Methoden

Marc Mültin* and Hartmut Schmeck

Plug-and-Charge and E-Roaming – Capabilities Of The ISO/IEC 15118 For The E-Mobility Scenario

Plug-and-Charge und E-Roaming – Potentiale der ISO/IEC 15118 für die E-Mobilität

Abstract: This paper presents the user-friendly plug-and-charge mechanism defined in the ISO/IEC 15118 standard which enables an automatic authentication, authorisation, and billing procedure during the charging process of an electric vehicle. The various certificates, their application in a public key infrastructure as well as the interplay with a clearing house are explained – illustrated using the German joint venture Hubject.

Keywords: Plug-and-Charge, E-Roaming, communication protocols, ISO/IEC 15118, Certificates, PKI, EV, EVSE, Authentication, Authorisation, Hubject, OICP, CA.

Zusammenfassung: Dieser Beitrag präsentiert Informationen über einen benutzerfreundlichen Plug-and-Charge Mechanismus, definiert im aktuellen ISO/IEC 15118 Standard, welcher eine automatische Authentifizierungs-, Autorisierungs- und Abrechnungsprozedur während des Ladevorgangs eines Elektrofahrzeugs beschreibt. Die diversen Zertifikate, deren Anwendung in einer zu erstellenden Public Key Infrastruktur sowie das Zusammenspiel mit einem Clearing House – illustriert am Beispiel des deutschen Joint Ventures Hubject – werden erläutert.

Schlüsselwörter: Plug-and-Charge, E-Roaming, Kommunikationsprotokolle, ISO/IEC 15118, Zertifikate, PKI, Elektroauto, Ladestation, Authentifizierung, Autorisierung, Hubject, OICP, CA.

***Corresponding Author: Marc Mültin,** Karlsruher Institut für Technologie (KIT), e-mail: marc.mueltin@kit.edu
Hartmut Schmeck: Karlsruher Institut für Technologie (KIT)

Abbreviations

CA – Certificate Authority
EV – Electric Vehicle
EVSE – Electric Vehicle Supply Equipment
EVCC – Electric Vehicle Communication Controller
SECC – Supply Equipment Communication Controller
OEM – Original Equipment Manufacturer
PKI – Public Key Infrastructure

1 Introduction

The breakthrough for the electric mobility (e-mobility) in Germany and many other parts of the world, especially regarding electrified passenger cars, has not yet occurred or is at least proceeding rather slowly, as registration statistics of the German Federal Office for Motor Traffic prove. One of the drawbacks has been the missing standardisation of hard- and software regarding the workflow of recharging an electric vehicle (EV). In January 2013, the German proposal for the type 2 plug (specified in IEC 62196 [1]) has finally been approved as the standard for EVs regarding AC (alternating current) charging by the European Commission. Furthermore, the European and American automakers agreed upon a unified charging system, the *Combined Charging System (CCS)*, in mid 2013. The CCS mainly consists of the EV inlet and the plug as well as connectors for AC and DC (direct current) charging. These decisions add up to security of investments for the automaker and charging infrastructure industry on the one side and a lowered barrier for the customers and drivers of EVs to engage into e-mobility on the other side.

Electric vehicles can be charged in four different charging modes which are defined in the IEC 61851 [2] standard. These modes basically differ with respect to the allowed charging capacities, communication mechanism with the EV and the required safety devices. The safety requirements increase from mode 1 to mode 3, which is why the European Automobile Manufacturers' Association (ACEA) recommends mode 3 charging for publicly accessible charging stations (henceforth called EVSEs for Electric Vehicle Supply Equipment), and mode 2 charging for

charging at home, if no mode 3 charging station is available [4].

Furthermore, IEC 61851 defines a mechanism which maps the maximum charging currents allowed by the EVSE *via* an analog PWM (Pulse Width Modulation) duty cycle signal using the control pilot (CP) pin of the charge plug and ensures that the power flow is only activated if the EVSE is connected to a stationary vehicle. Thus, IEC 61851 is an *analog safety-related low-level protocol*.

By means of the PWM duty cycle, a simple load control can indeed be realized, yet, essential information, such as the energy needed in total by the EV or the intended departure time, which would allow to exploit the *charging flexibility* of the respective EV and therefore realize a more sophisticated load control, cannot be communicated.

The need for a load control originates from the change of our existing power grid into an evolving system with wind and solar based power plants as our ever increasing source of electricity generation. The availability of this electricity is highly dependable upon the regional weather situation which leads to the fact that with the new evolving power system the energy consumers need to at least partly adapt their load towards the availability of electricity from those fluctuating renewable energy sources.

In 2009, the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) jointly formed a standardisation initiative to establish an internationally common ground for the definition of a *digital communication protocol* between an EV and an EVSE which would allow a user-friendly "plug-and-charge" mechanism for *authentication, authorisation, billing, and flexible load control* based on a wide set of information exchanged between an EV and an EVSE, including a contract concluded between customer and e-mobility provider which is stored inside the EV. An identification *via* an RFID card is no longer necessary, but still specified as a use case. This initiative yielded the international standard ISO/IEC 15118, entitled "Road vehicles - Vehicle to grid communication interface". It should be noted that the term "vehicle to grid" in this title is a bit misleading, since it is in fact only an "EV to EVSE" communication. The communication between an EV and EVSE *via* this protocol is built upon the basic signalling concept described in IEC 61851 and starts as soon as a PWM duty cycle of 5 % is applied. With regards to the conductive charging modes defined in IEC 61851, mode 3 is required for this high level communication protocol.

The ISO/IEC 15118 standard already consists of eight different parts, with the first three parts defining the *conductive charging* scenario, parts four and five specifying *compatibility tests* to ensure interoperability of different implementations, and parts six to eight complementing the conductive parts with specifics regarding wireless communication means for *inductive charging*. The functionality of this standard with respect to load control shall not be further discussed at this point. Refer to [3] for more detailed information on that matter. In fact, this paper focuses on the authorisation and authentication process which allows to realize an *e-roaming* scenario. E-roaming shall be understood as the possibility to charge one's EV not only at those EVSEs belonging to the e-mobility provider one has signed a contract with, but at all EVSEs connected to a common clearing house. As opposed to a manual identification process *via* an RFID card or any other external identification means, the concept described in ISO/IEC 15118 provides a mechanism where the driver just needs to connect his EV to an EVSE *via* his charge plug and all aspects of authentication, authorisation, billing, and even load control are taken care of automatically *via* the communication protocol – based on one single contract the driver has concluded with his energy provider. This mechanism gains even more significance in the inductive charging scenario since less interaction with the charging equipment yields a higher user comfort and raises acceptance of and belief in e-mobility.

2 Certificate concept in ISO/IEC 15118

The following information about the definition of certificates as well as their handling to enable authentication and authorisation is based on an informative annex of the second part of ISO/IEC 15118 (ISO/IEC 15118-2), entitled "Network and application protocol requirements" [5]. This document is currently in the state of a final draft for international standard (FDIS) and is expected to be adopted as international standard (IS) in Q2 2014.

The certificate concept implemented in this standard forsees several types of certificates which come into play when establishing a public key infrastructure (PKI). In order to understand this concept, some preliminary considerations need to be explained regarding automaker (henceforth called OEM) as well as so-called "secondary actor" requirements, where a secondary actor would for example be an e-mobility provider.

2.1 OEM requirements

An OEM generally has the desire to keep control units (such as the Electric Vehicle Communication Controller - EVCC) from becoming very expensive. Furthermore, manual treatment of a control unit (*e.g.* in a garage) causes overhead to the customer and has to be avoided.

The easiest way of installing a certificate into the vehicle without later effort is at production time. This, however, requires a very long validity of this certificate, at least as long as the lifetime of an EV. Such rather static certificates could be the root certificates used in a PKI.

Yet, on the other hand, the contract a customer concludes with his chosen e-mobility provider for charging his EV at public EVSEs as well as the corresponding contract certificate may not exist at production time of the EV. Moreover, a customer may want to change his e-mobility provider over time, which is a major reason why root certificates cannot be used for all purposes. Additionally, the validity of a contract certificate used for plug-and-charge is usually only bound to the validity of the contract.

Hence, it needs to be possible to install certificates *via* the charge protocol, especially non-static ones such as the contract certificates.

Moreover, since persistent storage is expensive in the automobile industry, the number of multiple certificates of the same type (*e.g.* multiple root certificates) to be installed, the respective chain length as well as each certificate's size must be reduced to a minimum.

2.2 Secondary actor requirements

The organisational overhead to manage a PKI should be kept small which means that the coordination between companies or organisations needs to be reduced to a minimum. A first approach would be to organize all secondary actors in one common group that uses and distributes a common root certificate which is then installed in each vehicle. All certificates (*e.g.* contract certificates) created by the secondary actors could then be derived from this single root ceritificate by signing the respective certificates with the private key of the root certificate.

It is, however, difficult to establish one common group world-wide, which is why the need for intermediate organisations and certificates arises. Therefore, a more reasonable approach would be to establish multiple groups, for example different groups for the various continents, countries and kinds of secondary actors (*e.g.* operators of EVSEs, utilities, and e-mobility providers). A central organisation within each group could then use its own root certificate and the corresponding (very secret) private key which makes the certificate management easier.

In order to reduce communication costs for the communication controller of the EVSE (Supply Equipment Communication Controller – SECC), it would be beneficial if the EVSE could stay offline during the whole charging procedure.

2.3 Certificate types defined in ISO/IEC 15118

Before the resulting decisions for the certificate concept are illustrated, we need to first introduce the different kinds of certificate types as they are defined in this standard. The wording is almost identical to the definition given in the ISO/IEC 15118-2 document.

V2G Root Certificates

These are globally valid (top level) root certificates of the PKI. They are used to check the authenticity of certificates. The corresponding private keys are in possession of the respective root certificate authorities (CAs). V2G stands for Vehicle-to-Grid.

Mobility operator root certificate

This kind of certificate is used to sign (*via* a chain of sub-CAs) contract certificates.

Contract certificate

This kind of certificate is used in the plug-and-charge use case (*i.e.* contract-based charging) to represent a contract between a vehicle and a secondary actor (the e-mobility operator). It is stored in an EVCC along with the corresponding private key. The EVCC uses it to prove the existence of the corresponding contract to the EVSE. Contract certificates are derived from a mobility operator root certificate.

SECC certificate

This kind of certificate is used to authenticate the SECC to the EVCC. The corresponding private key is in possession of the SECC. SECC certificates are derived from the V2G root certificates mentioned above.

OEM provisioning certificate

This kind of certificate is individual for each vehicle (installed *e.g.* at vehicle production) and used to verify the identity of a vehicle at the beginning of the provisioning process (see section 2.5).

OEM root certificate

Such an OEM root certificate is used to sign OEM provisioning certificates. Each OEM may create a (top level) root certificate and distribute it to the secondary actors (and clearing houses). The root certificate of an OEM is not part of the global PKI; *i.e.*, it is not necessarily signed by a V2G root certificate.

2.4 Resulting decisions for the certificate concept

Based on the OEM and secondary actor requirements stated above, which in some cases are of a conflicting kind, a number of decisions for the certificate concept were reached, reflecting at some points compromises made between the various perspectives of the OEM, e-mobility provider, and charging infrastructure industry.

Size of a single certificate

An X.509 certificate in DER (Distinguished Encoding Rules) encoded form shall not be bigger than 800 Bytes. This can be achieved by leaving out irrelevant information such as the address of the issuer.

Length of certificate chains

The OEMs desire to keep the memory space needed for certificates small conflicts with the secondary actors' view that long chains are easier to manage. A compromise is reflected by the decision to restrict the path length to three, meaning that the chains consist of a *root certificate*, followed by at most two *intermediate certificates* and finally the *leaf certificate* closing the chain.

One can imagine this chain as follows: There could be one single trust center with one single root certificate (V2G root certificate) for each continent. Now an arbitrary number of intermediate organisations can be created, one for each country, whose intermediate certificates are then signed with the private key of the continent's top level root certificate. One level below, each intermediate organisation (such as one created for Germany) could now create "company certificates" (mobility operator root certificates) for each secondary actor (such as a utility or any kind of e-mobility provider). Those second level intermediate certificates could then be used to create and sign the respective customer certificates such as the contract certificates (leaf certificate) used to authorize a customer for the charging process at an EVSE.

Number of root certificates

As a compromise, at least one root certificate is required to be installed in each EV, but a minimum of 5 root certificates (corresponding to the number of continents) is recommended.

Validity of root certificates

In order to avoid the necessity to create root certificates very often – which are installed at production time of the EV – it was decided upon a validity of 40 years, reflecting a time frame big enough to cover the usual lifetime of a vehicle.

Validity of OEM provisioning certificates

It is requested that new OEM provisioning certificates have a validity period of 30 years.

Installation of contract certificates

Those certificates are to be installed *via* the mechanisms of the charge protocol. The *CertificateInstallationReq/-Res* and *CertificateUpdateReq/-Res* messages defined in ISO/IEC 15118-2 (the request message is always initiated by the EVCC, the SECC answers with the respective response message) are used to realize the installation and update of contract certificates.

Validity of contract certificates

The minimum lifetime of these kinds of certificates is four weeks, unless the contract lifetime is shorter.

Validity period of SECC certificates

The validity period of those certificates it not further specified, it is solely mentioned that a "short term" time period is to be applied.

2.5 Provisioning certificate procedure

Installing a contract certificate into the EV should be done in an automatic way, as already discussed, in order to reduce overhead and costs for the customer. This procedure is called *certificate provisioning*. With the help of the CertificateInstallationReq/-Res messages the certificate contract can be transmitted from the secondary actor (*e.g.* e-mobility provider) to the vehicle for installation. In order to enable certificate provisioning, activities which happen outside the charge protocol are required additionally and illustrated in Figure 1.

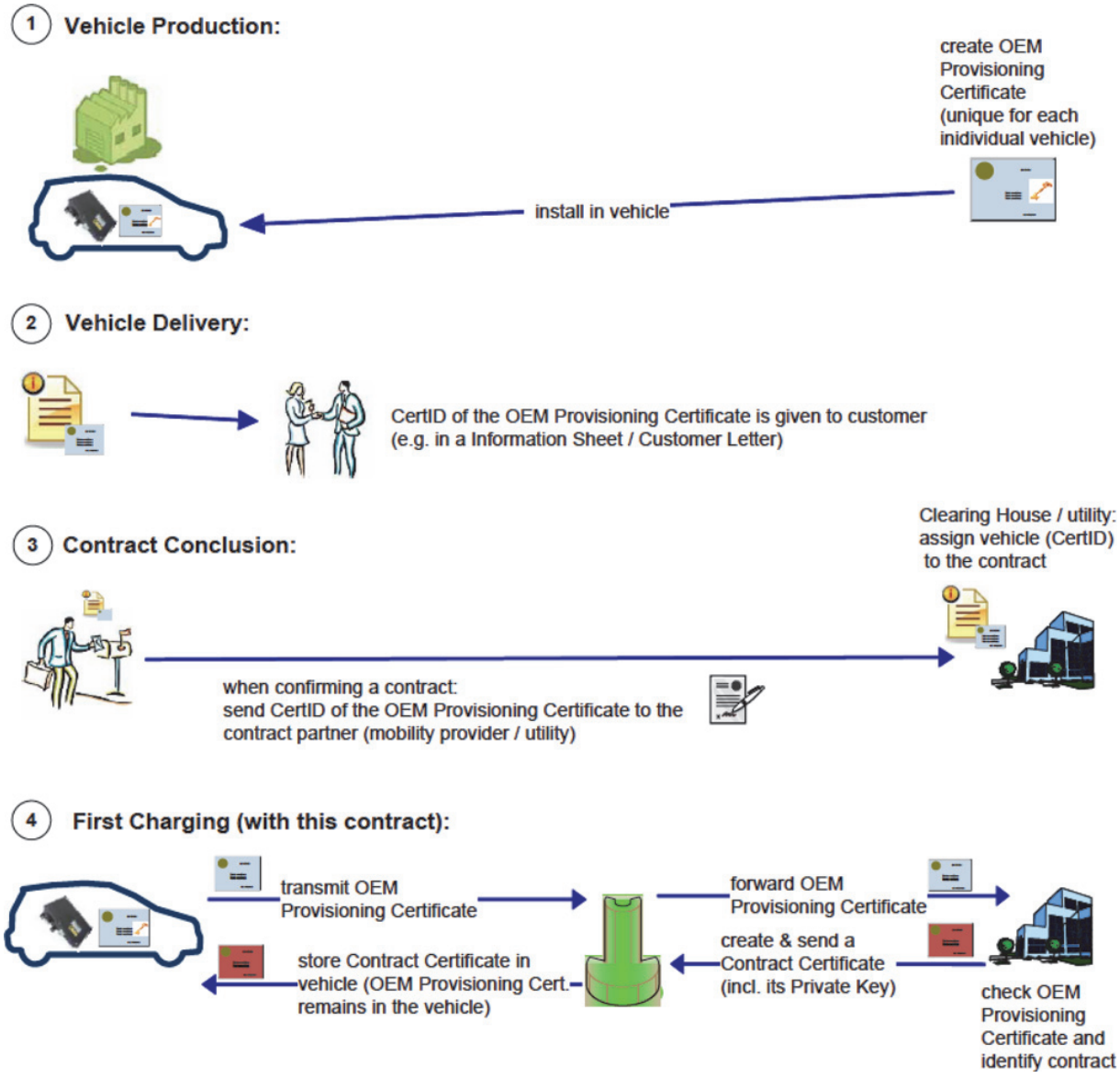

Figure 1: Activities required for OEM certificate provisioning (Source: ISO/IEC FDIS 15118-2).

The first step ① is the installation of a unique OEM provisioning certificate in the EV at production time.

As soon as a customer buys a new EV, he will be handed over the details of the OEM provisioning certificate (denoted with CertID in the figure) by either distributing information sheets, integrating the CertID in the vehicle documentation, or offering online access to the information ②.

When concluding a new energy contract to get access to charging infrastructure, the customer forwards the OEM provisioning certificate details to his contract partner (*e.g.* a utility or any other kind of e-mobility provider) who assigns the CertID to the contract information within his IT systems ③. Furthermore, the contract partner creates a contract certificate which is as well bound to the given unique CertID. The information about the existence of a contract for this CertID is forwarded to the clearing house of this country – ideally together with the contract certificate in order to avoid delays later on during the authentication process at the EVSE.

Now, whenever the customer charges his EV the first time at a public EVSE (or whenever the contract certificate already installed inside the EV is not valid any more), the EVCC forwards the OEM provisioning certificate to the

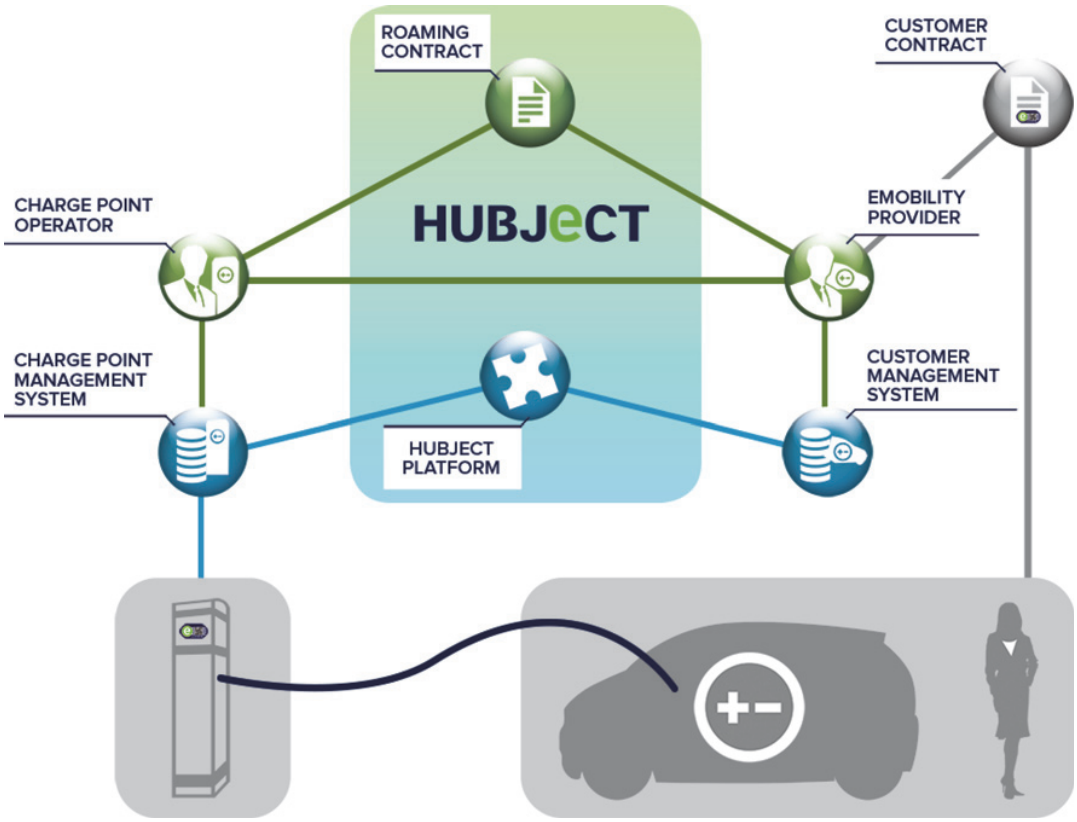

Figure 2: Hubject role model for the e-roaming scenario (Source: Hubject.com).

SECC (within the CertificateInstallationReq message) ④. The SECC in turn forwards the certificate information to the clearing house (or all known e-mobility providers)[1]. The clearing house checks whether the OEM provisioning certificate is valid by using the OEM root certificate and checks whether a contract for this provisioning certificate is registered. If the corresponding contract certificate was not sent to the clearing house before, then the clearing house requests a contract certificate from the e-mobility provider which concluded the contract.

Finally, the contract certificate (including the certificate chain necessary for validation) and the corresponding encrypted private key are sent *via* the SECC to the vehicle by using the message CertificateInstallationRes. It should be noted that the certificate chain of an SECC is certainly as well transmitted to the EVCC (but not installed) to enable an authenticity check of the SECC before a TLS connection is established.

As one can see, the certificate handling outlined in the ISO/IEC FDIS 15118-2 document seems to be a rather complicated mechanism at first glance and time will prove if these ideas will prevail and be widely implemented by the respective actors, *i.e.* OEMs, clearing houses, and e-mobility providers. However, a customer usually has a contract with his e-mobility provider which allows him to charge his EV at those charging stations belonging to this provider. Yet, those EVSEs might not be installed all along the route of the EV driver, especially when it comes to international road trips. The introduced certificate concept thus illustrates how this problem could be solved, lowering range anxiety for EV drivers, raising customer comfort and at the same time lowering costs needed to provide several RFID cards to authenticate oneself at different EVSEs belonging to different e-mobility providers. This vision works the better the more e-moblity providers join a common clearing house.

There are already bilateral coordinatory meetings taking place between some German OEMs and the German

1 The Open Charge Point Protocol (OCPP) [7] describes a method enabling EVSEs to communicate with managing central systems from different vendors (not necessarily a system of the charge point manufacturer) *via* web service communication (SOAP). The central management system itself then needs to communiate with the clearing house. For further information regarding this workflow refer to [3].

joint venture Hubject which acts as a clearing house to enable e-roaming in the e-mobility context. Hubject is a B2B service platform providing a simple information and transactional gateway for the automation of contract-based business relationships between power suppliers, car manufacturers, infrastructure service providers as well as further mobility business parties. Its vision is amongst others to provide customers a simple and provider-independent access to public and semi-public charging infrastructures, thereby linking regional and national (European) e-mobility markets. Its e-roaming system allows the customers to access all public charging stations connected to the platform, both those of other suppliers and those operated by their own e-mobility providers which are partners in the Hubject network. For this purpose, the customer needs to conclude just one single contract. An illustration of this concept is given in Figure 2.

The Hubject role model forsees two major business roles: Participants in the Hubject network either just operate EVSEs and thus supply energy (charge point operators) or they directly act as e-mobility providers and supply the customer with an energy contract. It is also possible that a market participant takes both roles, with the utility RWE – one of the founding business partners of Hubject – being just one example.

Hubject released its Open InterCharge Protocol (OICP) [6] in April 2013 and has since then acquired international partners in Europe (*e.g.* Finnland, Denmark, Netherlands) and even world-wide, such as in Japan.

It should be noted at this point that the OICP is closely related to the far greater standardisation initiative of the European "Green eMotion" Project [8]. The objective of this mammoth project (with 43 industry partners participating on a European scale) is the development and demonstration of an interoperable and customer-friendly e-mobility system – going beyond e-roaming – on the basis of a B2B service platform.

The public key infrastructure discussed in this paper does not yet exist. Authentication and authorisation at Hubject-compliant EVSEs is yet realised by various external identification means, such as RFID card, SMS and QR-code scanning *via* a smartphone. The question arises as to which future player will act as a nationwide root certificate authority. Should it be a public authority such as *e.g.* the Federal Office for Motor Traffic (Kraftfahrtbundesamt – KBA), or could a privately run company like the Telekom – which is a well established trust center – or even a new joint venture from the e-mobility sector take the role as a security provider? Either way, it must be an organisation which is commonly perceived as being trustworthy and neutral.

2.6 Simplified certificate management in a private environment

The overhead needed for public charging can be reduced when it comes to private or semi-public charging. Each local environment, be it a private parking garage or a garage or parking lot of a company with its own EV fleet, needs a unique so-called private operator root certificate. Each EVSE (wall-box or charging station) in this local environment will then be equipped with an SECC certificate which is signed by the private operator root certificate – previously created by the EVSE manufacturer – specifically created for this local environment. The respective EVs which are supposed to charge at this local environment need the private operator root certificate to be installed as well in order to check at TLS connection creation whether the SECC certificate is in fact derived from the private operator root certificate.

Compared to the public charging scenario, no intermediate CAs and certificates are needed, all leaf certificates are directly signed by the private operator root certificate. The billing aspect in private environments is not addressed as this issue is not the focus of this technical specification (in the form of an informative annex). However, at least two alternatives are conceivable:

1) A separate smart meter installed inside or exclusively connected to a wallbox (EVSE) is used to measure the energy which is to be billed corresponding to the same energy contract which has been concluded to charge one's vehicle at public EVSEs.
2) The charged energy is registered *via* the meter already installed at home (or on the premise of a company) and is therefore billed on the basis of the energy contract applied for the respective premise.

The latter case seems to be the more reasonable one, especially since the operational costs of a smart meter are – at least in Germany – passed to the customer who might not accept this additional financial burden.

3 Conclusions

We presented the concept of a user-friendly plug-and-charge mechanism for *authentication, authorisation and billing* based on the ideas sketched in the ISO/IEC 15118 standard, currently in the status of a final draft for international standard (FDIS). Having introduced the various demands from the OEM's and e-mobility provider's view regarding ease of certificate management and establishment of a PKI, we illustrated the various certificates which come

into play as well as their application in an e-roaming context. One representative of a German clearing house, the joint venture Hubject, has been pointed out to illustrate the interplay between the market participants OEM, customer, e-mobility provider and charge point operator. At last, the application of certificates for the charging process in a private environment (*e.g.* private garage, company car park with its own fleet) has been explained and compared to the public use case.

After all, time will show if these ideas prove themselves to be the most convenient way of implementing an e-roaming infrastructure which not only prevails nationwide, but internationally.

Acknowledgement: We gratefully acknowledge the financial support from the Federal Ministry of Economics and Technology for the project iZEUS (funding number 01ME12013) and EIT ICT Labs which provided the environment for this paper.

Received January 8, 2014; accepted February 5, 2014.

References

1. *IEC*: IEC 62196-2 ed1.0: Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles URL: http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/45684?OpenDocument [Access on 5.1.2014].
2. *IEC*: IEC 61851-1 ed2.0: Electric vehicle conductive charging system - Part 1: General requirements URL: http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/44636 [Access on 5.1.2014].
3. *M. Mültin, C. Gitte, und H. Schmeck*: Smart Grid-Ready Communication Protocols And Services For A Customer-Friendly Electromobility Experience. In: GI 2013 LNI ISBN 978-3-88579-614-5, Pages 1470-1484.
4. *ACEA - European Automobile Manufacturers' Association*: ACEA position and recommendations for the standardization of the charging of electrically chargeable vehicles. URL: http://www.acea.be/images/uploads/files/Updated_ACEA_position_on_charging_ECVs.pdf [Access on 5.1.2014].
5. *ISO/IEC*: ISO/FDIS 15118-2 Road vehicles – Vehicle-to-Grid Communication Interface – Part 2: Network and application protocol requirements. URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=55366 [Access on 5.1.2014].
6. *Hubject*: Open InterCharge Protocol v1.1. URL: http://www.hubject.com/pdf/closed/v_1.1_Open_Intercharge_Protocol_(OICP).pdf [Access on 5.1.2014].
7. *E-laad*: Open Charge Point Protocol v2.0. URL: www.ocpp.nl [Access on 5.1.2014].
8. *Green eMotion*: The European framework for an interoperable electromobility system. URL: http://www.greenemotion-project.eu [Access on 5.1.2014].

Dipl.-Inform. Marc Mültin
Karlsruher Institut für Technologie (KIT),
Institut AIFB – Geb. 05.20, Kaiserstraße 89,
76133 Karlsruhe
marc.mueltin@kit.edu

Dipl.-Inform. Marc Mültin joined the research group of Prof. Schmeck at the Institute AIFB in May 2009 and is an active member of the German standardisation committee (DIN) NA 052-01-03-17 AK "Kommunikationsschnittstelle vom Fahrzeug zum Stromnetz (V2G CI)" for the ISO/IEC 15118 standard. His main interests are: future ICT-based efficient energy systems, integration of bi-directionally charging electric vehicles (EVs) into the energy management system of a smart home, optimized charge control of concurrently charging EVs. He also maintains a blog under http://www.smart-v2g.info/blog.

Prof. Dr. Hartmut Schmeck
Karlsruher Institut für Technologie (KIT),
Institut AIFB – Geb. 05.20, Kaiserstraße 89,
76133 Karlsruhe
hartmut.schmeck@kit.edu

Prof. Dr. Hartmut Schmeck has a Chair of Applied Informatics at the Institute AIFB of the Karlsruhe Institute of Technology (KIT), additionally he is a director of the Institute for Applied Computer Science (IAI) of KIT and of the Research Center for Information Technology (FZI). He has been the coordinating Principal Investigator in several cooperative projects on future energy systems and electric mobility like MeRegio, MeRegioMobil, and iZEUS. His main interests are: controlled self-organisation in networked adaptive systems, challenges of volatile and highly decentralized power generation in future energy systems.