Securely connecting Electric Vehicles to the Smart Grid

Rainer Falk and Steffen Fries
Corporate Technology
Siemens AG
Munich, Germany
e-mail: [rainer.falk | steffen.fries]@siemens.com

***Abstract*—Rechargeable electric vehicles are receiving increasing attention from different stakeholders: from customers as gas prices are constantly rising, from car manufacturers to address customer, market, and environmental demands, and also from electric energy utilities for integrating them into smart electric grids. While in the first step, the emphasis is placed on electric vehicles as energy consumers, using their battery for storing energy and feeding it back to the energy network will be the consequent next step. Batteries of electric vehicles will realize a distributed energy electric storage for stabilizing the electric power grid. Thus the electric vehicle will participate as a mobile energy node within the smart grid having two types of interfaces, one for electricity and one for data communication for charging and feedback control, information exchange, and for billing. Since IT security in the smart grid is already considered as a major point to be addressed, the enhancement of the smart grid with electric mobility has to address IT security as well. This article describes example interactions of electric vehicles with the charging infrastructure and it shows which security requirements have to be fulfilled in important use cases. Moreover, security considerations of current standardization activities in ISO/IEC and SAE are described.**

Keywords*—*eMobility security; Smart Grid security; charging infrastructure; IEC 61851; IEC 15118

I. INTRODUCTION

The Smart Grid can be roughly characterized as a combination of two infrastructures, the electrical grid carrying the energy, and the information infrastructure used to supervise and control the electrical grid operation. The importance of information security for the power systems communication infrastructure has increased tremendously over the last couple of years. Until recently, automation has mainly targeted the transmission network to address the multilateral exchange of energy from different providers. With the advent of decentralized energy resources like wind parks and solar cells and their interaction with the electric grid there is a higher demand for automation in the distribution network. These energy resources show a high fluctuation depending on the environmental conditions and also go along with the possibility to influence energy demand. This will require supporting demand response services. The introduction of electric vehicles as flexible load, and in the future potentially as decentralized energy resource (power feedback), emphasizes this development (see also [1]).

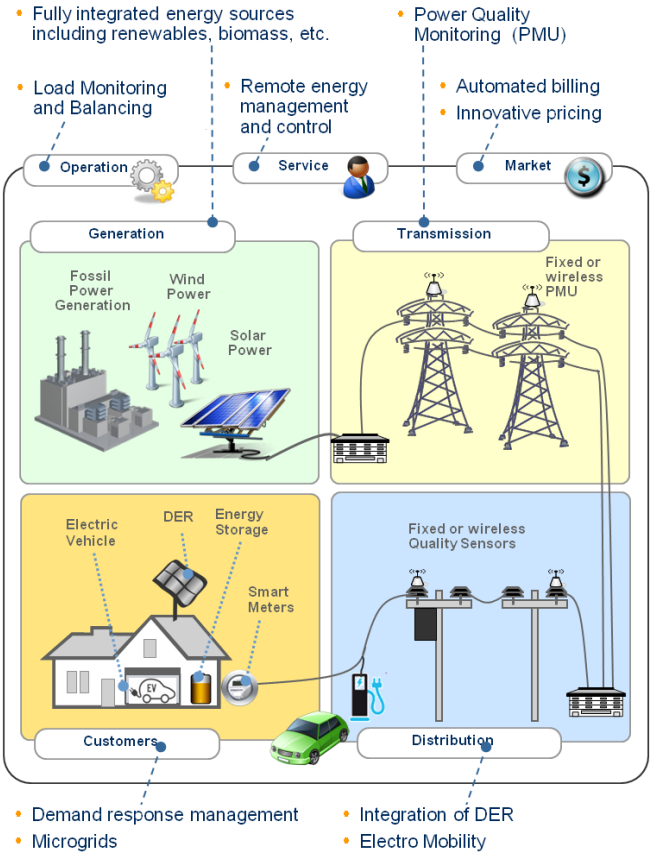

Figure 1. Potential Smart Grid Scenarios.

Figure 1 shows a high level view on typical smart grid scenarios, also targeting the integration of electric vehicles. The four center domains shown are the typical domains, used to describe a smart grid:

- **(Bulk) Energy Generation** is the process of converting non-electrical energy into electricity, and is the first step in the process of delivering power to consumers. Besides classical energy generation like coal- or gas-fired power plants or nuclear power plants, decentralized energy generation using photovoltaic, block heat and power plants, or windmills are getting more and more integrated into the power grid for bulk energy generation.
- **Power Transmission** is the bulk transfer of electric power to substations. A power transmission network connects power plants generating electrical energy with

substations and typically works on high voltage level (e.g., 380 kV).

- **Energy Distribution**: Substations distribute the electrical energy further down to industrial, commercial, or residential consumers in the range of medium voltage (typically covers the range between 20kV to 100kV). Substations provide the transition to the low voltage area (typically around 400V). The energy distribution level is likely to provide connection points for vehicle charging, especially, when high power AC or DC charging spots are used.
- **Customer**: The customer role as consumers of electric energy was typically the endpoint for the energy transfer. Within the Smart Grid, this role may change due to the option to move from pure consumption of energy to producing and storing energy in residential areas. Then the customer would become a so-called prosumer. As visible in Figure 1, electric vehicles may connect to the customer or the distribution domain.

There exists further Smart Grid domains like operation and service of the four domains stated above as well as the market, which enables the interaction between energy generators an energy consumers. The number of electric vehicles as bicycles, motorcycles, and cars is expected to increase significantly. Electric vehicles will be connected with the Smart Grid for charging or even for power feedback. Typically, they connect to the Smart Grid through charging stations or charging points. Charging points in public or corporate places provide the possibility for high power AC or DC charging. Other connection points may be provided by combined service stations, e.g., for parking lots or common home power plugs in residential areas. Closely linked with the pure flow of energy is the management and control of the energy demand for charging electric vehicles. It allows matching the energy demand for the charging process with the energy available at the specific location within the energy grid. A defined part of the vehicle battery's capacity can also be used as energy storage to stabilize the energy grid when needed by feeding back energy from the vehicle to the electrical grid. Besides the control of energy flow there may be a second communication channel for the billing for consumed or provided energy.

The charging infrastructure as a part of the critical infrastructure Smart Grid requires integrated protection against unintentional and intentional attacks. Safety and IT security measures, which are already being part of the Smart Grid core (e.g., defined as standard or realized in proprietary deployments), need to be enhanced to cover also the Smart Grid access infrastructure. This Smart Grid access infrastructure is provided for electric vehicles through the charging infrastructure. While current deployments do not feature an information exchange between the electric vehicle and the charging infrastructure beside a minimum local control of the charging process through pilot signals, upcoming standards and proposed scenarios provide feature rich communication options. The Smart Grid communication and control network of an energy utility is increasingly opened to various nodes not being under control of any energy network operator and thereby exposed to attacks.

Highly dependable management and operations of the information infrastructure are prerequisites for a highly reliable energy network as the power system increasingly relies on the availability of the information infrastructure. Therefore, the information infrastructure must be operated according to the same level of reliability as required for the stability of the power system infrastructure to prevent any type of outage. Especially consumers and utility companies can both benefit from managing this intelligently, and standards anticipating the new environment are emerging from many directions (see [2]). The immediately apparent security needs target the prevention of financial fraud and ensure the reliable operation of the power grid. Both are complex objectives. But surely all of the security ramifications of the charging infrastructure have not been discovered yet. Especially the interaction between new market participants and value added services is currently under investigation. In any case, ensuring privacy, safety, and assuring that the charging service is operating correctly are basic objectives to derive related IT security requirements. Hence, integrated information security is a central part of the charging infrastructure.

The remainder of this paper is structured as follows: Section II describes use cases around the electric vehicle charging infrastructure. Section III discusses information assets derived from the use cases, threats to these assets and also defines first security requirements. Section IV gives an overview about the security standardization for the vehicle to grid interface, while Section V concludes the document.

II. USE CASES

The electrical vehicle charging infrastructure consists of a combination of power services for electric vehicles and value-added services based on the information and communication infrastructure as illustrated in Figure 2.

One main goal of this information and communication infrastructure is to offer customers a choice of service options beneficial to all three, the utility company, the mobility operator as power (service) provider, and the customer. The utility can operate most efficiently when energy demand is fairly constant over time. Price incentives can be offered towards those customers having a flexible vehicle charging schedule with the objective to smooth out energy demand variations. This requires the analysis and consideration of several variables, e.g., schedule, equipment, location, payment options, and additional services.

The variety of peers in a charging infrastructure as depicted in Figure 2 shows the complexity, but also the manifold of possibilities for optimized service offerings.

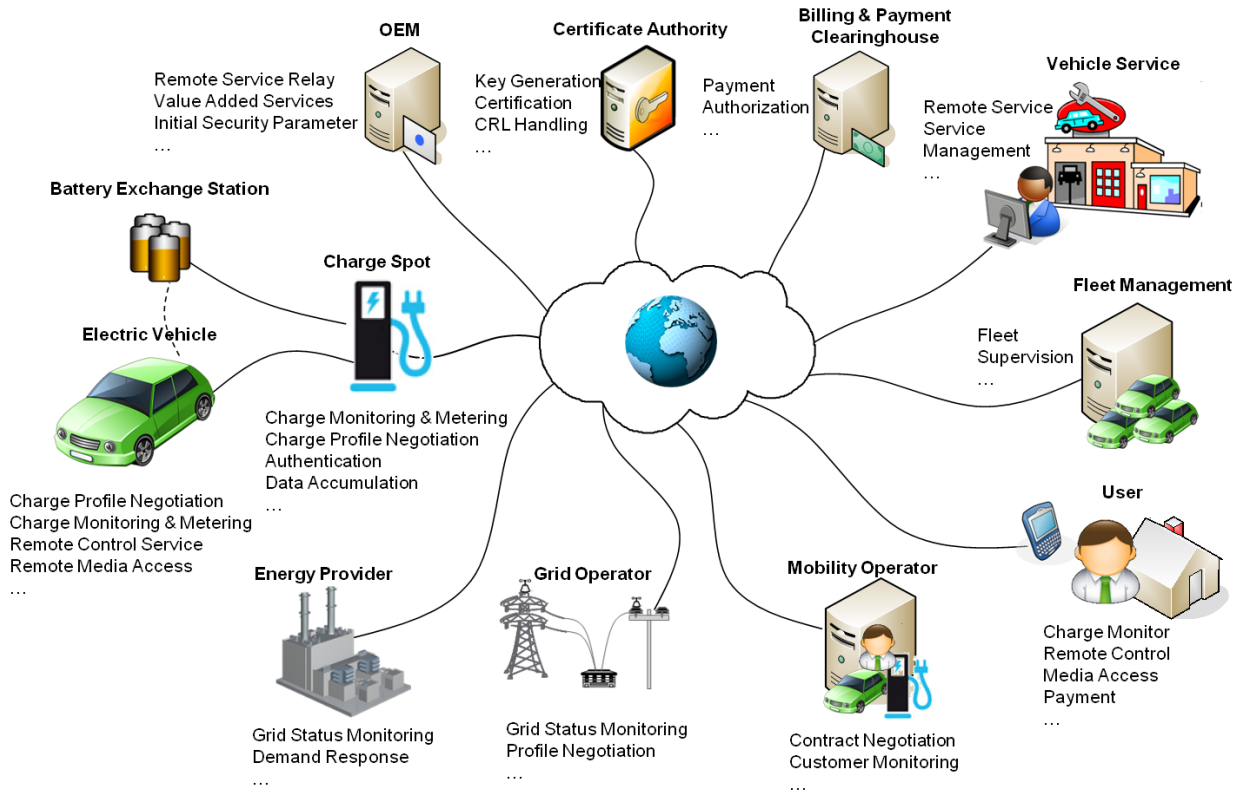

Figure 2. Communication among Actors of an Electric Vehicle Charging Infrastructure.

While not shown in Figure 2, there are different protocol frameworks being used for the communication between the different participants in the scenario.

The following list provides a short overview of potential protocol candidates:

- ISO/IEC 15118 – Communication between electric vehicle and charging spot (cf. [6], [7], and [8])
- IEC 61850 – Communication between charging spot and energy provider (cf. [11])
- OCPP (Open Charge Point Protocol) for the communication between charging spot and mobility operator. Note, as OCPP is not yet a standardized protocol per se, work is currently ongoing to define an infrastrucutre related protocol. It is likely, that this will enhance the exisiting IEC 61850 protocol series.
- OCSP (Online Certificate Status Protocol) between charging spot (or mobility operator) and certification authority.

Further protocols exist, which are not stated here, allowing user interaction with the electric vehicle or the charging infrastructure as well as protocols for the provisioning of value added services. Value added services may be for instance the firmware update of the infotainment system during charging.

The following subsections provide an overview on potential use cases surrounding the charging infrastructure. Each subsection provides potential realization options for the considered use case. Note that the use case discussion stems mainly from standardization work currently done in ISO (International Standardization Organization), IEC (International Electrotechnical Comission), and SAE (Society of Automotive Engineers). but the use cases show the potential of a Smart Grid charging infrastructure to be a flexible platform to realize a variety of known and upcoming service offerings.

A. Control of the Electric Vehicle Charging Environment

Connecting electric vehicles with the charging infrastructure provides flexible control of the charging process through enhanced communication between electric vehicle, charging spot, and the energy provider in the backend, e.g., to adapt the charging to the current energy provisioning situation. It also covers scenarios with limited control of the charging operation through the charging spot or backend. Charging in these scenarios may be controlled completely by the electric vehicle to the limits set by the environment. This is typically the case for AC (alternating current) charging, while in DC (direct current) charging control is being performed by the charging spot.

B. Connecting to the Charging Infrastructure

Connecting a vehicle to the charging infrastructure may use a portable cord set to be provided by either the electric vehicle owner or the charge spot operator. This cord set and the connectors may be different depending whether charging is being done using AC or DC , or depending on the country. An alternative is provided through wireless (inductive)

charging avoiding any power cord to the car. Special consideration of the physical charging environment is necessary here, to ensure safe operation.

C. Billing and Payment for Charging Service

Billing and payment for consumed energy or value added services can be performed through various options:

- At the charging spot, including money, prepaid, credit cards, combination with parking ticket, etc.
- From within the vehicle (e.g., via a contract-related credential stored within the car). This option includes identification of the electric vehicle as well as charging contract verification.

Besides the direct customer interaction, there is also the interaction with clearinghouses that settle accounts between different energy providers. These become necessary when using contract based payment from within a car at a charging spot belonging to a different mobility provider.

D. Negotiated Incentive Rate Plan

Negotiating incentive rate plans may depend on, e.g., the contract between the customer and the mobility provider. Thus different realization options may be:

- **Time of use (TOU)**: The utility provides a price incentive to charge a vehicle at times of lower demand typically based on time of day, day of week, and season of year. Prices are set ahead of time, in an attempt to shift load towards a more favorable time of day.
- **Direct load or price control through utility**: The customer receives a price incentive to give the utility direct control over the charging process. Normally, the customer is given a fixed, reduced price, and the utility has the option to interrupt or delay charging at critical times.
- **Dynamic tariffs**: This is a variation of time of use sometimes called real-time pricing (RTP). Price schedules vary more frequently, usually daily. Once delivered, the prices are firm and the customer, not the utility, controls the load.
- **Critical peak pricing (CPP)**: This is another variation on time of use, in which the utility retains the right to override the price schedule with higher prices on a limited number of days having particularly high demand or other unusual events.
- **Optimized charging**: The customer gives the utility control of the charging load in turn for a price incentive. The utility may, at critical times, reduce or interrupt charging, based in part on the state of charge of the vehicle.

E. Charging Location

The charging location may vary effecting potentially also the provided service and payment options:

- Charging in private environments like the vehicle owner's home or another's home within the same utility's service area or another's home within a different utility's service area. The charging location may not be directly connected with the charging infrastructure in terms of dynamic charging control. Hence, certain options for tariffs or value added services may not always be available.
- Charging at public charge spot can also be distinguished based on the contractual relation of the vehicle owner to the charging spot operator or mobility operator like: charging spot belonging to the same utility as customer contracted, different utility (comparable to "roaming") or charging without a contractual relationship (payment based on money, pre-paid card, credit card, etc.).
- Fleet operator premises may not require a contractual relationship per vehicle directly. They may be based on the fleet operator, providing an energy "flat rate". Control of the charging process may be distinguished as described above.

F. Value Added Services

Connecting the vehicle with a charging spot featuring a communication interface provides the opportunity to leverage this communication connection also for value added services. Examples comprise:

- Software updates for Engine Control Unit (ECU) or infotainment systems
- Remote diagnosis and maintenance
- Multimedia service during charging

G. Electricity Feedback

While in the first place charging is the main service provided for electric vehicles, it is also envisioned to use electric vehicles as dynamic energy storage. The electric vehicle could feed back energy into the Smart Grid upon request. Here, a distinction of the use cases can be done in a similar way as for charging:

- Based on the feedback locations, e.g., for integration within micro grids, to increase their independence from the main grid allowing the local usage of stored energy.
- Based on a local feedback plan, where the customer configures, e.g., a certain amount of energy, which is required as minimum capacity of the vehicle battery.
- Based on backend scheduling / needs.

These use cases show a variety of different services for the electric vehicle charging infrastructure. They illustrate how valuable the transmitted information is for the availability and reliable operation of the services, but also for the safety and privacy of the end user.

III. Information Assets, Potential Threats, and Derived Security Requirements

As just shown in the previous section, various use cases exist in which different peers exchange information to realize a dedicated service. Experience with the existing data communication infrastructure can be leveraged to analyze the charging infrastructure regarding potential threats as well as to determine suitable countermeasures. This may especially comprise security protocols or security mechanisms, which have been proven effective in the current communication infrastructures. Examples comprise security protocols like TLS (Transport Layer Security [4]) and digital signatures.

A. Information Assets in Charging-Related Communication

The information transported over the different connections is the asset that may motivate attacks against the charging infrastructure. The following table summarizes important information assets and their criticality for the system. The majority of these information assets are expected to be transmitted especially over the vehicle-to-grid interface.

TABLE I. INFORMATION ASSETS IN THE ELECTRIC VEHICLE CHARGING INFRASTRUCTURE

Information asset	Description, potential content	Security relation
Customer ID and location data	Customer name, vehicle identification number, charging location, and charging schedule	Affects 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.	Affects system control and billing
Control Commands	Actions requested by one component of other components via control commands. These may also include inquiries, alarms, or Notifications.	Affects system stability and reliability and also safety
Configuration Data	Configuration data (system operational settings and security credentials, also thresholds for alarms, task schedules, policies, grouping information, etc.) influence the behavior of a component and may need to be updated remotely.	Affects 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.	Affects system control (stability and reliability and also safety) and billing
Access Control Policies	Determination whether a communication peer is entitled to send and receive commands and data. Such policies may consist of lists of permitted communication partners, their credentials, and their roles.	Affects system control 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 system reliability.	Affects 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.	Affects customer privacy and competition

B. Potential Threats

Some example threats are described in the following to illustrate the need to integrate security measures into the charging infrastructure right from the beginning. The described threats focus on the specifics of electric vehicle charging and connected communication.

1) Eavesdropping / Interception

Eavesdropping is a passive attack to intercept information, which may compromise privacy or be used to gain more information for additional, active attacks. Eavesdropping requires the adversary to have either physical or logical access to the communication connection. Both the link to the vehicle and to the backend may be intercepted (Figure 3).

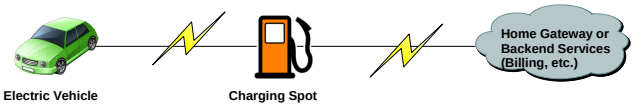

Figure 3. Potential Locations for Eavesdropping.

Communication with the charging spot in general can be done using different technologies, like Wireless or Powerline Communication (PLC). Common to these technologies is that the radiation of the communication transfer (through the frequency used) is high enough that it is sufficient for an adversary to be in closer vicinity to the communication instead of having direct physical access. Missing security measures will enable an adversary to eavesdrop the communication. As shown above, charging related communication may include a variety of information being valuable for an attacker like tariff information, charging status information, or billing relevant information.

2) Man-in-the-Middle Attack

An attacker may intercept communication on the interface between the vehicle and the charging point and modify this information. An example may be tariff options provided by the mobility operator and send via the charging spot to the vehicle. This may be accomplished in the easiest case through a modified charging cable.

Another example is the usage of a faked charge spot as depicted in Figure 4: A potential adversary may use its own (faked) charging spot to which honest customer connect. The adversary's charge spot is connected to an official charge spot and only routes the communication between the honest customer and the original charge spot. The adversary can then consume the charging energy partially, so that the honest customer receives only a fraction of her purchased energy, but pays for the complete consumption by her vehicle plus the adversary's vehicle.

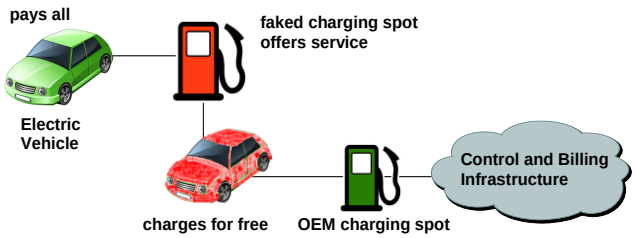

Figure 4. Man-in-the-Middle Attack to steal Energy.

Interesting in this attack is that the adversary actually performs the manipulation on the energy provisioning path and not on the communication path. The latter one is

untouched. This attack shows the need for connecting the flow of energy to the flow of information.

3) Transaction Falsifying or Repudiation

The customer himself may intentionally or unintentionally claim to have received less energy than stated on the billing record. Likewise, the utility may claim to have delivered more energy to the customer.

4) Attack network from within vehicle (and vice versa)

If the electric vehicle is connected to the charging infrastructure, e.g., using a value added service, an adversary (software) may inject or modify application-level traffic intentionally (as an attack) or unintentionally (faulty software component, malware).

5) Tampered or substituted component

A customer may manipulate a component trusted by the utility to provide accurate billing or control information. This affects both components in the charging spot and within the electric vehicle. Examples are pirated or faked replacement parts.

C. First Set of Security Requirements

Basic security requirements of the electric vehicle charging infrastructure have to be addressed. They target the availability and reliable energy provisioning. Moreover, they aim to limit attack effect (geographical and functional), enforce authorized control actions on the smart grid, and correct billing of energy transactions between involved peers (customer, charging spot operator, market, utility).

Based on the stated information assets and depicted threats, the basic security requirements can be addressed more specifically by requiring dedicated cryptographic measures as there are:

- Mutual authentication of end-to-end communicating entities. The authentication may be performed on different layers of the OSI reference model, e.g., on transport layer and on application layer. This is especially useful, if the peer to authenticate against is either a local communication peer or a backend peer, depending on the online state of the charging spot. Hence, end-to-end authentication strongly relates to the related OSI layer and its terminating end points.
- Non-repudiation of billing and tariff information to ensure secure transactions and the connected payment process.
- Protected communication between the electric vehicle and the charging spot, the electric vehicle and backend services, the charging spot and backend services, between backend services.
- Privacy preserving communication between the electric vehicle, the charging spot, and the backend
- Authorization, especially for control of the charging.
- Integrity-protected, authenticated and authorized software updates to avoid malfunctions through software from unauthorized sources
- Logging of security relevant events to enable auditability of the system.
- Security failure and exception handling, to support system reliability, also in case of security breaches.
- In general confidentiality and integrity of sensitive data.
- Support of a secured key management to support all of the requirements above.

These security requirements typically lead to technical and organizational security measures. Hence, to ensure a thorough security approach supporting the interaction of different peers using equipment from different vendors, standardization of an appropriate security approach as part of the overall system approach is necessary.

IV. STANDARDIZATION LANDSCAPE FOR THE CONNECTION TO THE CHARGING INFRASTRUCTURE

This section details the standardization activities focusing on the communication interface between the electric vehicle and the charging spot, but further connections to the backend are also considered. The main focus is placed on standardization activities from the ISO/IEC. An overview about related SAE activities is given as well.

As shown in Figure 5, standardization activities of ISO/IEC and SAE can be divided into four categories: charging connector, charging communication, charging topology, and safety. The following table summarizes more information about relevant standards.

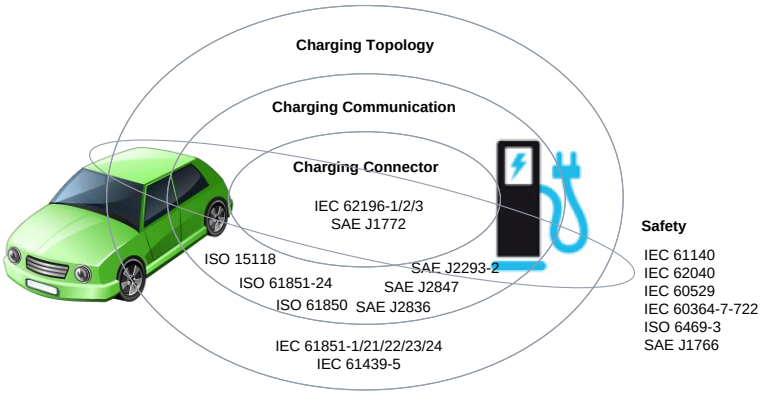

Figure 5. Communication Standards for the Electric Vehicle Charging Infrastructure [1].

TABLE II. COMMUNICATION STANDARDS AND THEIR SCOPE FOR THE ELECTRIC VEHICLE CHARGING INFRASTRUCTURE

Standard	Scope	Content
IEC 62196	Charging Connector	Plugs, socket-outlets, vehicle couplers and vehicle inlets – Conductive charging
SAE J1772	Charging Connector	Electric Vehicle Conductive Charge Coupler
ISO 15118	Charging Communication	Road vehicles - Communication protocol between electric vehicle and grid
SAE J2293	Charging Communication	Energy Transfer System for Electric Vehicles
SAE J2836	Charging Communication	Use Cases for Communication between Plug-in Vehicles and the Utility Grid (-1), Supply Equipment (EVSE) (-2), Utility Grid for Reverse Power Flow (-3)
SAE 2847	Charging Communication	Communication between Plug-in Vehicles and the Utility Grid (-1), Supply Equipment (EVSE) (-2), Utility Grid for Reverse Power Flow (-3)
IEC 61850	Power Systems Communication	Communication networks and systems in substations
IEC 61851	Charging Topology	Electric vehicle conductive charging system
IEC 61439	Charging Topology	Low-voltage switchgear and control gear assemblies

The following sections describe ISO/IEC activities related to charging communication and their IT-security considerations. This overview shows the increasing consideration of IT security requirements in the definition of evolving charging communication protocols. This is especially the case for new protocols like ISO/IEC 15118 targeting the communication for charging control and value added services between electric vehicles and charging spots.

A. *Simple Communication EV/EVSE – IEC 61851*

IEC 61851 (cf. [12][11]) defines a conductive charging system and was standardized in 2001. The standard addresses equipment for charging electric road vehicles at standard AC supply voltages (as per IEC 60038) up to 690 V and at DC voltages up to 1000 V, and for providing electrical power for any additional services on the vehicle if required when connected to the supply network. The standard comprises different parts addressing specific charging options:

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

IEC 61851 targets four different charging modes:

- Mode 1 (AC): slow charging from a standard household-type socket-outlet
- Mode 2 (AC): slow charging from a standard household-type socket-outlet with in-cable protection device
- Mode 3 (AC): slow or fast charging using a specific EV socket-outlet and plug with control and protection function permanently installed
- Mode 4 (DC): fast charging using an external charger

The communication between the vehicle and the charging spot depends on the mode applied. There is no data communication in Mode 1 and Mode 2. In Mode 3 only the control pilot communication exists, while in Mode 4 additional communication functions are available to allow battery management. Common to all modes is that IT-security is not provided. Therefore, there is no protection against any threats discussed in section III.B. Nevertheless, for the vehicle integration into a smart-grid-connected charging infrastructure, (secure) communication is required for tariff exchange, billing, optimization of charge cost and grid load, value added services, etc. To support these functions in the future, ISO/IEC 15118 is currently being specified addressing these communications needs, including an integrated security concept (see next section).

B. *Enhanced Communication EV/EVSE – ISO/IEC 15118*

ISO/IEC 15118 is being standardized in an ISO/IEC joint working group. Its main focus is the interface between an electric vehicle and a charging spot interface. Communication with the backend infrastructure is not directly targeted. The specification is split into different parts, which are all still work in progress:

- ISO 15118-1: General information and use-case definition [6]
- ISO 15118-2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements [7]
- ISO 15118-3: Physical layer and Data Link layer requirements [8]

Security is integral part of the standard and has been considered right from the beginning of the design phase. ISO/IEC 15118-1 contains a security analysis, which investigates in specific threats, which are partly stated in section III above. This security analysis is the base for the security requirements and resulting security measures targeting the specified use cases.

The security measures defined in ISO/IEC 15118-2 build upon existing standards as far as possible. The access media for AC and DC charging will be power line communication in the first step. Support of inductive charging will most likely use wireless communication. As both feature different OSI layer 1 and 2, security measures have been placed on higher layers, to allow an independent solution. Besides the AC and DC profiles, charging options also exists regarding the authentication means. In general, authentication can be performed at the charging spot (External Authentication Means – EAM) or from within the car (plug&charge, or PnC).

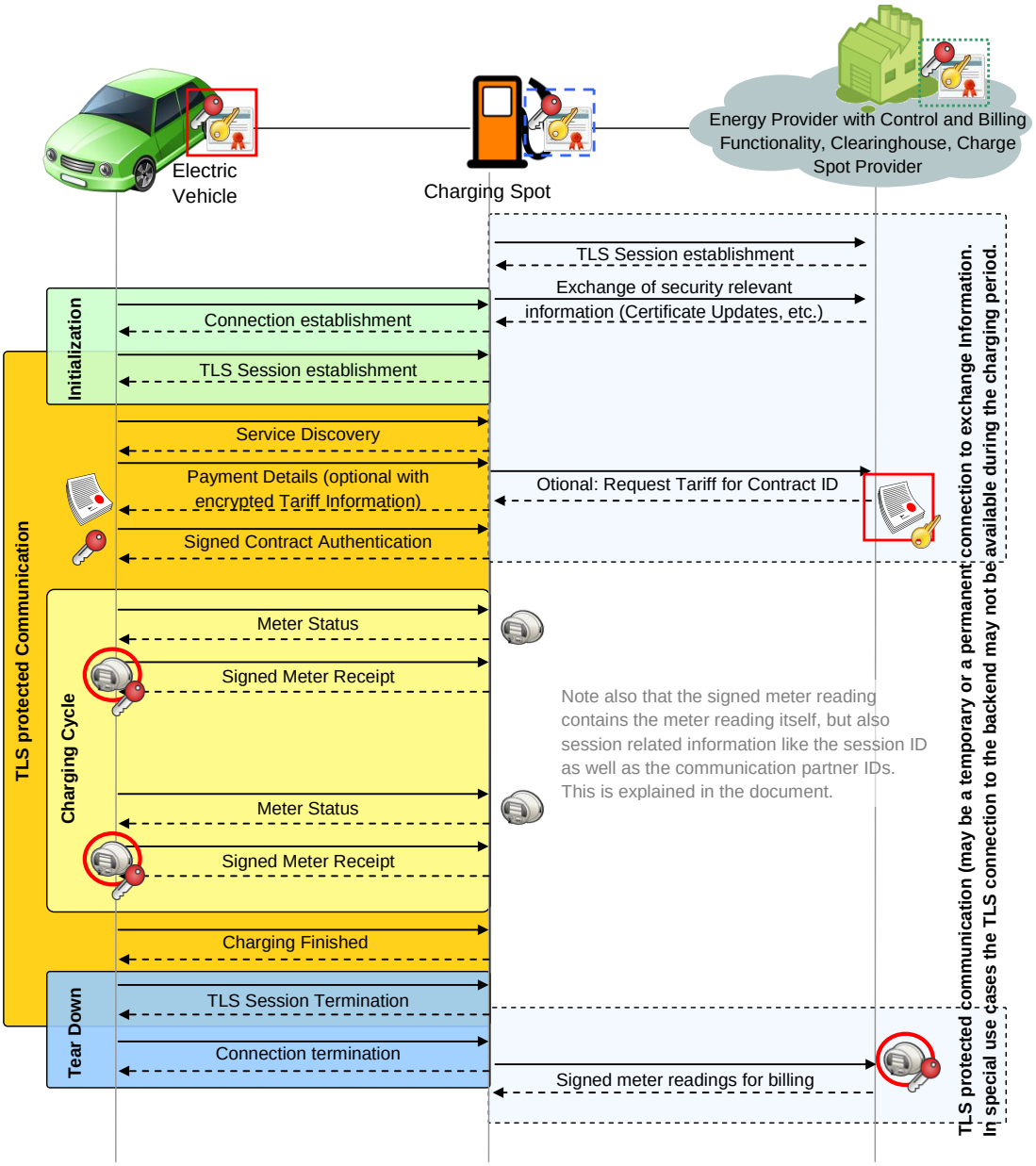

Figure 6. Information Exchange for Electric Vehicle Charging.

While in the first case the user typically may pay directly at the charging spot using either coins or credit cards. Alternatively, authentication can also be done using Near Field Communication (NFC), e.g., an RFID tag (Radio Frequency IDentification) or a mobile phone featuring a NFC interface. In case of PnC, the EV features a security credential allowing it to authenticate itself. While this security credential is typically applied to authenticate towards the charging infrastructure, it may also be used to identify stolen vehicles while charging.

As shown in Figure 6, ISO/IEC 15118-2 applies TCP/IP for the communication between the vehicle and the charging spot. Consequently, security is applied on transport layer using TLS (cf. [4]) ensuring a protected channel between both. Since ISO/IEC 15118 targets the communication between the vehicle and the charging spot, this might be sufficient at the first glimpse. But security measures on application layer have also been defined applying XML security (digital signatures and encryption).

Application layer security became necessary, as the communication also targets billing and payment relevant information, which are exchanged with the backend in contract based payment scenarios. Moreover, to enable contract based payments, the vehicles need authentication means.

To enable secure communication with the backend, the electric vehicle possesses a digital vehicle certificate and a corresponding private key. Here, X.509 certificates [9] are being applied. These security measures go beyond the communication hop between the electric vehicle and the charging spot. The direct data interaction of the electric vehicle with the backend is shown in Figure 6 in the charging cycle loop. Here, charging spot meter readings are signed by the vehicle and forwarded by the charging spot to the backend. They build the base for the billing process later on. Note that the general data exchange in Figure 6 has been simplified and mainly security related exchanges are shown.

The proposed security solution takes the connection state of a charging spot into account to support charging spots that have very limited or even no online connectivity. In general, the charging spot is assumed to be online at least once a day. This online period may coincide with the charging period of an electric vehicle. Therefore, explicit precautions have to be given to the exchanged data, especially, if the backend depends on these.

To enable secure transmission of data from the backend to the vehicle (e.g., updates of credential or of tariff information), a secret needs to be established between the vehicle and the backend allowing an end-to-end encrypted transfer. The vehicle certificate is an ECDSA certificate, where the public key can be considered as static Diffie-Hellman parameters to enable an easy setup of a session based encryption key with a communication peer. Only the backend needs to generate fresh per-session Diffie-Hellman parameters that are used to calculate a fresh Diffie-Hellman secret, which can then be used as session secret. This has the advantage, that the backend can pre-calculate session keys for vehicle communication, once the vehicle's certificate is known at the backend. This approach is known from many of today's web server applications, which use the same technique.

For the normal operation the vehicle certificate will be a contract-based credential. Thus the backend already possesses the certificate information, once the customer enrolled for a contract. For setup operation, the vehicle may possess an OEM credential installed during manufacturing of the car and used for bootstrapping the contact based credential. Notably, the used security mechanisms target elliptic curve cryptography (ECC) for authentication (during key management phases) and for digital signatures. The digital signature standard ECDSA based on ECC provide comparable security to RSA but uses significantly shorter cryptographic key sizes. As the certificates support ECDSA, the Diffie-Hellman key agreement is performed in its elliptic curve variant ECDH. Moreover, elliptic curves can be implemented efficiently in hardware. As ISO/IEC 15118 targets especially electronic control units (ECU) in vehicles and charging sports, memory and calculation constraints are evident and pose further implementation requirements.

The call flow as depicted in Figure 6 is based on the application of unilaterally authenticated TLS, where the electric vehicle implements the client part. Hence, the client is required to check the certificate validity including the issuer. The standard ISO/IEC 15118 requires vehicles to store only a fixed, limited number of root certificates to enable issuer verification. Moreover, it also restricts the number of supported intermediate certification authorities. Besides the validity and issuer, the client also needs to check the certificate revocation status.

One option to avoid the handling of certificate revocation lists is the usage of short term certificates from the server side. Another option is the provisioning of the revocation state by the server itself, e.g., by attaching a fresh Online Certificate Status Protocol (OCSP) response to the certificate during the authentication phase. To keep a balance regarding the implementation and operational effort, the current ISO/IEC 15118 proposal features both, short term certificates for the server side certificates and OCSP responses for intermediate CAs.

As said before, all of the security functionality in ISO/IEC 15118 builds on X.509 certificates and corresponding private keys. Hence, an infrastructure is necessary to manage this key material. It has to be noted, that there are different trust relations for the application and utilization of the key material.

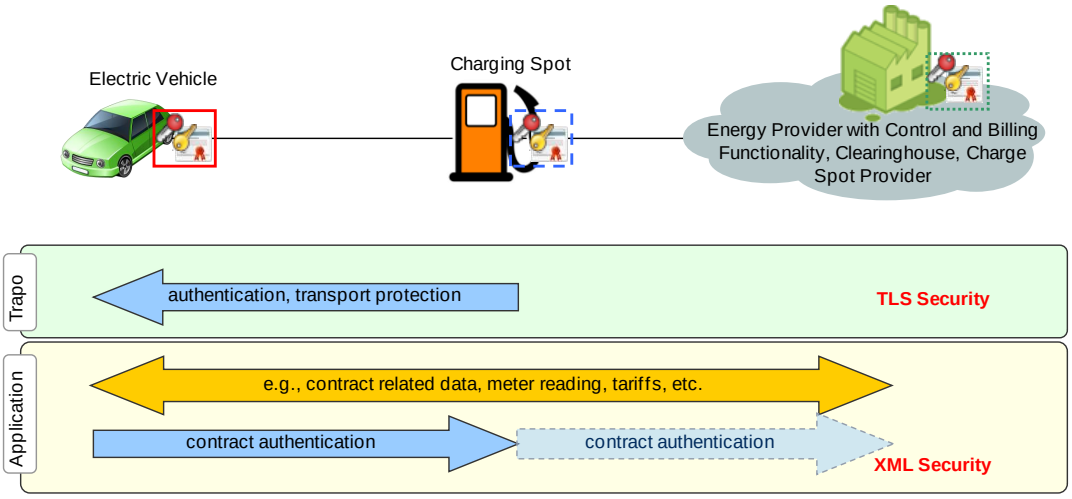

Figure 7. Information Exchange for Electric Vehicle Charging.

As shown in Figure 7 for the transport connection the trust relation exists between the electric vehicle and the charging sport. On application layer there are some messages, which are bound to the communication between the same peers. This applies for instances to the acknowledgement of cyclic meter readings through the electric vehicle by applying a digital signature.

Nevertheless, to get this security on an operational level, electric vehicle and charging spot, both have to get at least the X.509 certificates from a 3rd party. At least, as the generation of public key pairs may be either directly at the component or at the 3rd party. The 3rd party for issuing the certificates may be different. While the electric vehicle will get its contract certificates from a mobility operator, the charging spot will be equipped with a certificate also from potentially another mobility operator. Having different mobility operators relates to the typical situation of having different energy providers depending on the geographic area.

Figure 8 provides an overview of the certificates used by the different actors. Note that this figure reflects the current draft status of ISO/IEC 15118-2. Especially the certification path of the contract certificate may allow also other root certificates as the V2G Root CA in the future. On the vehicle site, the OEM is expected to provide an initial certificate during manufacturing. This certificate is used to enable the secure bootstrapping of operational credentials through the mobility operator. The mobility operator will issue contract based certificates, if the electric vehicle is going to participate in plug&charge scenarios, which allow the payment directly out of the vehicle, without additional identification and authentication at the charging spot. On the infrastructure side, the charging spot needs to possess a certificate and a corresponding private key. The certificate is also issued by the mobility operator, which is not necessarily the same as for the electric vehicle (the mobility operator issuing the contract certificates may be different in roaming scenarios). As the charging spot may be offline during charging and the electric vehicle may not have another communication path to the backend, certificate revocation needs to be addressed in some way. The one depicted in Figure 8 uses short term certificates for the charging spot. Another option is the utilization of multiple OCSP stapling. This approach avoids the handling of short term certificates as an OCSP for both, the charging spot certificated and the issuing sub certification authority certificate can be transmitted to the vehicle.

As described above, digital certificates for the charging spot, and, depending on the use case, also for the electric vehicle, are the basis for protecting the charging control communication. Common to all components for charging control is that the certification path of the certificates applied has a common set of (at east) five root certificates. Five root certificates have been agreed on to address the memory restrictions within an electric vehicle. To enable a smooth operation a dedicated credential management infrastructure (Public Key Infrastructure – PKI, cf. also [9]) handling the initial provisioning, but also the revocation and update of certificates and cryptographic keys is required.

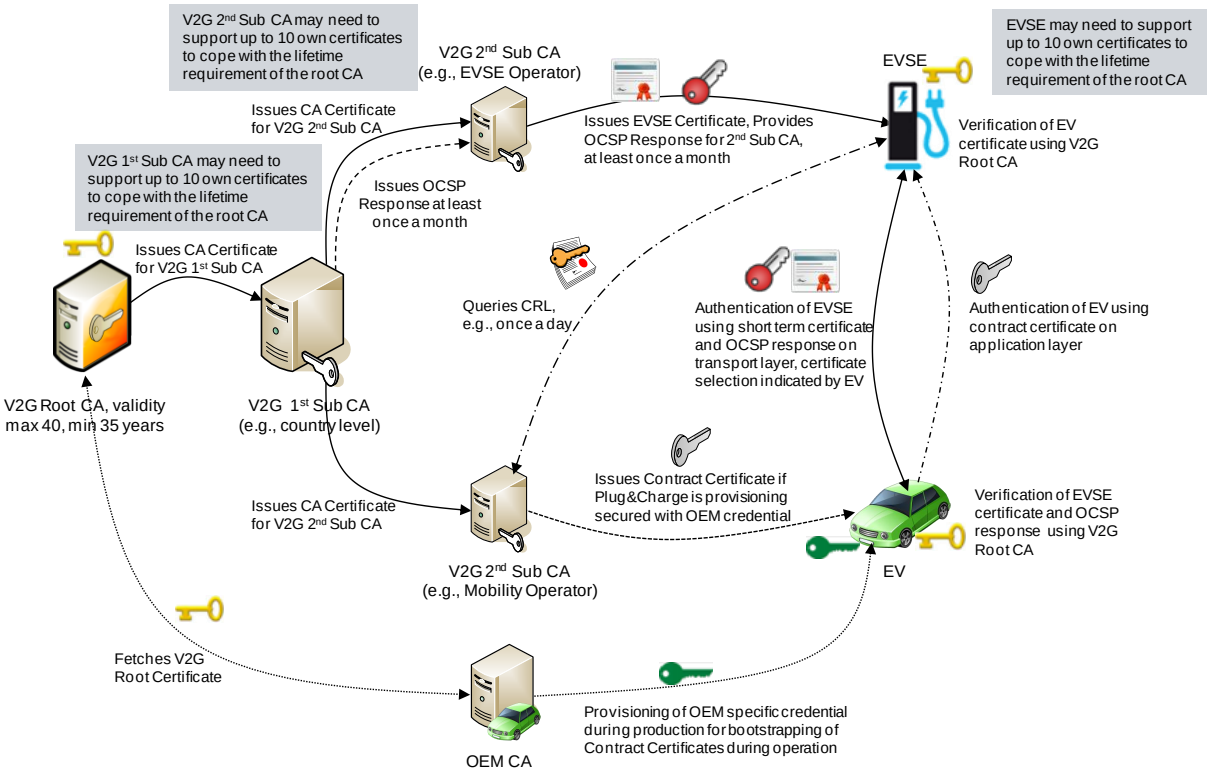

Figure 8. Credential Handling according to current state of ISO/IEC 15118 (DIS), cf. [7].

As ISO/IEC 15118 is in the process of getting finalized, it is expected that the application of certificates will be further optimized to address security on one hand and operation and maintainability on the other.

With the proposed mechanisms ISO/IEC 15118 addresses most of the threats depicted in section III B, with the focus of the interface between EV and EVSE. What is not addressed is the detection tampered of falsified components, which would support the system integrity monitoring. Also, authentication of the EV is only performed in the PnC use cases, which still leaves some possibilities for attacks from rogue EVs.

V. CONCLUSION

The focus of this paper has been the discussion of security requirements and solution approaches for the interface between an electric vehicle and a charging spot. Especially the standard ISO/IEC 15118 was in focus here addressing a variety of use cases while considering security right from the beginning. Nevertheless, to enable online control of the charging operation and also value added services, at least the charging spot needs to be connected to the Smart Grid core.

One standard, which can be directly applied for the energy automation communication is IEC 61850 [10], already applied in substation automation. This communication can be protected by security measures according to IEC62351 [11]. The security in IEC 62351 features similar protection means for TCP/IP based communication which are based on TLS as well. This eases the secure interworking between the Smart Grid communication core and the access via the charging infrastructure. All of these standards employ X.509 certificates. Thus, the key management as enabling functionality becomes a crucial point. The operational handling of an infrastructure providing and revocation information to a multitude of components can be seen as challenge here.

Another communication protocol to be named in this context is OCPP (Open Charge Point Protocol, cf. [14]), which can be used as a protocol between the charging points and the management station. This protocol uses TCP/IP for communication and XML for encoding of messages. Hence, existing security mechanism like TLS and XML security, which are also being employed to protect ISO/IEC15118 as described above, can be utilized here too.

Besides pure charging control, there may be also value-added services provided through the charging spot like multimedia services, software or firmware updates, remote diagnosis, and so on. All of these services have to be protected appropriately. The intrinsic complexity of this overall Smart Grid vehicle charging system requires a systematic approach to include required security measures right from the beginning that can be used and managed efficiently. It is expected that new use cases will enhance the existing security requirements and also influence the further development of communication standards.

VI. ACKNOWLEDGEMENT

The base version of this report (see [13]) compiled in June 2011 has been supported by the German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety within the Harz.EEmobility project under contract 03KP623 (see [3] for more information). The further research and investigation leading to this update of the initial report is part of the FINSENY (Future INternet for Smart ENergY) project (see [4] for more information). The authors gratefully acknowledge the contributions of all FINSENY project partners. FINSENY is partly funded by the European Commission within the FI-PPP, which is part of the Framework Program FP7 ICT.

REFERENCES

[1] R.Falk and S.Fries, “Electric Vehicle Charging Infrastructure – Security Considerations and Approaches”, Internet 2012, June 2012, ISBN: 978-1-61208-204-2, pp.58-64

[2] The German Standardization Roadmap for Electromobility, http://www.elektromobilitaet.din.de/sixcms_upload/media/3310/Normung-Roadmap_Elektromobilit%E4t_en.pdf, last access April 2012

[3] HarzEE-mobility, https://www.harzee-mobility.de/, last access February 2013

[4] FINSENY – Future Internet for Smart Energy: http://www.fi-ppp-finseny.eu/, last access February 2013

[5] T. Dierks and E. Rescorla: “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC5246, IETF, 2008.

[6] ISO/IEC 15118-1: Road vehicles — Vehicle-to-Grid Communication Interface — Part 1: General information and use-case definition, Work in Progress

[7] ISO/IEC 15118-2: Road vehicles — Vehicle-to-Grid Communication Interface — Part 2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements, Work in Progress

[8] ISO/IEC 15118-3: Road vehicles — Vehicle-to-Grid Communication Interface — Part 3: Physical layer and Data Link layer requirements, Work in Progress

[9] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC 5280, May 2008

[10] ISO-IEC 61850, Part 1-9, http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=61850, last access February 2013

[11] ISO-IEC 62351, Part 1-8, http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=62351, last access February 2013

[12] IEC 61851, Part 1, www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=61851, last access February 2013

[13] R. Falk and S. Fries: Securing the Electric Vehicle Charging Infrastructure – Current status and potential next steps, Oct 2011, Berlin, VDI-Berichte 2131, VDI-Verlag Düsseldorf. ISBN 978-3-18-092131-0.

[14] OCPP – Open Charge Point Protocol, http://www.ocpp.nl, last access February 2013