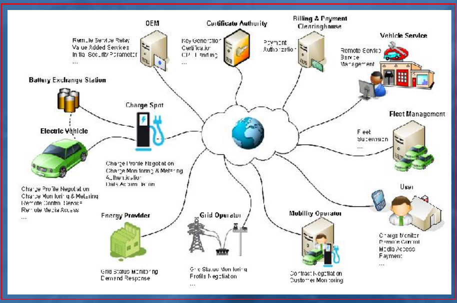
SIEMENS

Corporate Technology

Security Considerations for the Electric Vehicle Charging Infrastructure



Rainer Falk
Siemens AG, CT RTC ITS
☎ : +49 89 636 51653
💻 : rainer.falk@siemens.com

Steffen Fries
Siemens AG, CT RTC ITS
☎ : +49 89 636 53403
💻 : steffen.fries@siemens.com

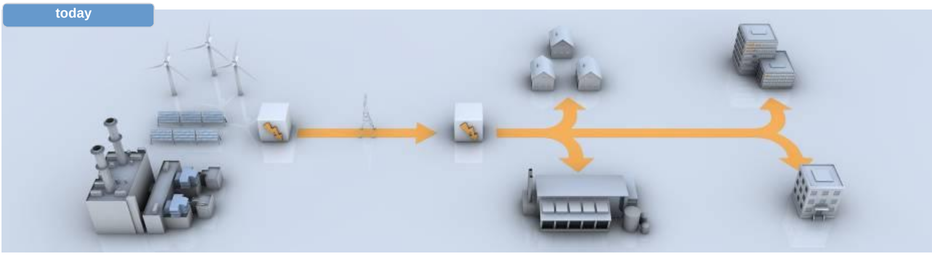
IARIA Conference SECURWARE 2012

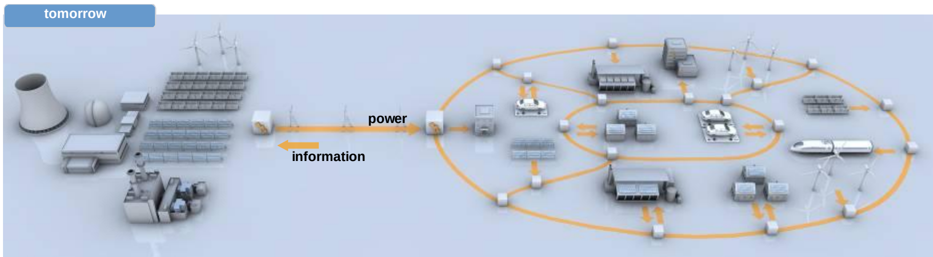
SIEMENS

Outline

- Smart Grid – What is it all about?
- Smart Grid Scenarios
- Incorporation of Electric Vehicles
- Vehicle-to-Grid Interface applying ISO/IEC 15118
  - Potential threats
  - Insights to the current Security Approach
- Summary & Challenges

Conversion of the Conventional Grid to a Smart Grid





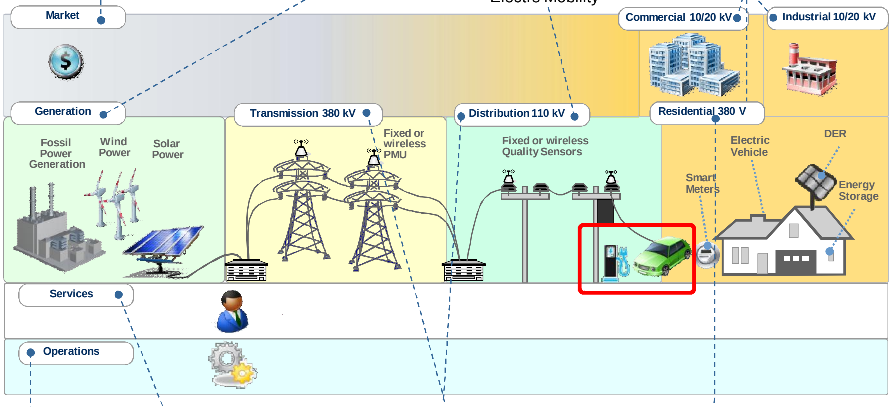
Smart Grid – Incorporation of Decentralized Energy Resources and Flexible Loads requires Security

- Automated billing
- Innovative pricing
- Market place interaction

- Fully integrated energy sources including renewables, biomass, etc.
- Load balancing

- Integration of DER
- Electro Mobility

- Demand response management
- Microgrids

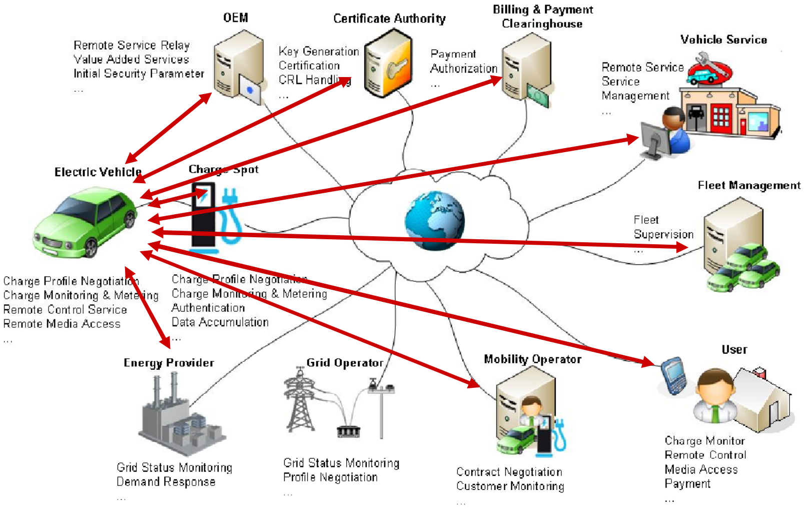


- Remote energy management and control
- Load Monitoring and Balancing

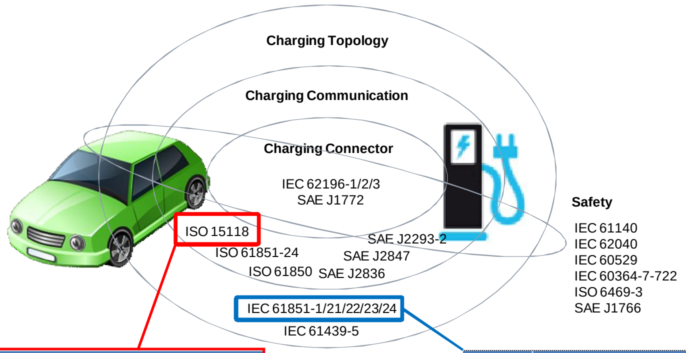
- Real-time outage notification
- Power Quality Monitoring (e.g., through application of PMUs)

- Smart metering
- Smart appliances

Vehicle to Grid Communication Demands



Vehicle to Grid Connection Standards



IEC 15118	Road vehicles – Communication protocol between electric vehicle and grid
1	General information and use-case definition
2	Technical protocol description and Open Systems Interconnections (OSI) layer requirements
3	Physical layer and Data Link layer requirements

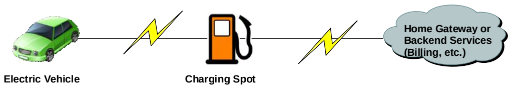
IEC 61851	Electric vehicle conductive charging system
1	General requirements
21	Electric vehicle requirements for conductive connection to an A.C./D.C. supply
22	A.C. electric vehicle charging station
23	D.C electric vehicle charging station
24	Control communication protocol between off-board D.C. charger and electric vehicle

Typical Data Exchanged over the Vehicle-to-Grid Interface and their Security Impact

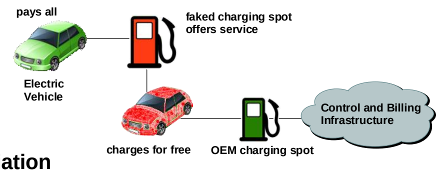
Information asset	Description, potential content	Security relation
Customer ID and location data	Customer name, vehicle identification number, charging location, and charging schedule	Effects customer privacy
Meter Data	Meter readings that allow calculation of the quantity of electricity consumed or supplied over a time period These are generated by the charge spot and may be validated by the vehicle.	Effects system control and billing
Control Commands	Actions requested by one component of other components via control commands. These commands may also include Inquiries, Alarms, Events, and Notifications.	Effects system stability and reliability and also safety
Configuration Data	Configuration data (system operational settings and security credentials but also thresholds for alarms, task schedules, policies, grouping information, etc.) influence the behavior of a component and may need to be updated remotely.	Effects system stability and reliability and also safety
Time, Clock Setting	Time is used in records sent to other entities. Phasor measurement directly relates to system control actions. Moreover, time is also needed to use tariff information optimally. It may also be used in certain security protocols.	Effects system control (stability and reliability and also safety) and billing
Access Control Policies	Components need to determine whether a communication partner is entitled to send and receive commands and data. Such policies may consist of lists of permitted communication partners, their credentials, and their roles.	Effects system control and influences system stability, reliability, and also safety
Firmware, Software, and Drivers	Software packages installed in components may be updated remotely. Updates may be provided by the utility (e.g., for charge spot firmware), the car manufacturer, or another OEM. Their correctness is critical for the functioning of these components.	Effects system stability and reliability and also safety
Tariff Data	Utilities or other energy providers may inform consumers of new or temporary tariffs as a basis for purchase decisions.	Effects customer privacy and also competition

Example Threats to a Charging Infrastructure targeting the Vehicle-to-Grid Interface

1. **Eavesdropping or Interception**



2. **Man-in-the-Middle Attack**

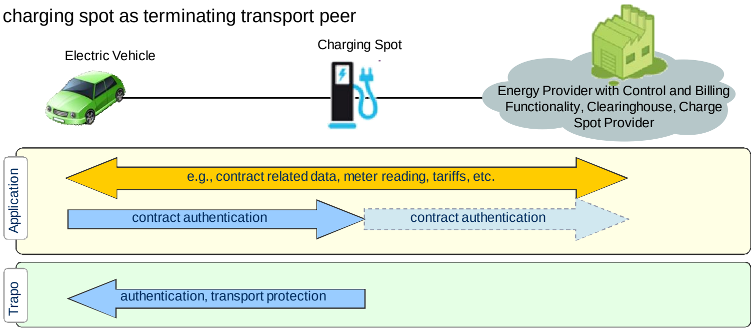

pays all
Electric Vehicle
faked charging spot offers service
charges for free
OEM charging spot
Control and Billing Infrastructure

3. **Transaction Falsifying or Repudiation**
4. **Attack network from within vehicle**
5. **Tampered or substituted component (in EV or EVSE)**
6. **….**

IEC 15118 –
Securely Connecting the Vehicle to the Smart Grid

SIEMENS

- **Standard for the interface between vehicle and charging station supporting**
  - Connection of vehicles to the power grid
  - Billing of consumed energy (charging)
  - Roaming of electric vehicles between different charging spot
  - Value added services (e.g., software updates)
- **Trust Relations from the electric vehicle to**
  - backend (Energy Provider) for signed meter readings and encrypted information (e.g., tariff)
  - charging spot as terminating transport peer


Electric Vehicle
Charging Spot
Energy Provider with Control and Billing Functionality, Clearinghouse, Charge Spot Provider
Application
e.g., contract related data, meter reading, tariffs, etc.
contract authentication
contract authentication
Trapo
authentication, transport protection

IEC 15118 – Approach based on Certificates and corresponding Private Keys (PKI)

SIEMENS

Connectivity Requirements

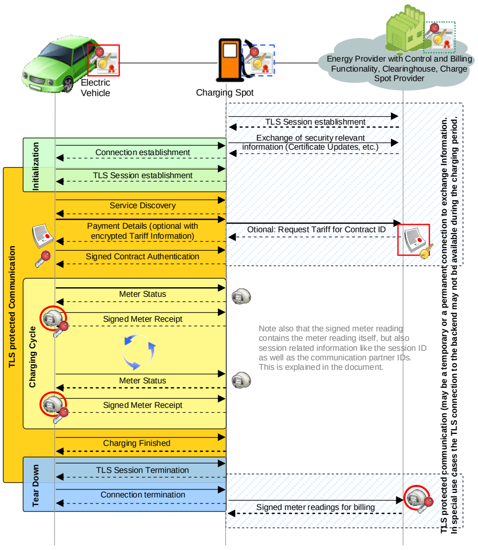
- EVSE has (Semi-)Online connection to the backend
- Persistent connection between EV and EVSE during charging to exchange charging process relevant information, (cyclic exchange of metering reading)

Approach

- Unilateral authenticated TLS to protect communication between EV and EVSE
- XML security for securing data exchange with the backend

Credentials

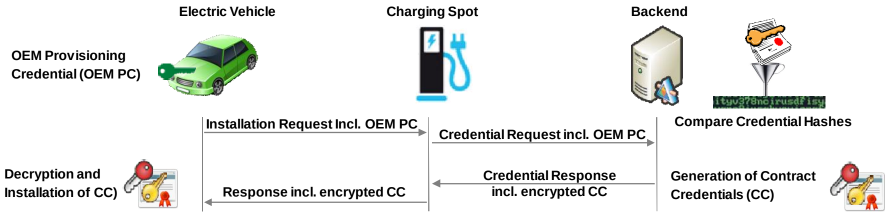
- Public/private key pair incl. certificate


Electric Vehicle
Charging Spot
Energy Provider with Control and Billing Functionality, Clearinghouse, Charge Spot Provider
TLS Session establishment
Exchange of security relevant information (Certificate Updates, etc.)
Initialization
Connection establishment
TLS Session establishment
Service Discovery
Payment Details (optional with encrypted Tariff Information)
Otional: Request Tariff for Contract ID
Signed Contract Authentication
TLS protected Communication
Charging Cycle
Meter Status
Signed Meter Receipt
Meter Status
Signed Meter Receipt
Charging Finished
Tear Down
TLS Session Termination
Connection termination
Signed meter readings for billing
TLS protected communication (may be a temporary or a permanent connection to exchange Information. In special use cases the TLS connection to the backend may not be available during the charging period.

Note also that the signed meter reading contains the meter reading itself, but also session related information like the session ID as well as the communication partner IDs. This is explained in the document.

IEC 15118 – Consideration of Contract Credential Bootstrapping

- **Credential installation or update of existing credentials in EV considered (for Plug&Charge)**
- **Allows for bootstrapping options like**
  - OEM Provisioning Certificate (PC) and corresponding private key provided during production time
  - Owner of EV receives derived information of the credential (e.g., a hash of the credential)
  - When applying for contract based credential (CC) the hash is provided by the owner out-of-band and checked by the mobility operator against hash received during communication.



Electric Vehicle

Charging Spot

Backend

OEM Provisioning Credential (OEM PC)

Installation Request Incl. OEM PC

Credential Request incl. OEM PC

Compare Credential Hashes

Decryption and Installation of CC)

Response incl. encrypted CC

Credential Response incl. encrypted CC

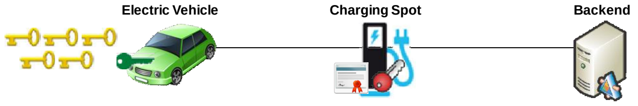
Generation of Contract Credentials (CC)

IEC 15118 – Some details of the PKI based approach

- **Cryptographic algorithm support**
  - Public Key: ECDSA 256
  - Hash: SHA-256 minimum
  - Symmetric Encryption: AES128
- **Security protocol and method support**
  - TLS supports ECDSA within different cipher suites (RFC 5289)
  - XML Security (Digital Signature and Encryption with ECC according to W3C candidate specs)
- **Security credential management**
  - EV supports 5 root certificates, no CRL handling (memory and performance limits)
  - Revocation of EVSE certificates not in scope, maximum lifetime 4 weeks
  - EVSE Issuing CA uses OCSP responses for own certificates
  - CRLs only for contract based certificates (checked at EVSE)

IEC 15118 –
Credential Handling during Operation

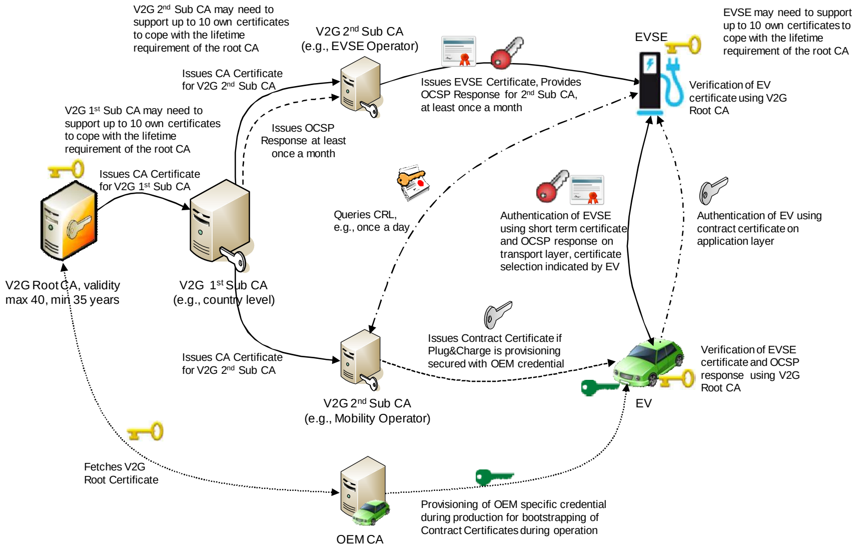
SIEMENS



- EV supports 5 Root Certificates each with 40 years validity (lifetime)
- Root CA certificate for EVSE certificate issuing shall have 35 years remaining validity
- 3 hierarchy levels of certificates allowed
- EV signals the supported Root CA(s) to enable EVSE to pick the right certificate for authentication during TLS handshake
- EVSE needs to possess 10 different own certificates to cope with potential EV requests (worst case)
- EV does not support CRLs, short term certificates and OCSP responses used → Regular updates!
    - 10 EVSE specific certificates
    - 1 OCSP response for the issuing CA
- Higher effort in credential handling on EVSE side → optimization requested, e.g., one public/private key pair and 10 certificates for the same public key to minimize storage requirements on EVSE

IEC 15118 –
Credential Handling during Operation (Example)

SIEMENS



V2G 2nd Sub CA may need to support up to 10 own certificates to cope with the lifetime requirement of the root CA

Issues CA Certificate for V2G 2nd Sub CA

V2G 1st Sub CA may need to support up to 10 own certificates to cope with the lifetime requirement of the root CA

Issues CA Certificate for V2G 1st Sub CA

Issues OCSP Response at least once a month

Issues EVSE Certificate, Provides OCSP Response for 2nd Sub CA, at least once a month

EVSE may need to support up to 10 own certificates to cope with the lifetime requirement of the root CA

Verification of EV certificate using V2G Root CA

Queries CRL, e.g., once a day

Authentication of EVSE using short term certificate and OCSP response on transport layer, certificate selection indicated by EV

Authentication of EV using contract certificate on application layer

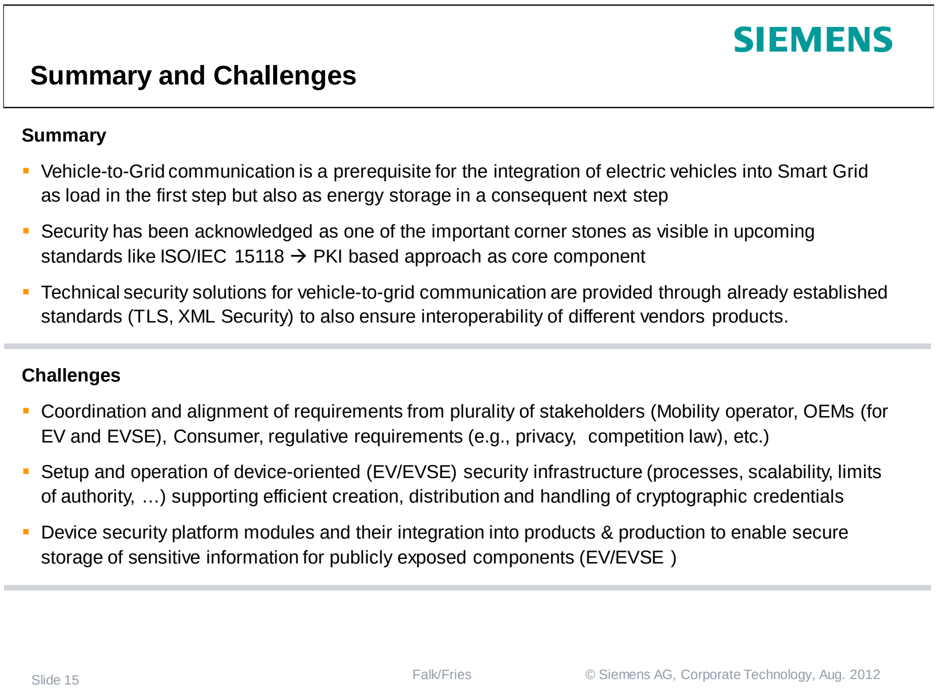
Issues CA Certificate for V2G 2nd Sub CA

Issues Contract Certificate if Plug&Charge is provisioning secured with OEM credential

Verification of EVSE certificate and OCSP response using V2G Root CA

Fetches V2G Root Certificate

Provisioning of OEM specific credential during production for bootstrapping of Contract Certificates during operation



Summary and Challenges

Summary

- Vehicle-to-Grid communication is a prerequisite for the integration of electric vehicles into Smart Grid as load in the first step but also as energy storage in a consequent next step
- Security has been acknowledged as one of the important corner stones as visible in upcoming standards like ISO/IEC 15118 → PKI based approach as core component
- Technical security solutions for vehicle-to-grid communication are provided through already established standards (TLS, XML Security) to also ensure interoperability of different vendors products.

Challenges

- Coordination and alignment of requirements from plurality of stakeholders (Mobility operator, OEMs (for EV and EVSE), Consumer, regulative requirements (e.g., privacy, competition law), etc.)
- Setup and operation of device-oriented (EV/EVSE) security infrastructure (processes, scalability, limits of authority, …) supporting efficient creation, distribution and handling of cryptographic credentials
- Device security platform modules and their integration into products & production to enable secure storage of sensitive information for publicly exposed components (EV/EVSE)

Slide 15

Falk/Fries