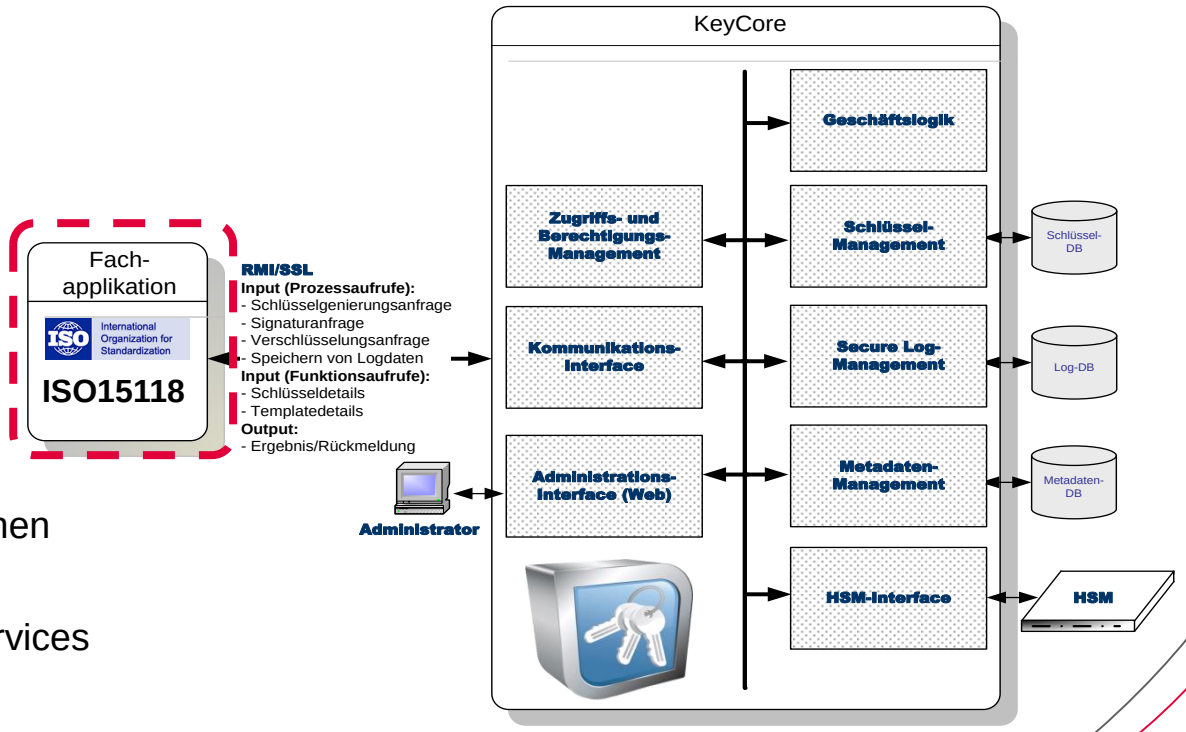
- Generate Certificate
- Verify Signature
- Encrypt Data

secunet ABS

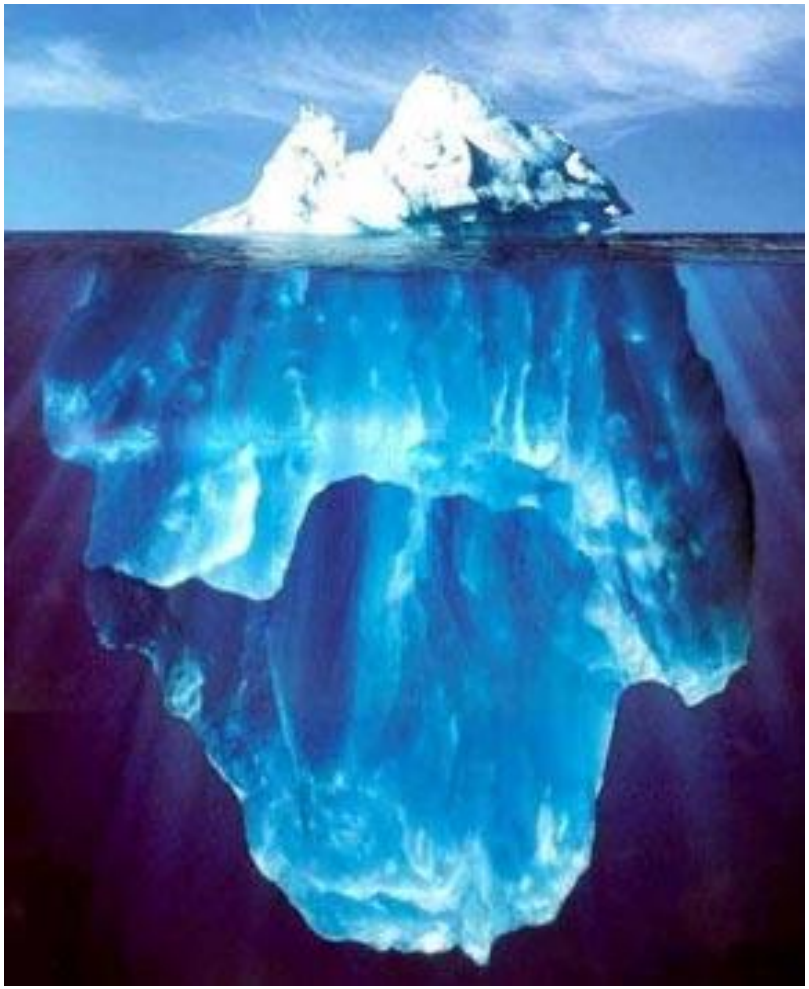
KeyCore

Referenz-Plattform Version 2.0

- **Unterstützung Key Provisioning nach ISO 15118**
  - Rollout von Contract Keys über OEM Schlüssel im Fahrzeug
  - Root- und CA-Key Wechsel über Ladeprotokoll
- **Zentrales Verification Server Modul**
  - Verifikation von signierten Meter Receipts
  - Zertfikats-Überprüfung auch zwischen unterschiedlichen Root CAs
  - SOA Architektur auf Basis Web Services
- **Support für ECC**



Zusammenfassung



- Sicher und überall tanken kann nur mit geeignete Sicherheitsmaßnahmen abgebildet werden
- ISO15118 definiert dafür die notwendigen Sicherheitskonzepte und PKI Strukturen
- Durch die speziellen Clients (Fahrzeuge, Ladeinfrastruktur) entstehen neue Anforderungen.
- D.h. neben den technischen Systemen besteht die Hauptherausforderungen in den abzubildenden Prozessen im Life-Cycle der Zertifikate einer PKI.

PKI ist 20% Technik und 80% Prozess – auch für die ISO 15118 !

secunet - security where IT meets automotive

secunet Security Networks AG
Harry Knechtel

Telefon +49 201 5454-2515
harry.knechtel@secunet.com