EVS32 Symposium
Lyon, France, May 19-22, 2019

A public key infrastructure for smart charging solutions:

for safe and seemless charging in an open market for electric vehicles

Baerte de Brey & Lonneke Driessen (*ElaadNL, Utrechtseweg 310, 6812 AR Arnhem, baerte.debrey@elaad.nl, lonneke.driessen@openchargealliance.org*)

Executive Summary

An important aspect of ISO 15118 is a supporting Public Key Infrastructure (PKI) for managing certificates.
With the exponentially growth of electric vehicles (EV) and their charginginfrastructure, the need for better security grows with it as well. Since electric cars and Smart Charging will be a crucial part of the electricity system in the near future, protocols and techniques which rely on measurements and data, the integrity and authenticity of data must be of uncontested reliability. In this paper, a study of the use and need of digital signatures in the EV infrastructure is discussed. This study aims to give more insight in how the implementation of digital signatures could technically work, what risks are mitigated and how the organizational process could work. Keywords: *Electric vehicles, cyber security, digital signatures, public key infrastructure*

1 Smart Charging

More and more electricity is generated by the power of the sun and the wind. This growth means that there will be times where there is more supply than demand for electricity. To fully use this abundance of power, storage is necessary. What better than to use the growing fleet of electric vehicles (EVs) to charge at the best possible moments via smart charging? With innovative techniques we can make sure electric vehicles are charged, for example during the night when the wind is blowing fast and there is little demand for electricity or in the afternoon at the moment the power of the sun is at its peak.

A very important aspect of smart charging is to make sure the EV receives the needed energy amount before the EV driver needs to depart. Research shows that, when EV drivers are confident that their EV will be charged by the time they need to leave, they are very receptive to smart charging programs. These programs can offer charging when energy prices are low, when renewables are abundant and at times when the grid can cope best. When the mobility needs of the EV driver are combined with pricing information and infrastructure constraints, an optimal charging schedule can be designed to meet everybody’ s needs. This of course needs to be done in a secure way. Secure EV charging is important for many reasons: EV drivers must be absolutely certain they can drive to work in the morning, or that they can use their car in case of emergency; Safety of operation of both the charging infrastructure, EV and the electricity grid must be guaranteed; Consumer data privacy and revenues must be protected.

2 Open Markets for Electric vehicles

Open markets enable fair competition between market players. The European Commission states that fair competition encourages enterprise and efficiency, creates a wider choice for consumers and helps reduce prices and improve quality (see appendix). In the emerging EV charging market, fair competition will stimulate the growth, innovation, quality and affordability of EV charging infrastructure and services and subsequently the adoption of electric vehicles.

3 Introduction of 15118

In the EV charging ecosystem there are many actors that exchange information, as can be seen in figure-1. The various routes for information exchange exist simultaneously and offer the industry and consumers options that are especially important in the developing EV charging industry. ElaadNL researches and tests all these routes in various projects and with many different project partners. This document focusses on the information exchange using ISO 15118.

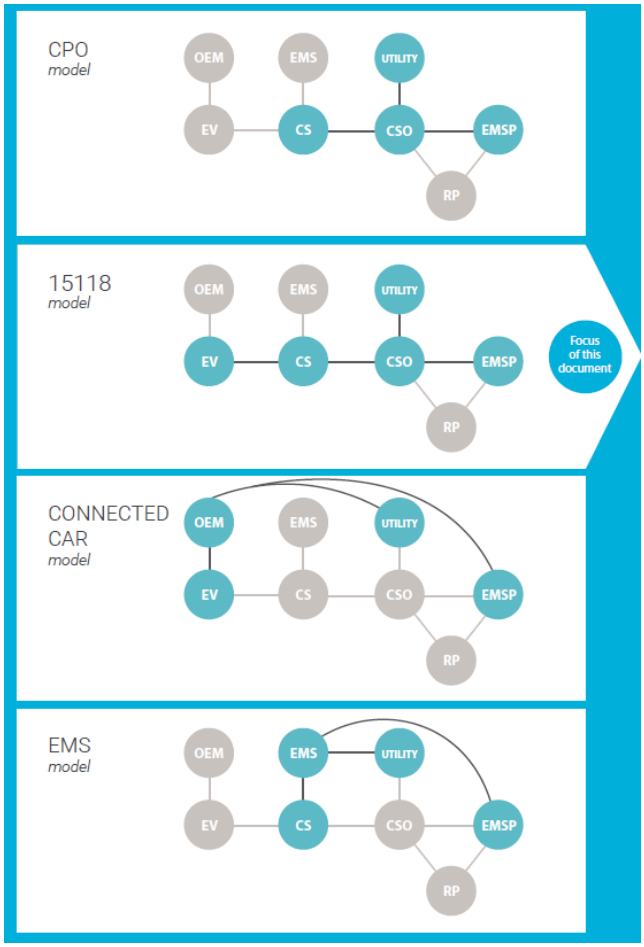


Fig 1. There are many different actors in the evolving EV Charging Ecosystem. When modelling this ecosystem, various sub-models can be identified.

The new ISO 15118 standard provides the necessary information exchange directly between the vehicle and the charging infrastructure. This information can then be passed onwards to the EMSP and the grid, ensuring secure and optimal charging that meets everybody's needs. The ISO 15118 standard was published in parts between 2013 and 2015 by the International Organization for Standards (ISO). It has since then been adopted by the International Electrotechnical Commission (IEC) and currently a joint working group of IEC and ISO continue the further development of the standard. The standard introduces more advanced communication, referred to as "High Level Communication", between EV and Charging Station. The main features of the standard are:

1. Ease of use for the EV user: authentication and authorization by just plugging in a charging cable, also known as "Plug and Charge".

2. Security, by using digital certificates both on the transport layer as well as for contracts on the application layer (instead of using charging cards). This also enables securely exchanging tariffs and metering data.

3. Smart Charging. This includes a number of use cases such as schedule-based charging and - in future versions - reactive power compensation and vehicle to grid charging. Currently the main feature of the standard from a Smart Charging perspective is that this protocol can communicate the mobility needs to the charging infrastructure (and onwards to the electricity grid) and pricing information and infrastructure capacity to the EV. It has the requirements needed to bring smart charging to the next level.

Currently, a draft version of the 2nd edition of ISO 15118 is under public review. At the time of writing this document, the draft edition 2 document does not impact the content of this report. It is essential for the ISO 15118 standard that it is supported by a Public Key Infrastructure (PKI). A Public Key Infrastructure is a

system for managing digital certificates that are used for securing digital communication. Such a PKI would need to be in place before ISO 15118 can be introduced to the EV charging ecosystem on a large scale, and that EV users can start making use of its benefits.

4 General explanation of a Public key Infrastructure system

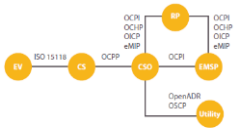
A Public Key Infrastructure (PKI) is asystem for managing digital certificates that are used for securing digital communication. Digital certificates are based on key pairs consisting of a private and a public key. These two keys are mathematically linked. A private key is kept secret by the owner of the certificate. The matching public key is part of a certificate that is shared with other participants in the ecosystem. By using this mathematical link, certificates can be applied as a means for authorization and for making sure data is not changed or cannot be read by others.

Certificates are issued by a Certification Authority or “CA”. Parties who decide to take part in a PKI, trust the Certificate Authority and use its public key to validate the digital communication. A subordinate certificate authority (SubCA) inside the PKI can also issue certificates. Trust in the SubCA is established by having its own certificate issued and signed by the RootCA.

Setting up a PKI is common practice and used for many applications where many parties want secure communication.

5 The use of certificates in a multi-player ev charging system

A number of choices must be made when setting up a PKI to enable secure communication for a new market or ecosystem. These decisionsmust be made beforehand, since the devices and systems that want to setup secure communication channels need to know what certificates have to be present to verify incoming connections and decrypt messages.



Before implementing any technological solutions, it is important to have an alignment between the roles and business requirements of the participating parties. The EV charging ecosystem consists of many players that exchange information: EVs, Charging Stations, Charging Station Operators, E-Mobility Service Providers and more. Every information interface between two players can use certificates to secure this information exchange: to authenticate the player at the other end and to encrypt and sign the data that is being exchanged. Many trust relations are established in this manner, between many different companies. All players will manage a number of certificates to authenticate themselves and others. When using ISO 15118, Contract Certificates are handed out by EMSPs and should be installed in an EV. With these Contract Certificates EV users can automatically start and stop charging sessions. Because the EMSP is not known when creating the EV in the factory, ISO 15118 provides a mechanism to install these certificates in the EV via the Charging Infrastructure.

Within the ISO 15118 standard number of technical measures are taken to reduce this complexity. In addition to that, the VDE application guide describes additional proposals concerning practical aspects on how ISO 15118 can be introduced in the EV market. This concerns for example using a central store for CSOs for getting contract certificates and handling the situation when contract certificates are stored at multiple locations be done in multiple ways. This is out of scope of the ISO 15118 standard, but is an important aspect that should also be addressed. Besides a mathematical validation of a “contract certificate”, it can be assumed that an additional validation is needed of the underlying contract that is represented by the certificate. This check can only be done at an EMSP, so existing channels between CSOs and EMSPs could be used here.

6 Design for a PKI system

A number of different designs for a PKI for using ISO 15118 within the EV market are possible, ranging from a system managed by a single party or a consortium of parties, to an open PKI that allows everybody in the EV market to participate in the PKI. The design determines what agreements must be made between market players.

Neutrality of the V2G Root Certificate Authority and access to certificate pools for all market players are key

elements in an open market. Additional measures regarding market processes will guarantee freedom of choice for the consumer of E-Mobility Service Provider and allow access to all charging infrastructure regardless of the brand of EV they drive. In this manner, all consumers can benefit from the opportunities ISO 15118 offers.

7 Conclusion

Consumers value choice and a seamless service. ISO 15118 provides secure, smart and easy charging. EV drivers should be able to benefit from the functionalities ISO 15118 offers, using any Service Provider of their choice, at any charging station that supports ISO 15118. This can be achieved with the open PKI design as described in this document.

A well-designed, open PKI can benefit all involved parties: EV users can have additional comfort by Plug and Charge authorization, all market players can join and EV charging is done in a secure way. More information becomes available for smart charging, offering customers lower prices, sustainable charging and making efficient use of the capacity of the electricity grid.

This document is intended to explain the design of a Public Key Infrastructure needed for ISO 15118 to all interested and affected parties. It presents a design with the aim that industry players and market authorities engage in a discussion on the way forward. In our vision on the way forward is an open PKI for ISO 15118 paving the way to create maximum benefit for the EV user and widespread adoption within the international EV charging markets.

Abbreviations

CPS	Certificate Provisioning Service
CS	Charging Station
CSMS	Charging Station Management System
CSO	Charging Station Operator
DSO	Distribution System Operator
EMAID	E-Mobility Account Identifier
eMIP	eMobility Inter-operation Protocol. Roaming protocol of Gireve
EMSP	E-Mobility Service Provider. Synonym for MO.
EV	Electric Vehicle
Intermediate Certificate	Certificate between the root certificate at the top of the certificate hierarchy and the leaf certificates.
ISO 15118	Protocol between Charging Station and EV which supports (among others) vehicle to grid communication for smart charging and plug and charge authentication.
Key store	A repository of leaf certificates, their associated private keys, and optionally intermediate sub-CA certificates; used for authentication and authorization at a given resource.

Leaf certificate	Any certificate that cannot be used to sign other certificates. For instance, TLS/SSL server and client certificates, email certificates, code signing certificates, and qualified certificates are all end-entity certificates. (
MO	Mobility Operator. Synonym for EMSP.
OCHP	Open Clearing House Protocol. Roaming protocol of e-clearing.net
OCPI	Open Charge Point Interface. Roaming protocol between EMSPs, CSOs and/or roaming platforms

Authors

Lonneke Driessen, director standardisation Open Charge Alliance

Baerte de Brey is the Chief International Officer within ElaadNL. ElaadNL is the knowledge and innovation centre in the field of (smart) charging infrastructure and is owned by the Dutch DSOs. Responsible for analyzing the long-term effect of electric mobility on the electricity grids, Baerte helps building a sustainable business case around this transition. This includes vehicle2grids, EV-storage and customer behavior research. He graduated from Leiden University in 2001 with a law degree and received a MBA from Nyenrode Business University in 2006. As an expert for the European Commission he sometimes reviews collective European programs concerning EV interoperability and smart charging. In his spare time he is a member of the Provincial Council of Utrecht.

Lonneke Driessen is director standardisation at the Open Charge Alliance. The Open Charge Alliance (OCA) is a global consortium of public and private electric vehicle (EV) infrastructure leaders that have come together to promote open standards in the EV-charging ecosystem. The Open Charge Alliance is currently responsibe for the specification development of OCPP (Open Charge Point Protocol) for back end to EVSE communication. Following the growing use of OCPP (through more investments, use in more countries and products developed by more companies) OCA will proceed by placing OCPP within an official Standards Development Organization (SDO). Lonneke has a master degree in electrical engineering at Delft University.