

Berlin, 7 December 2021

**BDEW, German Association
of Energy and
Water Industries**

Reinhardtstraße 32
10117 Berlin

www.bdew.de

Position Paper

Positions and open issues on working with the ISO 15118 communication standard for the Plug and Charge feature

The German Association of Energy and Water Industries (BDEW), Berlin, and its *Land* organisations represent over 1,900 companies. Its members range from local and municipal through regional and up to national and international businesses. It represents around 90 per cent of electricity production, over 60 per cent of local and district heating supply, 90 per cent of natural gas, over 90 per cent of the energy networks as well as 80 per cent of drinking water extraction and around a third of wastewater disposal in Germany.

Contents

1	Introduction.....	3
2	Positions and open issues regarding the individual steps when using Plug and Charge	3
3	Requirements for individual market roles and infrastructure components of a public key infrastructure (PKI) for ISO 15118	7
4	Glossary	10

1 Introduction

Automatic authentication upon connecting a charging cable to an electric vehicle is a convenience feature for the charging and paying process. In this way, customers no longer have to use an app or RFID card to start a charging session. As of today, however, an additional medium, usually an app, is required to search for charge points, display charging history, monitor the charging process, for price transparency and for ending the charging process. In future, this could also all be done via the vehicle.

There are currently various technical options that can be used to implement Plug and Charge. One option is the implementation of the ISO 15118 communication standard on the part of the vehicle and the charge point. Depending on the version, ISO 15118 can enable many features, including bi-directional charging, for example. The automatic authentication feature based on ISO 15118 is called Plug and Charge. Currently, the Plug and Charge feature is supported by version ISO 15118-2. Version -20 is being finalised and expected to be available on the market soon. It has to be noted that version -20 compared to version -2 contains a range of additional features as well as a number of innovations for the Plug and Charge feature (including the ability to store multiple contract certificates from e-mobility providers (EMP)). In 2020, Working Group 5 of the National Platform Future of Mobility (NPM) produced a [Roadmap](#) that provides an overview of all ISO 15118 features.

A second technical option for implementing Plug and Charge is AutoCharge that allows customers to automatically authenticate themselves. AutoCharge is already being used by charge point operators in Germany and the Netherlands. It provides a comparable level of convenience to the Plug and Charge process. It remains to be seen which technology will prevail as the most competitive one for automatic authentication.

As the ecosystem and market rules for a successful and fair implementation are more complex for Plug and Charge based on ISO 15118 than AutoCharge, this paper focuses on the ISO standard and the Public Key Infrastructure (PKI) necessary to implement Plug and Charge and other possible features. In addition to fundamental industry positions on safeguarding fair competition, we draw attention to unresolved issues which need to be clarified prior to any widespread adoption of the standard, in order to ensure the system runs smoothly, is fair and legally sustainable.

2 Positions and open issues regarding the individual steps when using Plug and Charge

Plug and Charge must be easy to use and the underlying processes must be as transparent as possible for customers. In order to ensure this, the responsibilities must be clearly assigned between the market participants at each step of the process. The central steps, associated requirements and open issues are set out below.

1



Installation of the e-Mobility providers' contract certificate into the vehicle

For customers to be able to use the Plug and Charge feature, a contract certificate from one or more e-Mobility providers must first be installed into the vehicle. In the interests of fair competition, the following conditions should be met:

- › The installation of the contract certificates via the vehicle (OEM telematics backend) must always be easy, fast and free of charge for customers. For this, customers must be able to easily obtain the unique identifier for their vehicle (provisioning certificate identifier, PCID) in order to initiate the installation. In addition, there is the option to install the contract certificate into the vehicle via the charge point. The retrieval of the contract certificates from a Plug and Charge Contract Certificate Pool (CCP - see glossary) by the vehicle manufacturer requires a standardised interface (API), that facilitates a uniform and secure process.
- › Customers must not be restricted to installing only contracts from pre-determined e-Mobility providers into their vehicles. It must be possible, at the customer's request, for one or more contracts to be installed into the vehicle at the time of purchase.
- › Following the introduction of ISO 15118-20, customers will be able to install more than one contract certificate into their vehicle. This will give customers greater freedom of choice. As a minimum, customers must be able to store at least five contract certificates in their vehicle for European roaming, irrespective of the root certificate authorities (see section 3 and glossary) established in Europe.
- › Currently, installing a contract certificate into a vehicle requires customers to use a two-factor authentication procedure to confirm to the e-Mobility provider that they wish a contract to be concluded with the corresponding vehicle. This process must be retained.

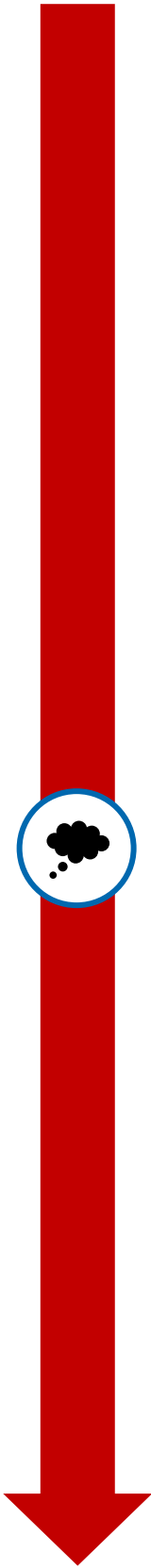
2



Display and selection of contract certificates or alternative means of authorisation

In the interests of customer transparency and of fair competition, clarification is needed on how customers' options will be displayed to them prior to each charging session. In this regard, the following conditions are key:

- › The vehicle manufacturer must be obliged to display the contract certificates stored in the vehicle either in the vehicle or in the OEM app for the vehicle. This means that the name of the e-Mobility provider or the relevant contract plan must be displayed in plain text rather than merely a technical presentation of the certificate number.

- 
- › The contract certificates must be displayed in a simple, overview format showing all installed contract certificates (with an option for customers to set their favourites).
 - › A further essential condition for Plug and Charge is price transparency. As there is currently no standardised approach for involving vehicle manufacturers in roaming processes, in order to allow pricing information of the e-Mobility providers to be displayed in the vehicle, the price must, for the time being, be displayed in the vehicle manufacturer's, e-mobility provider's or charge point operator's app.
 - › Customers need to be regularly informed by their vehicle manufacturer that different rates are available to them for the use of Plug and Charge, within their charging agreements, and that other means of authentication than Plug and Charge can be used. The idea is to ensure that customers make an informed decision about which rate they use. One conceivable solution would be for customers to be regularly informed, in their vehicle, as to which contract plan and rate applies to their current charging session and to be asked for confirmation accordingly. If customers do not wish to be reminded of their chosen rate and the available alternatives, they should be given the ability to deactivate this reminder function.

Open issues

- › A standardisation process is required in order to enable charging rates to be displayed in vehicles. This process must enable the vehicle manufacturer to be involved in the roaming processes. The necessary interfaces will require the close cooperation of all market participants, to ensure a trouble-free display of the information. This is of particular significance in light of the coming introduction of dynamic pricing.
- › In the interests of data protection and fair competition, vehicle manufacturers must not be allowed to access or share customer information on the use or frequency of use of an EMP product for Plug and Charge. This requires a standardised solution (e.g. separated roles of vehicle manufacturers and EMPs, or the creation of a "generic" EMP within the PKI which serves as a neutral intermediary).

3



Starting and stopping the charging session via Plug and Charge

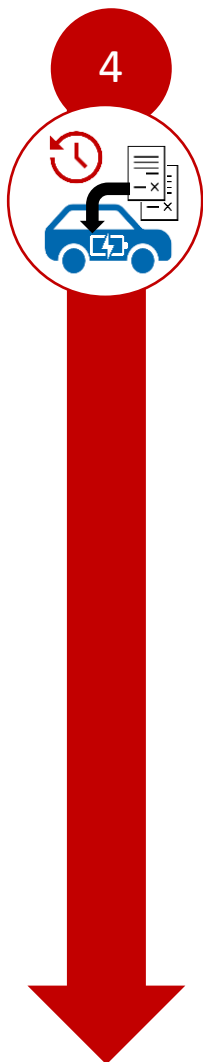
Providers will, in most cases, have to use existing methods (e.g. display in vehicle or app) for giving customers information about the status of the authentication process and the charging session as well as an easy way to stop the charging session. In the interests of customer transparency, the following must apply:

- › After the charging cable is plugged into the vehicle, customers should receive information as to whether the authentication process has either been successfully completed or terminated. This information should also be displayed in the vehicle.
- › If the authentication process fails due to a lack of a roaming connection between the e-Mobility provider and the charge point operator (CPO), an error message needs to be displayed in the vehicle, the vehicle manufacturer's app and, to the extent technically possible, in the app of the EMP used.
- › The display of information on the current charging session, the payment process and the charging history continues to be by currently available methods (app, vehicle, charge point).
- › To stop the charging session, customers will continue to use a confirmation either in the vehicle or via the EMP's app. For customers who have an RFID card with the same E-Mobility Account Identifier (EMAID) as the one stored in the contract certificate used, the charging session can also be ended using the RFID card.

Open issues

- › A standardisation process is needed for displaying error messages if the communication between vehicle and charge point fails. The cause of the failed communication should be communicated to the customer. Moreover, error messages need to be displayed regardless of whether Plug and Charge or any other authentication means is used (e.g. app or RFID card).





Post-sale installation and deletion of contract certificates

To enable customers to change contract certificates or add new ones at any time, it is important to establish a simple and intuitive process. The following points need to be taken into account in the interests of fair competition:

- › The process for installing certificates via the vehicle (OEM telematics backend) at a later date, just like the process for installing the first certificate, must always be simple, fast and free of charge for customers. Customers must be able to change the certificates themselves via the manufacturer, CPO or EMP without having to visit a car workshop. For this, customers must be able to easily obtain the unique identifier for their vehicle (provisioning certificate identifier, PCID) in order to initiate the change. As mentioned in step 1, a standardised interface (API) is also needed in step 4 to facilitate a uniform and secure process for the retrieval of the contract certificates from a Plug and Charge Contract Certificate Pool (CCP) by the vehicle manufacturer.
- › It must be possible for customers to easily and quickly delete contract certificates in the vehicle or in the vehicle manufacturer's app. Every vehicle manufacturer must make sure this is the case for their customers.
- › Any permanent cancellation of the connection between the contract certificate and the vehicle, e.g. if the vehicle is resold, must be carried out through the EMP. The EMP must cancel the connection between the EMAID and the PCID, and completely delete and revoke the contract certificate.

3 Requirements for individual market roles and infrastructure components of a public key infrastructure (PKI) for ISO 15118

In order to use Plug and Charge on the basis of ISO 15118, and also to be able to use additional ISO 15118 features in the future, a public key infrastructure is needed which issues and signs the required certificates in a non-discriminatory manner and thus ensures that the parties involved are trustworthy and the communication between them secure. To this end, certain requirements must be met by the different market roles. These include:

Vehicle-to-Grid Root Certification Authority (V2G Root CA)

- › It is to be expected that there will be several V2G roots for the creation of the PKI. Interoperability between these roots, e.g. via trust lists or cross certification (see glossary), will be key to maintain customer convenience.

- Trust lists:
 - Any use of a trust list requires a trust list owner who meets certain security requirements. Vehicle-to-Grid Root Certification Authorities (V2G Root CAs) can only be accepted onto the trust list if they also meet these security standards.
 - The trust list owner must be a neutral body that, for example, is set up by the EU Commission.
- › A V2G root CA has to act as a trustworthy institution for all CPOs and all certificates of the Certification Provisioning Services (CPS) as well as, optionally, for the certificates of the EMPs and the vehicle manufacturers.
- › V2G root CAs issue certificates to all market participants under the same security conditions for the certificates and the corresponding attributes.
- › In light of the key importance of the root CAs, they need to be subject to quality audits performed by an independent entity. Which ISO standards will govern these audits has yet to be decided.

Vehicle manufacturer (OEM)

- › All vehicle manufacturers have to install all V2G root CA certificates into the vehicles (at the factory or over-the-air).
- › For version ISO 15118-20: All OEM roots have to be added to the existing pools which are accessible by the other market participants.
- › One or more contract certificates can, upon the customer's express request, be pre-installed into the vehicle at the time of delivery or purchase, provided the customer is presented with and informed about alternative EMP options.
- › The Plug and Charge feature should be free of charge for customers of new vehicles and must be available, on a non-discriminatory basis, for all EMP contracts.
- › It must be possible for vehicle users to remove certificates and install new ones quickly, easily and free of charge.

E-Mobility Providers (EMP)

- › EMPs give the certificates, in a bundle, to a Certification Provisioning Service (CPS).
- › All EMP contract certificates have to be signed by a CPS certificate.
- › The CPS certificate is derived from a V2G root CA and is therefore trustworthy and secure.
- › All EMPs must have access to a CPS.
- › The CPS signs the certificates and makes them available in the Contract Certificate Pool.

Charge Point Operator (CPO)

- › All regionally relevant EMP roots and V2G root CA certificates should be installed either into the charge point or made available to the charge point via a charging station management system. This could be achieved by, for example, the CPO having access to the root certificate pools.

OEM Provisioning Certificate Pool (PCP) and Governance of the Certificate Pools

- › OEM Provisioning Certificate Pool (PCP):
 - Each vehicle manufacturer has to choose a PCP with which to store its OEM provisioning certificate.
 - If there is more than one PCP, all EMPs must have access to the directory service for OEM provisioning certificate pools.
- › Governance:
 - Governance is essential to ensure that all CPOs have access to all contract certificate pools and all EMPs have access to all OEM provisioning certificate pools. If more than one pool exists, all parties need to have access to a directory service.
 - A process will have to be established which facilitates the revocation of an existing EMP contract.

4 Glossary

Term	Meaning
Certification Provisioning Service (CPS)	Service which receives the contract data, including a contract certificate, from an EMP, signs it and makes it available to CPOs and/or OEMs.
Charge Point Operator (CPO)	The operator of a charge point.
Contract Certificate	A certificate issued by an EMP to a user and signed by the CPS which is necessary for authentication and authorisation purposes prior to starting a charging session.
Contract Certificate Pool (CCP)	Pool which stores all EMP contract certificates and makes them available to the other market participants.
Cross Certification	This is when two V2G root CAs mutually certify one another and by doing so also accept the authentication data from users of the other root CA.
E-Mobility Account Identifier (EMAID)	E-Mobility provider's unique identifier for their customers, required for authentication and billing purposes.
E-Mobility Provider (EMP)	Provider that offers e-mobility charging services to drivers of electric cars such as access to charge points in their network, payment and billing, navigation.
Original Equipment Manufacturer (OEM)	Vehicle manufacturer.
OEM Provisioning Certificate	Digital certificate, issued by the OEM root CA, which is unique to each vehicle and can thus identify that vehicle.
OEM Provisioning Certificate Pool (PCP)	Pool which stores all OEM provisioning certificates and makes them available to the other market participants.
OEM Root Certification Authority (OEM root CA)	The OEM root CA issues the OEM provisioning certificates which are unique to each vehicle.
Provisioning Certificate Identifier (PCID)	Unique identifier for the individual vehicle, which is needed, for example, to connect with the contract certificate of an e-Mobility provider.

Public Key Infrastructure (PKI)	Hierarchical structure of trusted organisations (CAs and sub-CAs) for handling certificates which enables secure communication between vehicle and charge point.
Root Certificate Pools	Pools which store all EMP roots and V2G root CA certificates and make them available to the other market participants.
Subordinate Certificate Authority (Sub-CA)	CAs which rank below a root CA in the hierarchy and whose certificates are signed by the root CA. There must be a minimum of one and maximum of two sub-CAs for each role or PKI branch (CPO, EMP and OEM).
Trust List	The trust list contains all trusted and authenticated V2G roots and guarantees the interoperability of the different V2G root CAs.
Trust List Owner	The trust list owner is a neutral body tasked with managing the trust list.
Vehicle-to-Grid Root Certification Authority (V2G Root CA)	Highest level CA within the PKI hierarchy which must be neutral and trusted by all market participants. There can be more than one root CA in a market. In that case, they must trust one another. For this, there are two options: using “trust lists” or “cross certificates”. The V2G root signs the certificates of all sub-CAs of the various market roles.

Contact person:

Amelie Thürmer
Unit Manager
Charging infrastructure
Energy Networks, Regulation and Mobility Division
Amelie.thuermer@bdew.de
Telephone: +49 (0)30 300199-1119

