TeleTrusT-Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 31.05.2011

Sebastian Kaluza
BMW Group
sebastian.kaluza@bmw.de

eMobility – Sicheres Laden
Standardisierung der Lade-Protokolle
Security in ISO/IEC 15118

Standardisierung Ladekommunikation
Einordnung ISO/IEC 15118

ISO/IEC 15118 spezifiziert die Kommunikation zwischen Fahrzeug und Ladesäule, sowie abstrakte Backend-Interaktion

Standardisierung Ladekommunikation
ISO/IEC 15118 – Überblick Struktur

ISO/IEC 15118

Road vehicles –Vehicle to grid communication interface

Part 1: General information and use-case definition **Security: High-Level Anforderungen**

Part 2: Technical protocol description and open systems interconnections (OSI) requirements **Security: Lösung / Nachrichten**

Part 3: Physical layer and data link layer requirements

Standardisierung Ladekommunikation

Status ISO/IEC 15118

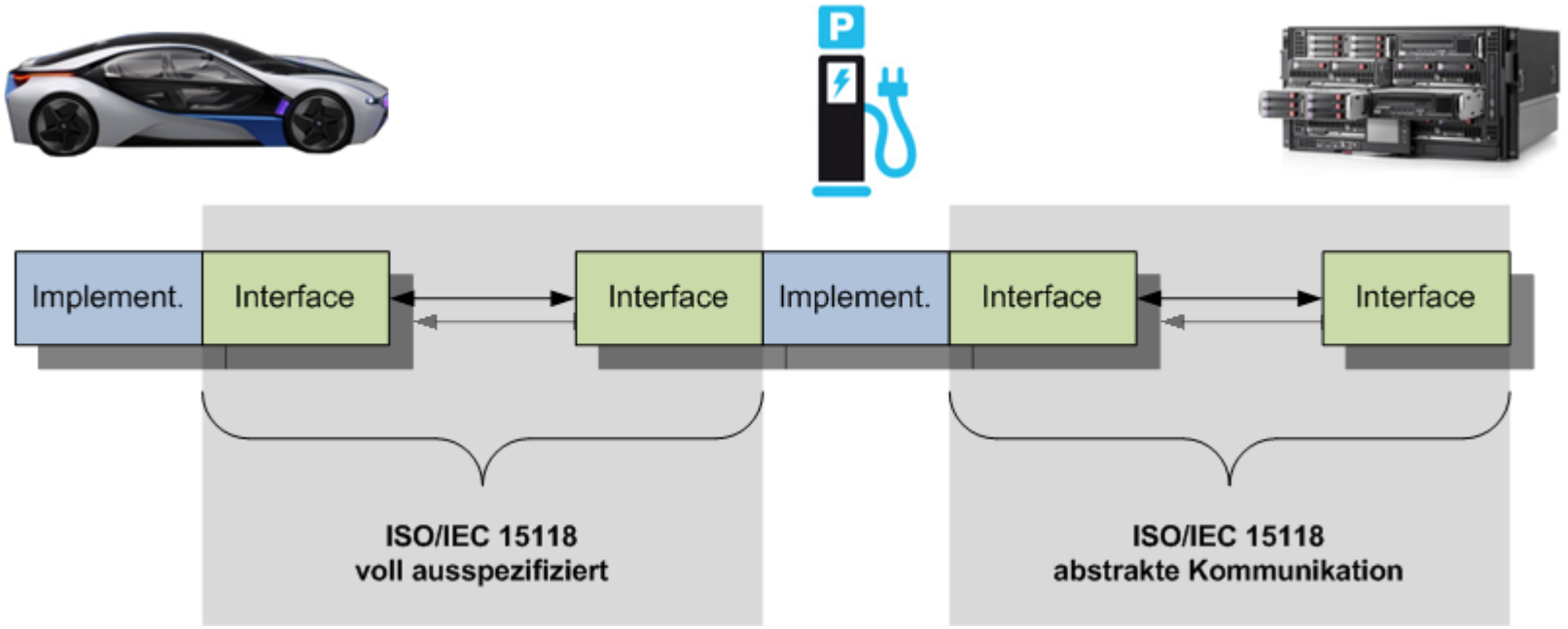
Der künftige Standard ISO/IEC 15118 befindet sich derzeit in der Entwicklung.

Es liegt noch kein “Draft International Standard” vor. Teile liegen intern als “Community Draft” vor.

Die hier skizzierte Security-Architektur basiert auf dem aktuellen Spezifikationsstand bei ISO/IEC.

Änderungen sind jederzeit möglich.

Standardisierung Ladekommunikation
Überblick



Interface zwischen Fahrzeug und Ladesäule über alle Netzwerkschichten definiert.

Kommunikation ins Backend nur abstrakt definiert.

Sicherheitsmechanismen Ladekommunikation

Motivation / Security-Anforderungen

Anforderung:
Automatischer Ladevorgang ohne Interaktion des Fahrers mit der Ladesäule; Säule ist dabei nicht online; Abrechnungsmechanismen werden ermöglicht

Lösungsansatz: → **Applikative Security-Mechanismen**
Vertrags-ID ist im Fahrzeug gespeichert,
Ladesäule authentisiert Vertragsnummer,
Fahrzeug bestätigt Zählerstände (Stromkonsum)

Anforderung:
Schutz des Fahrzeugs gegen Angriffe über Ladeinterface,
Schutz personenbezogener Daten im Fahrzeug

Lösungsansatz: → **Transport Layer Security (TLS/SSL)**
Fahrzeug kommuniziert nur mit authentischer Ladesäule

Sicherheitsmechanismen Ladekommunikation

Schlüsselinfrastruktur, Algorithmen

Public Key Architektur.

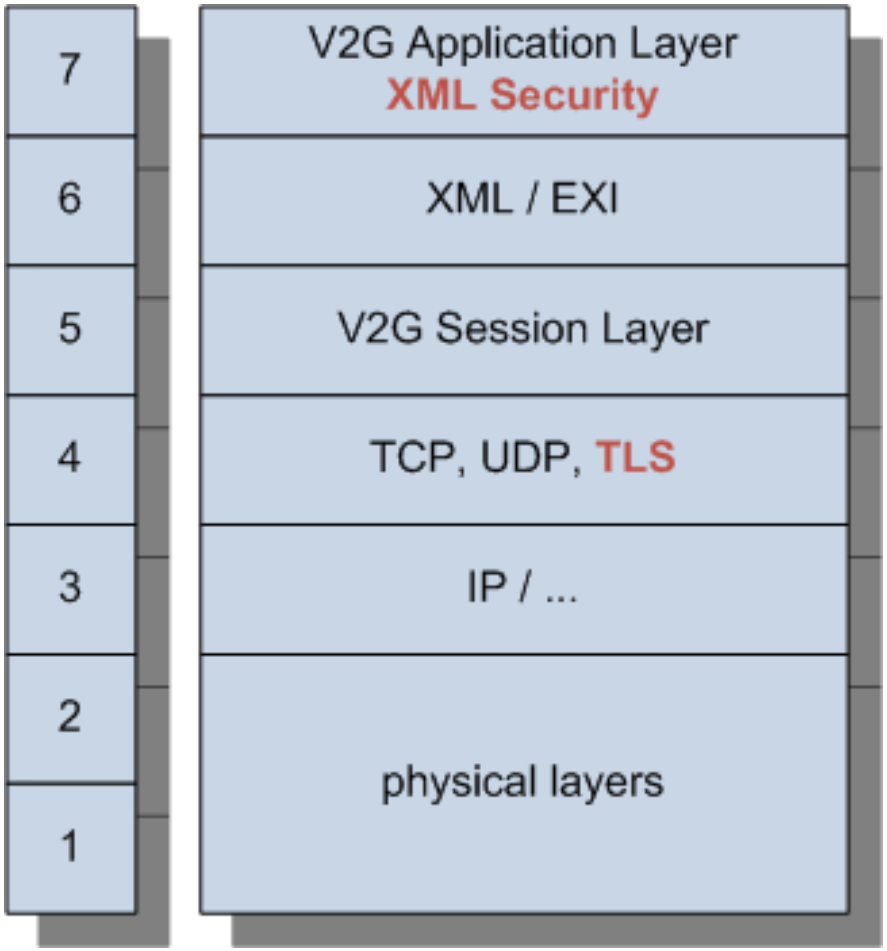
Verwendete Algorithmen:

- asymmetrische Signatur mit elliptischen Kurven
- elliptische Kurven über Primkörper mit 256 bit
- keine optionale Verwendung von RSA

- Hashing mit SHA256
- symmetrische Verschlüsselung mit AES128

Sicherheitsmechanismen Ladekommunikation

Einordnung in ISO/OSI Netzwerk-Layer



Sicherheitsmechanismen auf applikativer Ebene

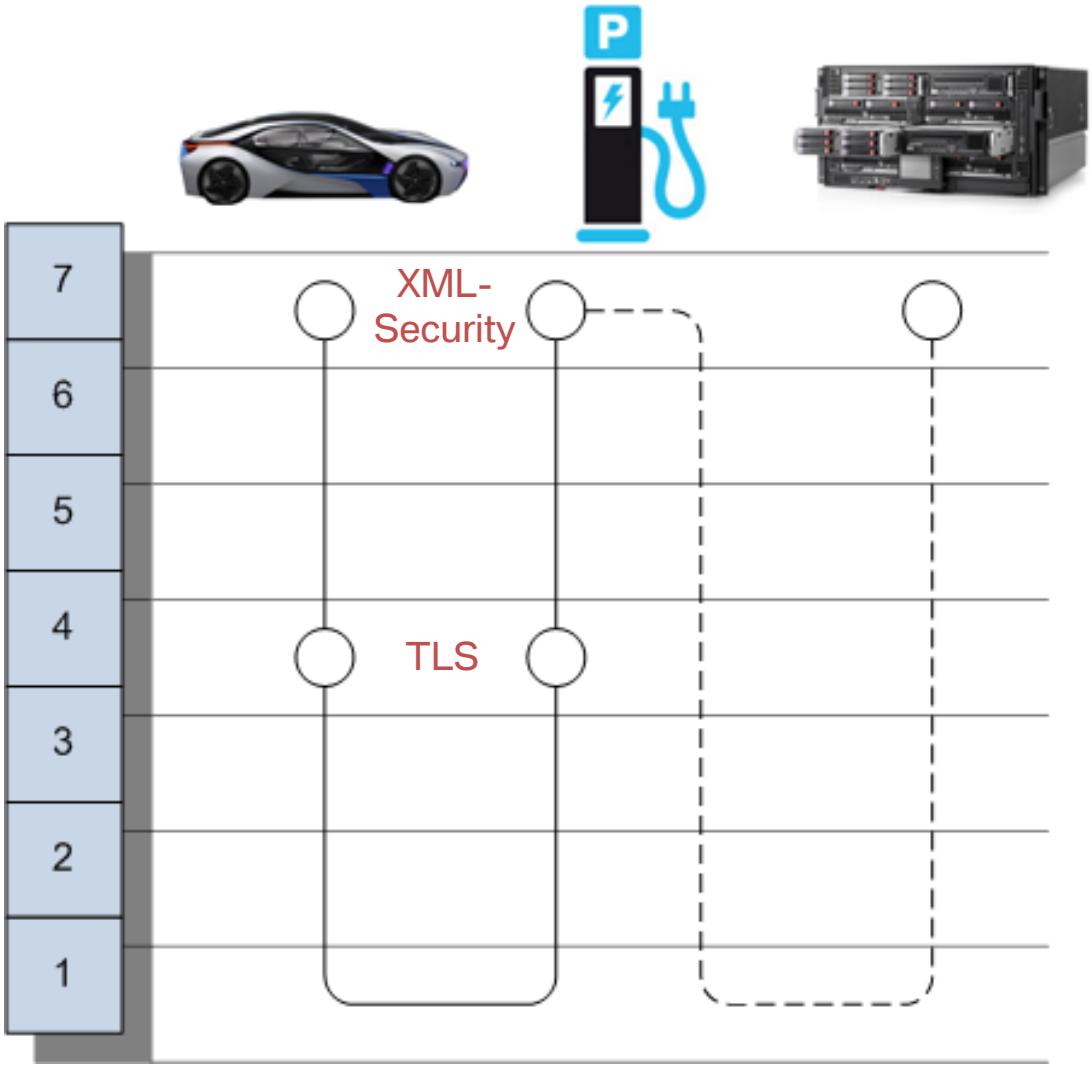
Sicherheitsmechanismen auf Transport-Ebene

Sicherheitsarchitektur unabhängig von der physikalischen Übertragung

Sicherheitsarchitektur ebenfalls unabhängig von Strom-Art (AC/DC) / Stromstärke / Kontaktierung

Sicherheitsmechanismen Ladekommunikation

Backend-Kommunikation



Backend liefert:
- Zertifikate
- Signaturschlüssel
- Revocation-Listen
- Preistabellen

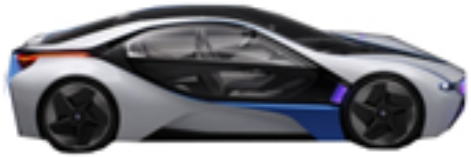
Backend empfängt:
- Zählerstände

ISO/IEC 15118
über alle Layer

Kommunikation mit
Backend abstrakt

Sicherheitsmechanismen Ladekommunikation

Authentisierungen



Applikations-Ebene

Vertragsauthentisierung:
Säule authentisiert den
Vertrag im Fahrzeug

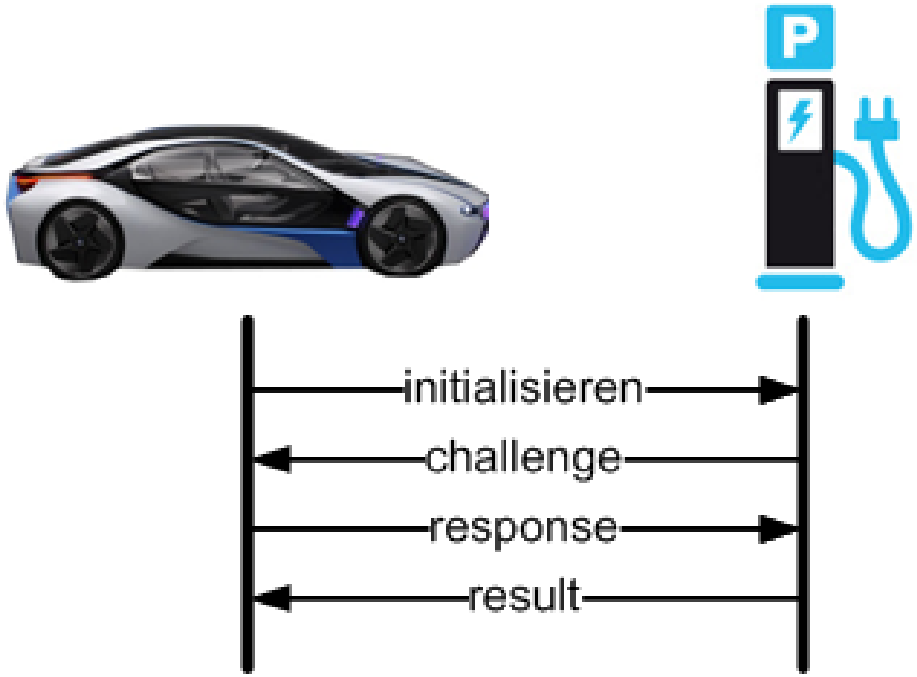
Transport-Ebene

Transport-Schutz: Fahrzeug
authentisiert die Ladesäule

Sicherheitsmechanismen Ladekommunikation

Vertragsauthentisierung

Vertrags-ID ist im Fahrzeug gespeichert;
Ladesäule authentisiert Vertrags-ID beim Laden.



Klassischer Challenge-Response-Machanismus.

Sicherheitsmechanismen Ladekommunikation

Zertifikate installieren und aktualisieren

Herausforderung:

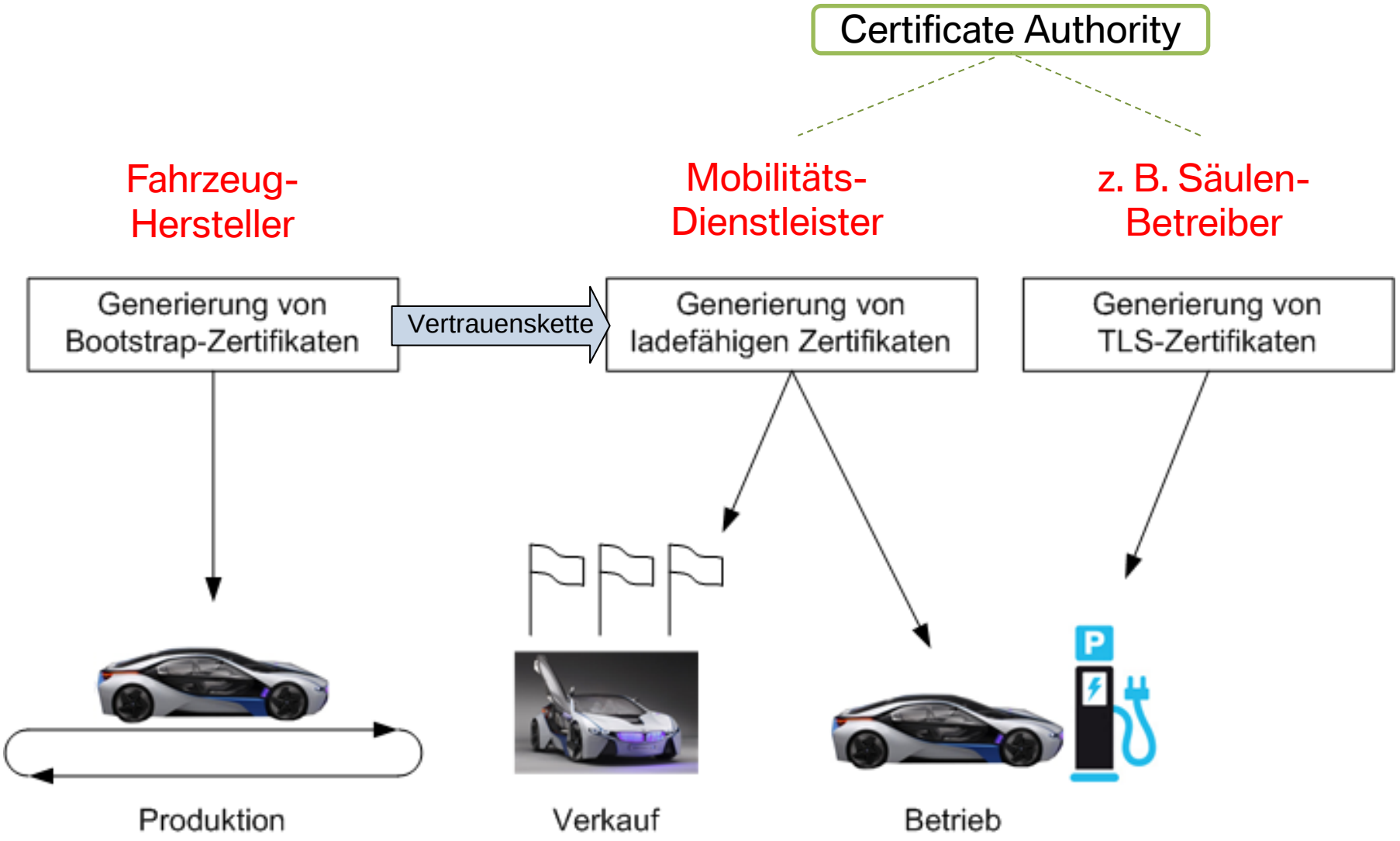
- Fahrzeug benötigt ein Vertrags-Zertifikat und geheime Signatur-Schlüssel
- Bei Fahrzeugproduktion ist noch keine Zuordnung zu einem Kunden möglich.
- Zertifikate müssen im Betrieb aktualisiert werden.

Lösung:

- Mechanismus für Zertifikats-Update ist definiert.
- Der Standard gibt eine Empfehlung für initiales Zertifikats-Bootstrapping

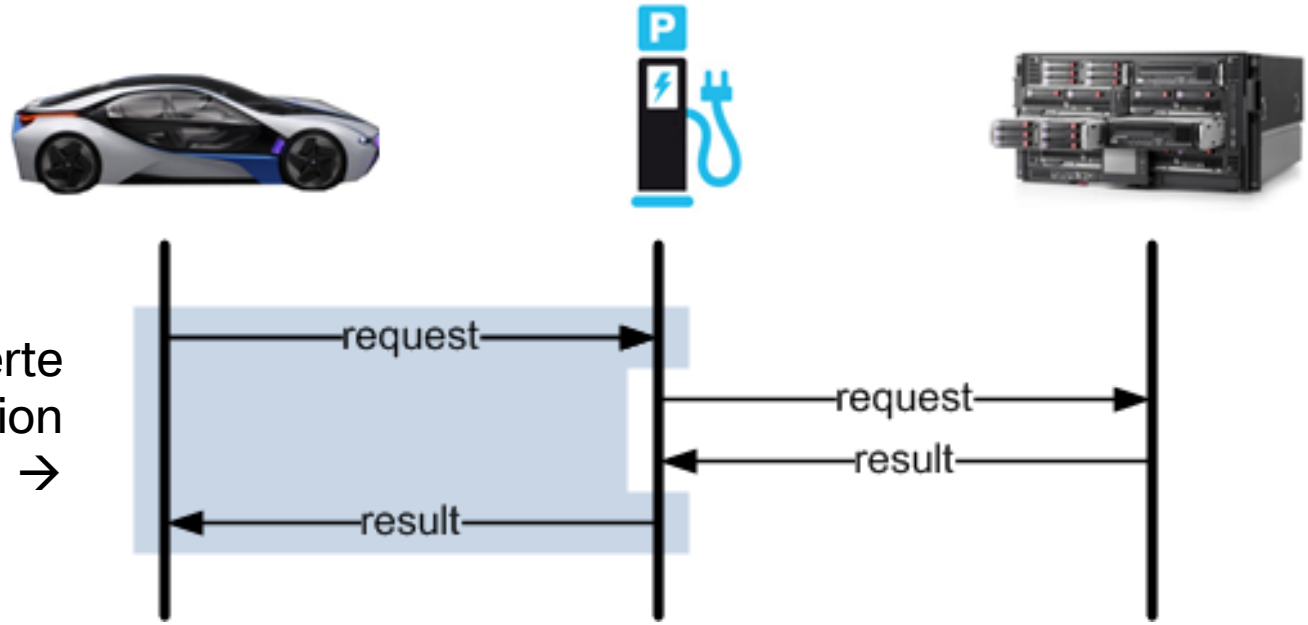
Sicherheitsmechanismen Ladekommunikation

Zertifikate installieren und aktualisieren



Sicherheitsmechanismen Ladekommunikation

Zertifikate installieren und aktualisieren



spezifizierte Kommunikation →

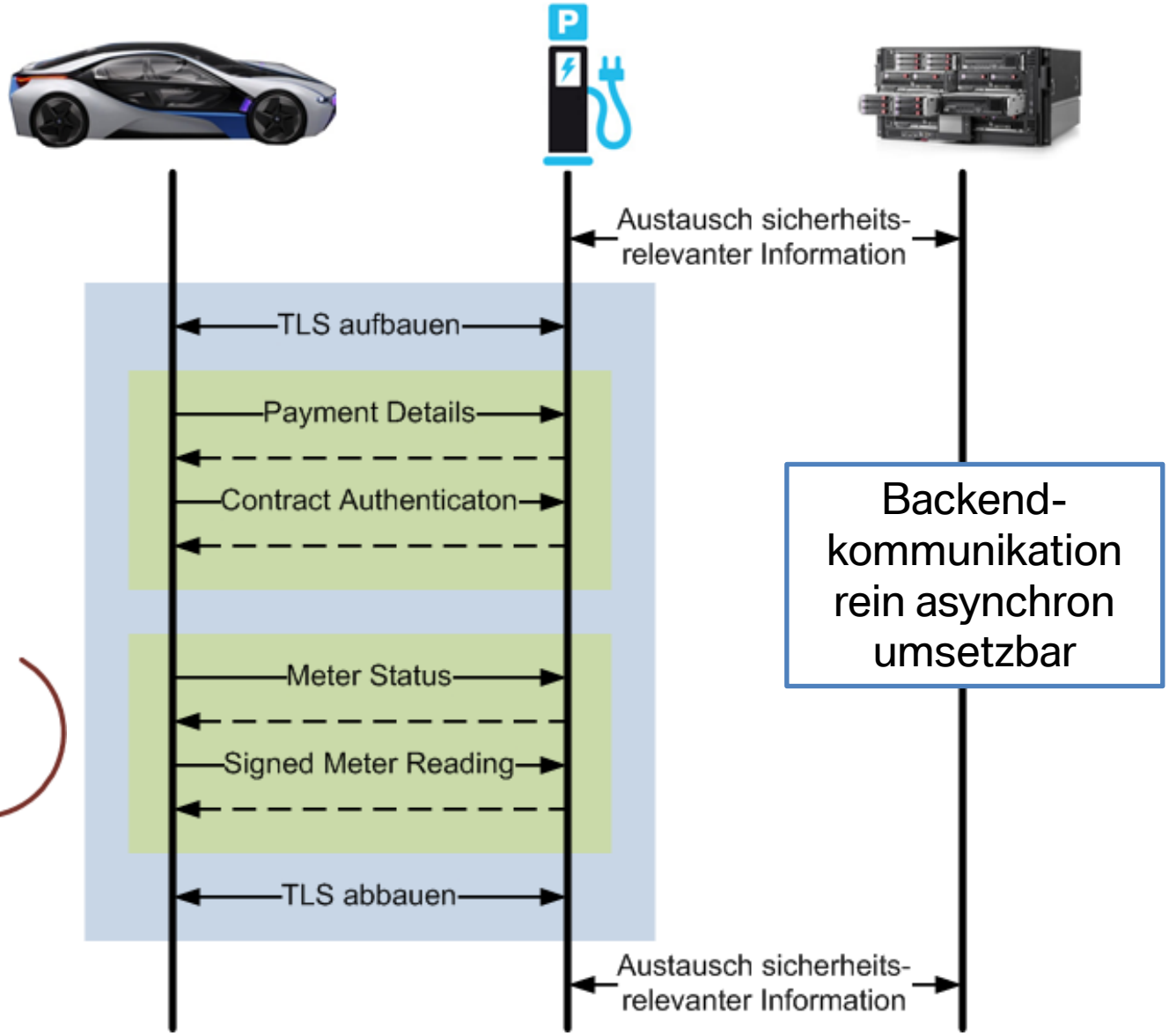
Fahrzeug fragt immer bei der Ladesäule an.

Ladesäule versucht, von einem Backend-System Zertifikate zu bekommen (Säule geht online).

Ladesäule meldet Ergebnis an Fahrzeug zurück.

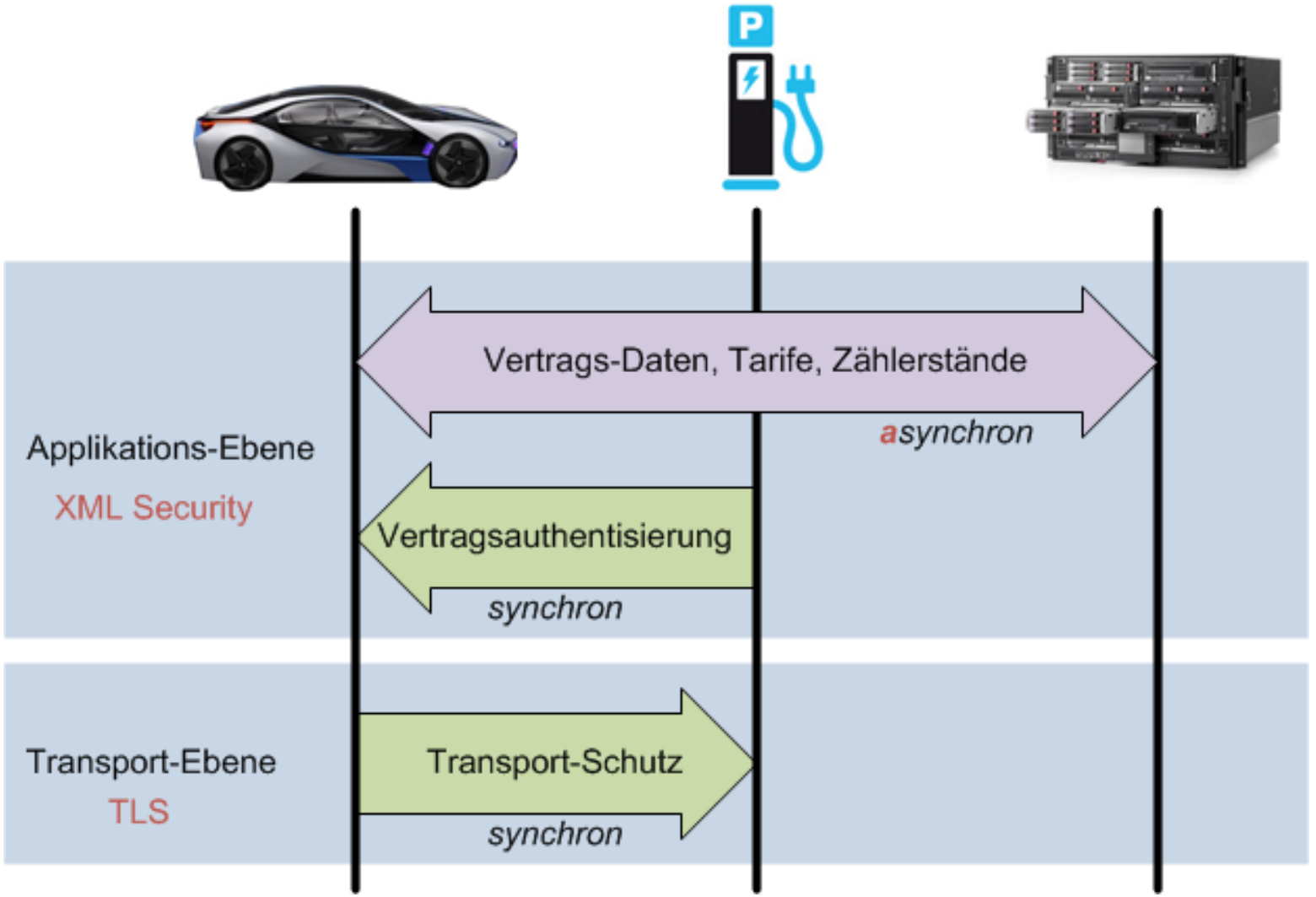
Sicherheitsmechanismen Ladekommunikation

Ablauf und zyklische Zählerstandssignatur



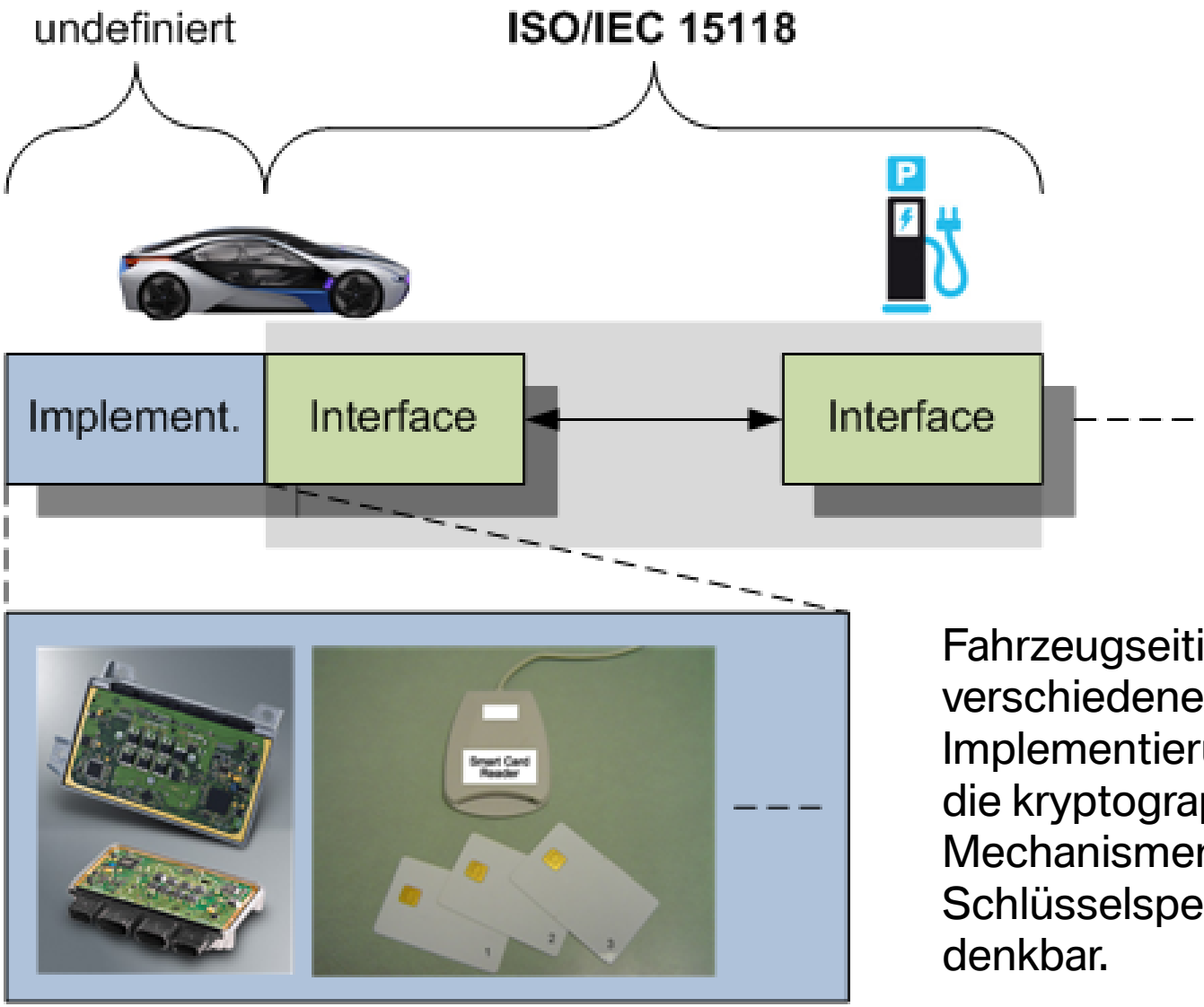
Sicherheitsmechanismen Ladekommunikation

Vertrauensverhältnisse



Sicherheitsmechanismen Ladekommunikation

Implementierungsoptionen



Fahrzeugseitig sind verschiedene Implementierungen für die kryptographischen Mechanismen und Schlüsselspeicher denkbar.

Sicherheitsmechanismen Ladekommunikation

Zusammenfassung

Der Standard ISO/IEC 15118 spezifiziert die Lade-Kommunikation zwischen Fahrzeug und Ladesäule auf allen Layern, sowie abstrakt zu einem Backend.

Die Sicherheitsarchitektur ermöglicht autarke Lade-Vorgänge und schützt das Fahrzeug vor Angriffen.

Das Fahrzeug ist mit einer Vertrags-ID ausgestattet zur automatischen Kundenauthentisierung.

Die Sicherheitsarchitektur in unabhängig von der physikalischen Datenübertragung und der Strom-Art/Übertragungsart (AC/DC / konduktiv/induktiv).

Sicherheitsmechanismen Ladekommunikation

Vielen Dank.