Exploring the Public Key Infrastructure for ISO 15118 in the EV charging ecosystem

Technical Report · November 2018

CITATION
1

READS
3,893

2 authors, including:

Paul Klapwijk
Delft University of Technology
6 PUBLICATIONS **30** CITATIONS

SEE PROFILE

EXPLORING THE

PUBLIC KEY INFRASTRUCTURE

FOR

ISO 15118

IN THE

EV CHARGING ECOSYSTEM

Elaad nl

EXPLORING THE

PUBLIC KEY INFRASTRUCTURE

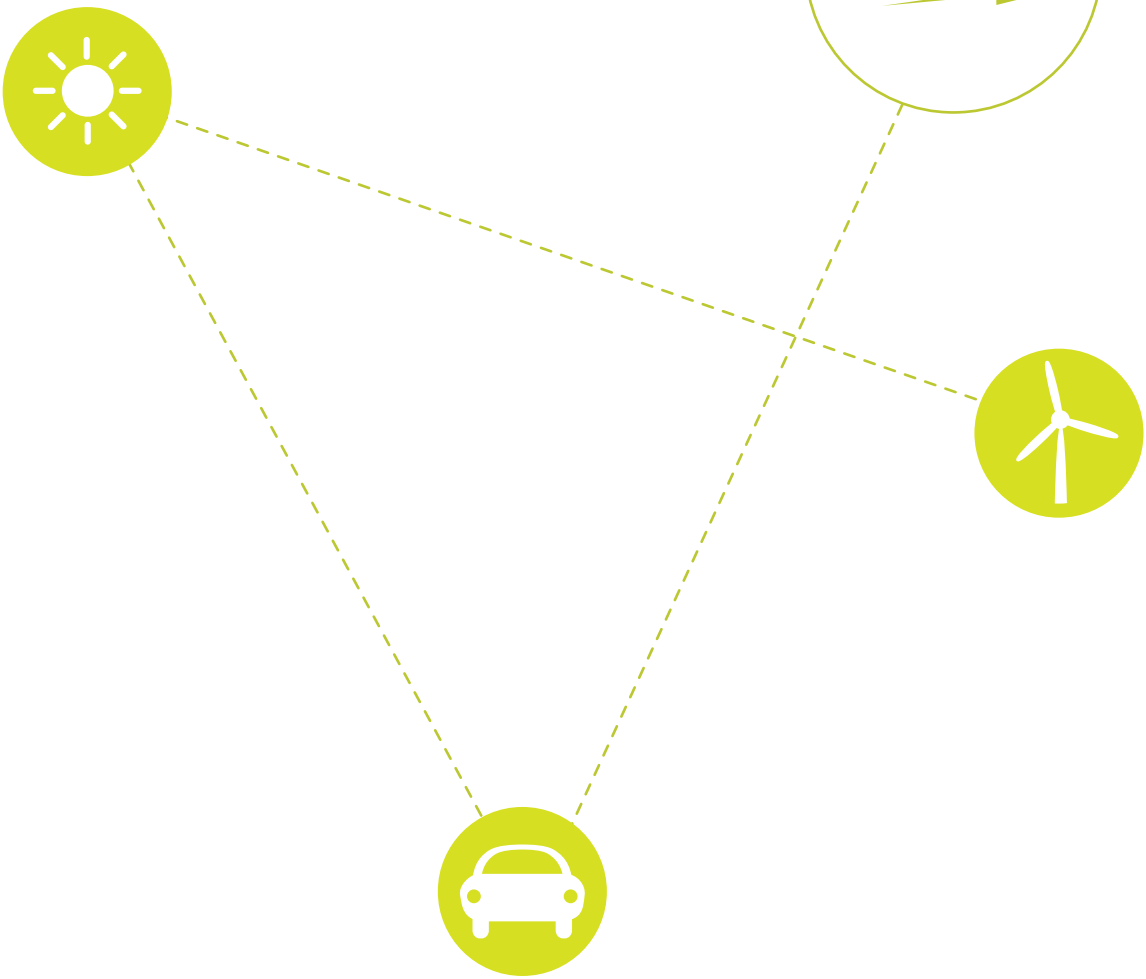
FOR

ISO 15118

IN THE

EV CHARGING ECOSYSTEM

Elaadnl



COLOPHON

This report is published as part of the
GLOBAL EV CHARGING TEST
On the 15th and 16th of October 2018
in Arnhem, The Netherlands

Publication

Title:	Exploring the public key infrastructure for ISO 15118 in the EV charging ecosystem
Publisher:	ElaadNL, Arnhem, The Netherlands
Date:	November 2018
Version:	1.0

Editorial team

Business analysis, technical analysis
Paul Klapwijk & Lonneke Driessen-Mutters
Reviewed by Dr. Marc Mültin

Design

Content analysis & visualization
Marcel Nahapiet • nahapiet.com

Contact

Utrechtseweg 310 B42
6812 AR Arnhem, The Netherlands
+31(0)26 31 20 223

info@elaad.nl
TW @ElaadNL
www.elaad.nl

CONTENT

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

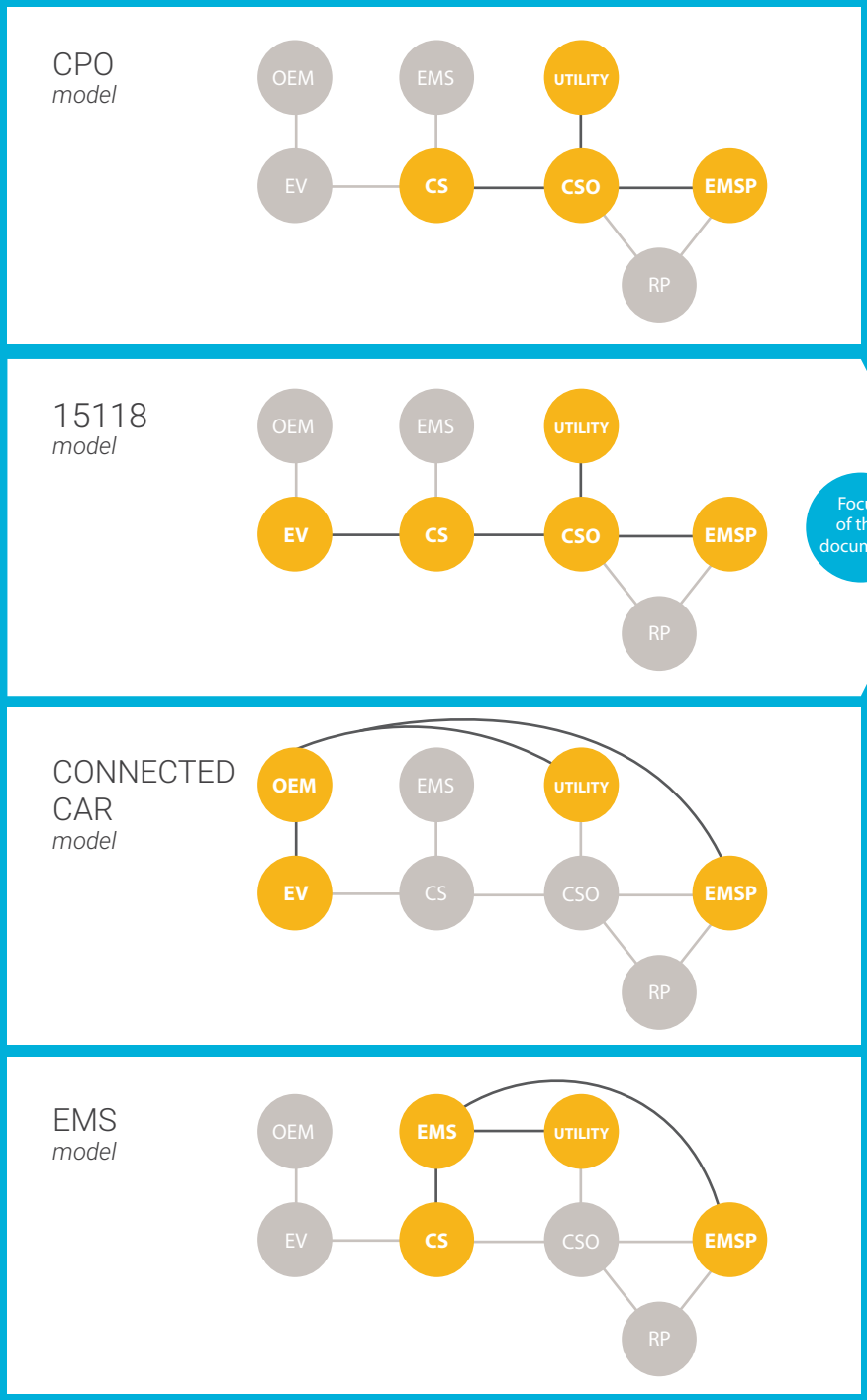


FIGURE 1: *Overview of information exchange options*

1. INTRODUCTION

ElaadNL is the knowledge and innovation centre in the field of smart charging infrastructure in the Netherlands. ElaadNL is a partnership of the Dutch grid operators who manage the Dutch electricity and gas networks. Through their mutual involvement in ElaadNL, the Dutch grid operators prepare for a future with electric mobility and renewable energy sources.

The growth of both electric driving and renewable energy sources have significant impact on the electricity grid. ElaadNL researches and tests together with partners the possibilities of Smart Charging, to ensure that the network can support these exciting developments whilst remaining reliable and affordable.

1.1. 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. It is the mission of ElaadNL to make sure that in the future everyone can smart charge.

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.

1.2. OPEN MARKETS FOR EV CHARGING

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.

1.3. INTRODUCTION TO ISO 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.

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.

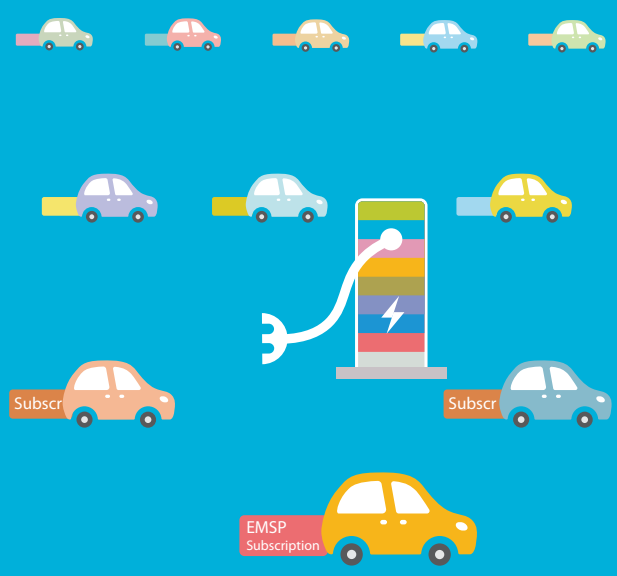
3. Smart Charging. This includes a number of use cases such as schedule-based charging and - in future versions - reactive power compensation and vehicle to grid charging. Currently the main feature of the standard from a Smart Charging perspective is that this protocol can communicate the mobility needs 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.

1.4. PURPOSE

The purpose of this document is twofold. Firstly it provides information on how an EV charging system including ISO 15118 works from a technical point of view. The report shows how ISO 15118 fits into the EV charging ecosystem and explains the rationale behind design choices. Knowing the rationale behind some of the (technical) decisions could strengthen trust in the standard and help market adoption. Secondly it provides information on what still needs to be done regarding the Public Key Infrastructure (PKI) needed to operate ISO 15118 and make the standard a widespread success in an open market.



"Information on how an EV charging system including ISO 15118 **works from a technical** point of view."

1.5. REPORT STRUCTURE

1

Chapter 1
Gives a general introduction to this document.

Chapter 2
Presents a general explanation of a public key infrastructure

2

Chapter 3
Illustrates the use of certificates in the EV charging eco-system

Chapter 4
Addresses solutions that are / could be implemented to reduce complexity and make a PKI workable in an open, multi actor EV charging ecosystem

3

Chapter 5
Discusses the PKI designed as a single party system, a consortium or an open system

Chapter 6
Describes a design for an open PKI

4

Chapter 7
Presents the key takeaways

"Information on **what still needs to be done** regarding the Public Key Infrastructure - (PKI) - needed to operate ISO 15118 and make the standard a widespread success."

CHAPTER 2 IN A NUTSHELL

A Public Key Infrastructure (PKI) is a system 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.

2. GENERAL EXPLANATION OF A PUBLIC KEY INFRASTRUCTURE

2.1. INTRODUCTION TO A PUBLIC KEY INFRASTRUCTURE (PKI)

A Public Key Infrastructure is a collection of hardware, software, personnel and operating procedures that issues and manages digital certificates that are used for securing digital communication. These certificates link public keys to people or systems. The public keys can be used to verify digital signatures that were created with their associated private keys, for authentication and for encrypting data communication.

Certificates are issued by a trusted authority called Certification Authority (CA). The certificate contains information on the owner of a specific public key, until when that key is valid, which CA issued and signed the certificate, and the digital signature of that

CA. If the digital signature is incorrect or if the expiry date has passed, the certificate is considered invalid.

The most common use of certificates consists of two unique and very long chains of characters, called keys. One of these keys is kept secret by the owner of the certificate and is called the "private key". The other keyword is publicly shared and is called the "public key". The two keywords are mathematically linked. This mathematical relation means that when a message is encrypted by the owner of the certificate with the private key, it can only be decoded with the public key and vice versa. In this way, the recipient of a message encoded with the private key can use the public key to decrypt the message and check that the message originated from the owner of the certificate.

It is important that the validity of the public certificate can be checked, and for this purpose the certificate has a digital signature that is created with the private key of the Certification Authority. By (mathematically) verifying it with the public key of the Certification Authority, anyone can check whether the public key is valid.

By using these keys and certificates, the following security functions can be performed:

- **Encryption** – As described above, certificates provide the capability to encrypt data that can only be decrypted by someone in possession of the private key. To send someone encrypted data, you can obtain their public key and encrypt the data with their public key. The receiver can then decrypt the message with their private key.

- **Digital Signatures** – A digital signature can provide assurance that a piece of data such as a document, executable, or script came from a specific source and has not been tampered with since it came from that source. As described above, this mechanism is also used for verifying certificates themselves.

- **Authentication** – PKI provides a solid method for authenticating and identifying users or systems. By asking a user or system to perform a digital signature operation with their private key, they provide assurance that the entity presenting you with the certificate has possession of the matching private key. This proves that they are who they are asserting to be.

Use of a PKI requires a clear definition of the roles and the functions in the ecosystem. Each actor in the ecosystem will have the option to create and manage its certificates.

2.2. CERTIFICATE SIGNING

Secure communication between organizations is achieved if they share their public certificates and trust each other's certificates. However, when creating a trust relation by principle it cannot be the case that one of the 2 participating parties creates and distributes the certificates. To ensure a trust relation between certificates of different organisations, a neutral / central third party should be recognized by all the participants in the ecosystem as a trusted party.

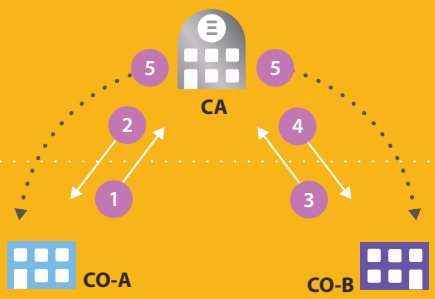
When using such a trusted party in an "ecosystem", the public key of the certificate generated by each of the different organisations should be signed by this party, a Certificate Authority, as already mentioned in the introduction. A number of parties in the world are recognized (and thus trusted) as certificate authorities (CA's), such as VeriSign, Digicert, Thawte etc. The public keys of these organisations can be used to verify certif-

Issuing certificates

2 4
Issues certificate and signs it with **private key of CA**

Send certificate signing request with **public key**

1 3



5
Acquire **public CA certificate** (e.g. download from website)

Setting up the connection

6
Send signed public cert. **CO-A** for setting up connection

Verify signature of public cert. **CO-A** using public **CA** certificate
7

Verify signature of public cert. **CO-B** using public **CA** certificate
9

Send signed public cert. **CO-B** for setting up connection
8

Sending encrypted data

10
Send data encrypted using **public key B**

Decrypt data using **private key B**
11

13
Decrypt data using **private key A**

Respond with data encrypted using **public key A**
12

Signed certificate of CO-A

Signed certificate of trusted CA

Issues certificates

Public key

Signed certificate of CO-B

Uses certificates

Private key

icates that are signed by these CA's and are therefore, for example, included in internet browsers. Your PC uses them to set up a secure connection to for example your bank. **Figure-2** illustrates the Certificate Authority signing certificates from different organisations.

FIGURE 2:

A (neutral) Certificate Authority signs certificates of different parties.

When doing a technical handshake (step 6-12), the chain of public certificates (see 2.3) is often exchanged automatically. Of course, to be sure that the certificate chain can be trusted, the certificate at the top of the chain should be a "known" certificate, i.e. known to a browser or system as a trusted root certificate. These "known" certificates are usually stored in a "trust store", whereas private keys are usually stored in "key stores".

2.3. CERTIFICATE HIERARCHY

Signing of certificates can be done in a "hierarchy" consisting of more than one certificate used for signing (see **figure -3**). When viewing a certificate chain as a "tree", it starts growing at the root, attached are the branches and at the end are the leaves. The levels of hierarchy in a certificate chain are:

- **Root certificate** – the certificate of the root Certificate Authority (CA).
- **Intermediate certificate** – the certificate of an intermediary or subordinated Certificate Authority (SubCA), located between a root certificate and a leaf certificate. Reasons for introducing a SubCA layer are: "grouping" certificates e.g. by type, letting a delegate party issue certificates and reducing the risk of compromising the root certificate (i.e. this can be stored securely / offline when SubCA's are used for issuing leaf certificates).
- **Leaf certificate** – a term often used for a certificate of an individual organisation or entity. In certificate hierarchy, this is the end certificate. It's associated private key is, therefore, not used to sign other certificates.

Any organisation may choose to issue their own certificates for different machines, systems, and individuals in their organization. As such, it can act as a "delegate party", for example for avoiding the costs of requesting many separate certificates from a (commercial) Certificate Authority. In order to make sure the certificates they issue are trusted outside their own organisation, they have a recognized CA issue and sign their

SubCA certificate. That SubCA certificate can then be used to verify the signatures of certificates they issue themselves. This way, other parties can first check whether the certificate they receive is indeed signed by this SubCA and can then check the validity of the SubCA by checking whether the SubCA certificate was correctly signed by a known / trusted root CA. This chain of sub certification can be extended to multiple levels.

This is illustrated in **figure-3**. The certificate of organisation A (CO-A) is signed with the private key of a "SubCA α", whose certificate in turn is signed by the higher-level "CA". In this case, to validate the certificate of organisation A, the entire "chain of certificates" above it is required for validation.

In principle there is no limit to the number of sub-levels in a Certificate hierarchy. However, having additional certificates in a chain requires either storing more trusted intermediate certificates or exchanging more certificates during the handshake. Furthermore, every intermediate certificate in the certificate chain might have its own accompanying list of revoked certificates (see next section for more explanation). Since checking these lists could be part of the validation process, this might lead to complex (and possibly slow) validations.

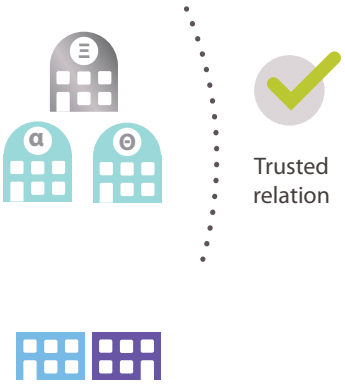


FIGURE 3:

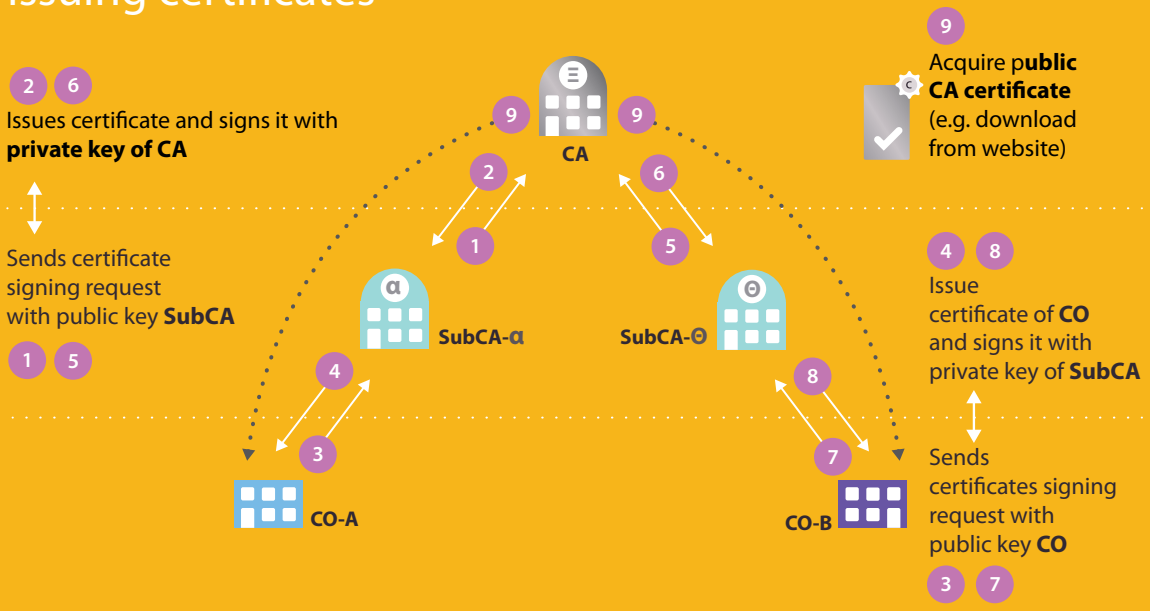
A (neutral) Certificate Authority signs certificates of different parties via SubCA's.

A copy of the public CA certificate should be available at the system where the validation takes place.

Validation of the public SubCA Θ certificate can be verified by checking the signature of the SubCA Θ certificate with the public CA certificate.

Validity of certificate of organization B can be verified by checking the signature with the public SubCA Θ certificate.

Issuing certificates



When certificates have been issued, all actors have the necessary tools for the normal operations of setting up connections and exchanging data.

CO-A has

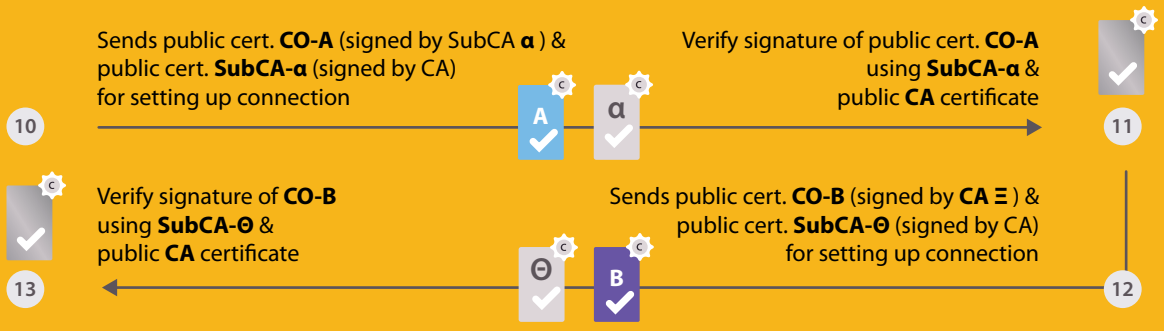
CO-B has

A **signed public certificate** specific for **their organization**, that can be used for setting up connections and exchange data.

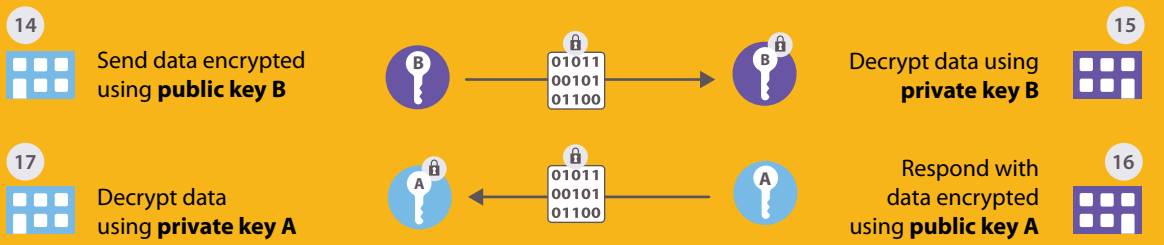
Signed SubCA certificates, that can be used to verify the signature of the public leaf certificates.

The public certificate of the **trusted root CA** that has been acquired separately from the CA (e.g. downloaded from the CA website). This can be used to verify the signature of the SubCA certificates.

Setting up the connection



Sending encrypted data



Signed certificate of CO-A

Signed certificate of CO-B

Signed certificate of trusted CA

Signed certificate of SubCA-α

Signed certificate of SubCA-Θ

Public key

Private key

Issues certificates

Uses certificates

2.4. CERTIFICATE VALIDITY CHECKING

Checking the validity of a certificate entails several steps:

- **Checking** whether the **current time** is between the "from and to" validity date in the certificate
- **Verifying** that a certificate is indeed from a **trusted party** (and not a "fake" copy), based on the signatures of the certificates from the top of the chain (root certificate) to the lowest certificate in the chain (leaf certificate). This can be done either by:
  - **Storing** the **public certificate** of the root CA **and all underlying Sub-CA's** in a trust store and validate the leaf certificate with these stored certificates or
  - **Storing only** the **public certificate of the root CA** and exchanging the leaf certificate and public SubCA certificates during the handshake.
- Checking if the certificate has been **revoked** (see 2.5)

2.5. CERTIFICATE REVOCATION

When for some reason a CA can no longer be trusted, its public key is removed from all lists of trusted certificates (worldwide). Websites / organisations using a certificate signed / issued by that CA are no longer trusted. In the case of internet browsers, this means that a certificate is then removed from all internet browsers and when visiting a webpage that uses a certificate that is no longer trusted, the user gets a security error. This only occurs when the private key of a certificate authority is compromised. When the certificate of an individual organisation that was signed by a CA is compromised and is no longer considered a trusted certificate, it is "revoked". For example, a reason for this could be that the associated private key of an organisation is "stolen".

Revoking a leaf certificate does not have an impact on the CA certificate. For this pur-

pose, an online Certificate Revocation List (CRL) of "revoked" certificates is available per CA. These lists are checked online when validating certificates, to ensure that a certificate that is technically and mathematically valid, has not been revoked. For example, when a contract is not paid for, the corresponding certificate that is linked to that contract can be revoked.

If private key of CA is compromised, all underlying certficates (i.e. issued and signed with private key of this CA) are also no longer trusted

If private key of CO-B is compromised, certificate is added to certificate revocation (CRL) list of CA

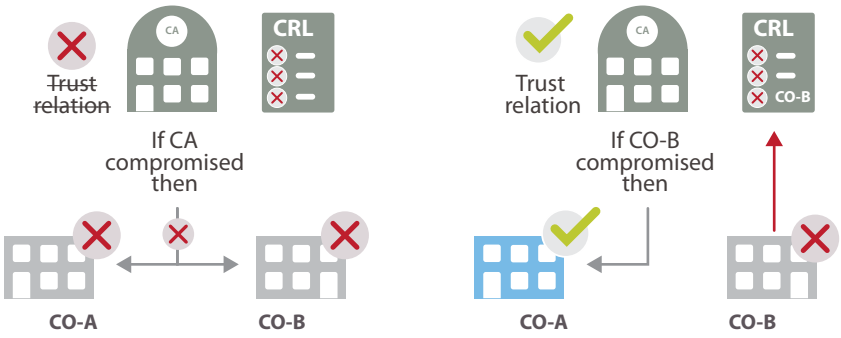


FIGURE 4: *Compromised CA certificate (l) vs. certificate revocation (r)*

As shown in **figure-4**, when a private key belonging to a certificate is compromised it will be added to the CRL of the CA who issued the certificate. The impact of a leaf certificate being compromised is therefore limited to the fact that the certificate is then considered invalid from that point onwards. However, if a (CA or intermediate) certificate higher in the chain is compromised, all certificates "below" it in the certificate hierarchy are not considered valid anymore. In that case, each certificate that is no longer trusted should be replaced. It could be decided to accept the certificates for a short time, this depends on an estimated risk (i.e. chance of hacking / misuse and cost impact). The impact of this can be quite large. If certificates are installed in remote devices, for example

EVs or charging stations, it could, depending on the PKI, have an impact on all charging stations or EVs within a certain area. If replacing certificates is not possible remotely, it could even mean that each device, e.g. each EV, is recalled to the garage to replace its certificate.

The CRLs that are mentioned above, are files that are made available by certificate authorities, which can be accessed online. For each certificate authority multiple CRLs could be available, commonly one for the Root CA and one per SubCA. The location of the CRL is often part of the certificate, for example: http://crl.entrust.net/g2ca.crl. If for example the chain of certificates contains 3 intermediate levels, this would mean that for the verification of each certificate, the 3 URLs of these CRLs should be retrieved from the certificates, the most recent version of these lists should be downloaded and checked before the certificate can be verified. This approach is time consuming. One way to reduce this time is caching CRLs, but this means that the verification might be done with "outdated" lists.

An alternative way of checking a certificate is via a dedicated central server from which the status of a certificate can be requested. A synchronous, HTTP based standard can be used for this, the Online Certificate Status Protocol (OCSP). The response from an OCSP responder is signed, which means that it can be verified that the response is indeed from a trusted OCSP responder. The status that is reported back by the OCSP responder should (of course) also be based on data that is maintained by the responsible CAs. This dedicated central server abstracts away the downloading and checking of different lists.

CHAPTER 3 IN A NUTSHELL

A number of choices must be made when setting up a PKI to enable secure communication for a new market or ecosystem. These decisions must 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. It is a complex system that is explained in more detail in this chapter.

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.

3. THE USE OF CERTIFICATES IN THE MULTI-PLAYER EV CHARGING ECOSYSTEM

The EV charging ecosystem consists of many different roles that exchange information. **Figure-5** shows these roles and the communication protocols used for information exchange that are considered in this document.

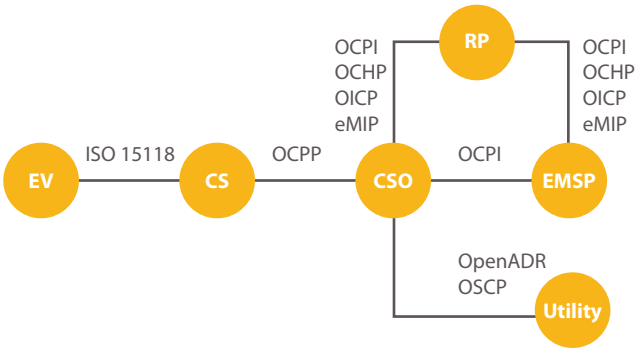


FIGURE 5:

Overview of protocols and roles

This selection of roles and protocols is based on the practical market experience (primarily in Europe) that ElaadNL has accumulated over the past years, the protocols that it has encountered in the EV market and pilot projects that have been executed by ElaadNL and partners. For more information about these protocols please refer to the ElaadNL standard publication 'EV related protocol study' (see appendix).

The next paragraph provides an overview of the protocols from **figure-5** and whether certificates are used and if so, the reason why certificates are used. When looking at this table, you can see that most protocols utilise certificates for authentication, initializing an encrypted connection and for verifying signed messages.

3.1. APPLICATION OF CERTIFICATES IN EV PROTOCOLS

Certificates are currently used for a number of protocols listed in the previous paragraph and preparations are made for future use, e.g. for ISO 15118 Charging Stations. In **table 1**, for each protocol, the reason(s) for using certificates are listed. Each protocol uses certificates to setup the TLS connection, i.e. for encryption purposes. For some protocols, identification, signing and authorization are also reason to use certificates. This choice depends on the developers of the protocols and their risk analysis, industry requirements, and specific market related requirements (e.g. "Eichrecht" in Germany).

The table above only shows the use of certificates for sending messages via the different protocols. However, more certificates are in use than this table might suggest, such as the certificate that the OCSP responder uses or the certificates that are included in an EV in the factory ("OEM certificates"). In the remainder of this chapter these will be explained.

TABLE 1: *overview of certificate use for protocols including application:*
A = Authorization
E = Encryption
S = Signing

PROTOCOL	REASON FOR USING CERTIFICATES	APPLICATIONS		
		S	A	E
ISO 15118	TLS connection between Charging Station and EV (ISO 15118)		●	●
	Verifying the signature of energy metering values	●		
	Authenticating of EVs with their Contract Certificate	●	●	
	Installation of Contract Certificates into EVs (Provisioning)	●	●	●
OCPP 2.0	TLS connection between Charging Station and CSMS			●
	TLS connection between Charging Station and EV (ISO 15118)			●
	Signing metering data	●		
	Authenticating Charging Station and CSMS		●	
OCPI	TLS connection between CSMS and EMSP system			●
	TLS connection between CSMS and Roaming Platform			●
	TLS connection between EMSP system and Roaming Platform			●
OCHP	TLS connection between CSMS and Roaming Platform			●
	TLS connection between EMSP system and Roaming Platform			●
OCHP direct	TLS connection between CSMS and EMSP system			●
OICP	TLS connection between CSMS and Roaming Platform			●
	TLS connection between EMSP system and Roaming Platform			●
	Identification / authorization of EMSP (based on client certificate)		●	
	Identification / authorization of CSO (based on client certificate)		●	
eMIP	TLS connection between CSMS and Roaming Platform			●
	TLS connection between EMSP system and Roaming Platform			●
	Identification / authorization of EMSP (based on client certificate)		●	
	Identification / authorization of CSO (based on client certificate)		●	
OSCP	TLS connection between CSMS and DSO system			●
OpenADR	TLS connection between CSMS and DSO system		●	●
	Message signing using XML signatures	●		

3.2. NUMBER OF TRUST RELATIONS AND CERTIFICATES IN THE EV CHARGING ECOSYSTEM

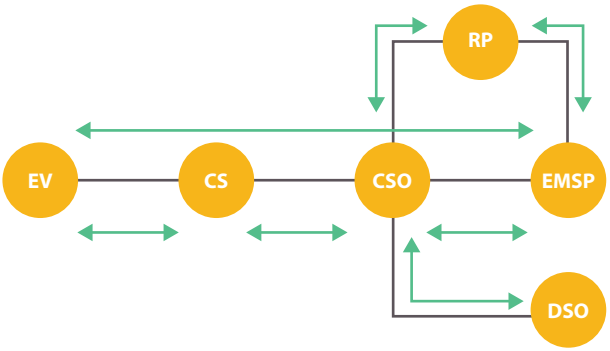


FIGURE 6: *Trust relations between actors.*

In the coming decade, the number of participants in the global EV Charging ecosystem will increase significantly. Many governments and companies (in the Netherlands, California, Norway etc.) have set targets for the number of EVs on the road and charging stations in the field in the coming years. Below is a very rough estimate of the numbers in the EV ecosystem by 2030:

- Number of **EVs** globally could be in the order of magnitude of 100.000.000s
- Number of **Charging Stations** could be in the order of magnitude of 10.000.000s
- Number of **Charging Station Operators** could be in the order of magnitude of 100s
- Number of E-Mobility Service Providers could be in the order of magnitude of 100s
- Number of **OEMs** could be in the order of magnitude of dozens
- Number of **Roaming Platform** could be in the order of dozens

- Number of **Utilities** and DSOs is in the order of 1000s

This also means than the absolute number of certificates used to establish trust relations increases significantly.

3.2.1 LIMITATIONS REGARDING THE NUMBER OF CERTIFICATES THAT CAN BE HANDLED

As the following paragraph will explain, many different certificates are involved, from installation of the Charging Station to starting a charging session. If all parties were to issue their own certificates, it will have several consequences:

- An EV should store **certificates of all CSOs and EMSPs**, which theoretically (when not using known CAs, but acting as CAs themselves) could become hundreds or even a few thousand certificates.

- A **Charging Station** should store certificates of all EMSPs (again theoretically: hundreds or even a thousand certificates) in its trust store for enabling validating contract certificates locally / offline certificate validations.

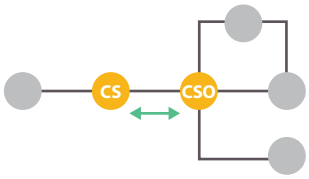
- **Validating** certificates could take a **long time** due to the different CRLs or OSCP checks.

Device memory, processing capacity and communication bandwidth for an EV and charging station are limited. Using too many root certificates will be memory intensive, whereas sending larger messages can decrease customer experience (e.g. waiting a long time when starting a charging session) and increase data costs from Charging Station to back office.

A PKI design for the EV charging ecosystem should take these limitations into account. Therefore, in order to let ISO 15118 work, a number of simplifications are introduced in the standard. These simplifications will be further discussed in Chapter 4.

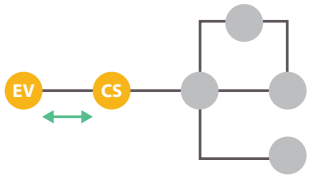
In the following paragraphs the main focus will be on the trusted relations that have to be established between the Charging Station and the CSO, between the EV and the Charging Station, and between the EV and the EMSP.

3.2.2 THE USE OF CERTIFICATES BETWEEN CHARGING STATION AND THE CSO



The CSO and the CS use certificates to allow the creation of a secure communication channel between the CSO and Charging Station. The integrity and confidentiality of messages on this channel should be protected with strong cryptographic measures to protect authorization information and to avoid any energy loss due to hacking. Besides this, it is used to provide mutual authentication between the Charging Station and the CSO and provide a secure firmware update process (i.e. check the source and integrity of firmware).

3.2.3 THE USE OF CERTIFICATES BETWEEN EV AND CHARGING STATION

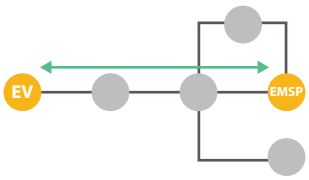


The EV and the Charging Station use certificates to setup a secure connection, to encrypt the data transferred and for signing authentication data. The EV should have a CA certificate in its trust store, that is used to setup a trust relation with a Charging Station. In ISO 15118 this certificate is referred to as V2G Root CA certificate. The EV can request "proof" of validity of (SubCA) certificates from an OCSP responder.

When an EV is plugged in for the first time, a connection is established for which only the unique factory installed OEM provisioning certificate from the EV can be used. To be able to trust this OEM provisioning certificate, the complete chain of OEM CA certificates (root CA and possible SubCAs) of the OEM should be known by the Charging Station. However, this validation of the EV (client) is not required from ISO 15118, so a Charging Station should accept any EV. If a Charging Station would like to do this validation outside of the official ISO 15118 standard, this could be achieved by using a private key belonging to a public key that is derived from the V2G Root CA certificate (explained later), to sign the OEM certificate (due to the certificate hierarchy that is imposed by ISO 15118, which is explained later, see 4.1.2) or by adding the OEM CA certificate of each OEM to the trust store of the Charging Station.

The EV always checks the certificate of the Charging Station. When using ISO 15118, the EV uses the Charging Station to communicate to "the grid". This means that when first connecting, the EV has to trust on something that is already in the EV. This can be achieved by adding the Charging Station CA certificate to the trust store of the EV when it leaves the factory. Due to the certificate hierarchy that is imposed by ISO 15118 (which is explained later) this should be the V2G Root CA but in principle this could also be another CSO CA certificate.

3.2.4 THE USE OF CERTIFICATES BETWEEN EV AND EMSP



An EV driver can sign up at an EMSP. In order to use its services, a Contract Certificate should be installed in the EV, so that the EV can authenticate itself at Charging Stations, can sign the data exchange from the EV to the EMSP ("MeteringReceipt") and can verify the data exchange from the EMSP to the EV ("SalesTariff").

In the case of ISO 15118, the trust relation between the EV and the EMSP is not straightforward, since the private key of the Contract Certificate needs to pass through several systems before it gets securely stored inside the EV.

3.3. INSTALLATION PROCEDURE OF A CONTRACT CERTIFICATE IN AN EV

The Plug-and-Charge functionality that is introduced with the ISO 15118 standard, requires an EMSP to create a Contract Certificate for a certain EV user and install it in that user's EV. Since the EMSP is not known at the moment of manufacturing the EV, this needs to be installed later.

The ISO 15118 standard includes methods to install the Contract Certificate in the EV using the communication channels over the charging infrastructure that are already in place.

There are two important considerations to take into account with the installation of a Contract Certificate in an EV:

- **Secure transportation of the Contract Certificate from EMSP to EV**

  The communication from the EMSP, through a Charging Station and the back office of a CSO (CSMS), to the EV should be secure. Certain points through which the Contract Certificate is transported could be operated by different parties (possibly competitors). This means that the transport of a crucial piece of information from EMSP to EV, the private key belonging to the Contract Certificate of an end user, needs to be secured in such a way that only the EV can read the private key. In order to achieve secure communication between EMSP and EV, ISO 15118 uses encryption using the public key of the certificate that was put in the EV in the factory, the "OEM provisioning certificate". This means that the EMSP needs the public key of the specific EV when preparing the Contract Certificate for sending (encryption is done using a public key, decryption can only be done with the private key from the EV). This means that the EMSP is required to have a connection with the OEM of the EV in order to get this public key, and that the OEM needs to store all public keys of all its EVs and keep these available during the lifetime of the EV. This storage is called the 'OEM Provisioning Certificate Pool', a term that is introduced in paragraph 4.2. .

- **Installing the Contract Certificate into the EV fast enough**

  When an EV connects to a Charging Station, it can request to install or update its Contract Certificate. The Charging Station passes on this request to the CSO, which needs to be able to get this certificate from "somewhere". Due to the time limits prescribed in ISO 15118 (see appendix), this has to be "fast" (within 5 seconds). To do this, the concept of a 'Contract Certificate Pool' is introduced (see paragraph 4.2), which is a (partially) centralized store where contract certificates can be put by the EMSP. This enables the EMSP to prepare a contract certificate, encrypt the private key and store it in the pool, so that the CSO can request it based on the ID of the EV and can get an answer directly.

3.4. UPDATING A CONTRACT CERTIFICATE AT THE INITIATIVE OF THE EMSP

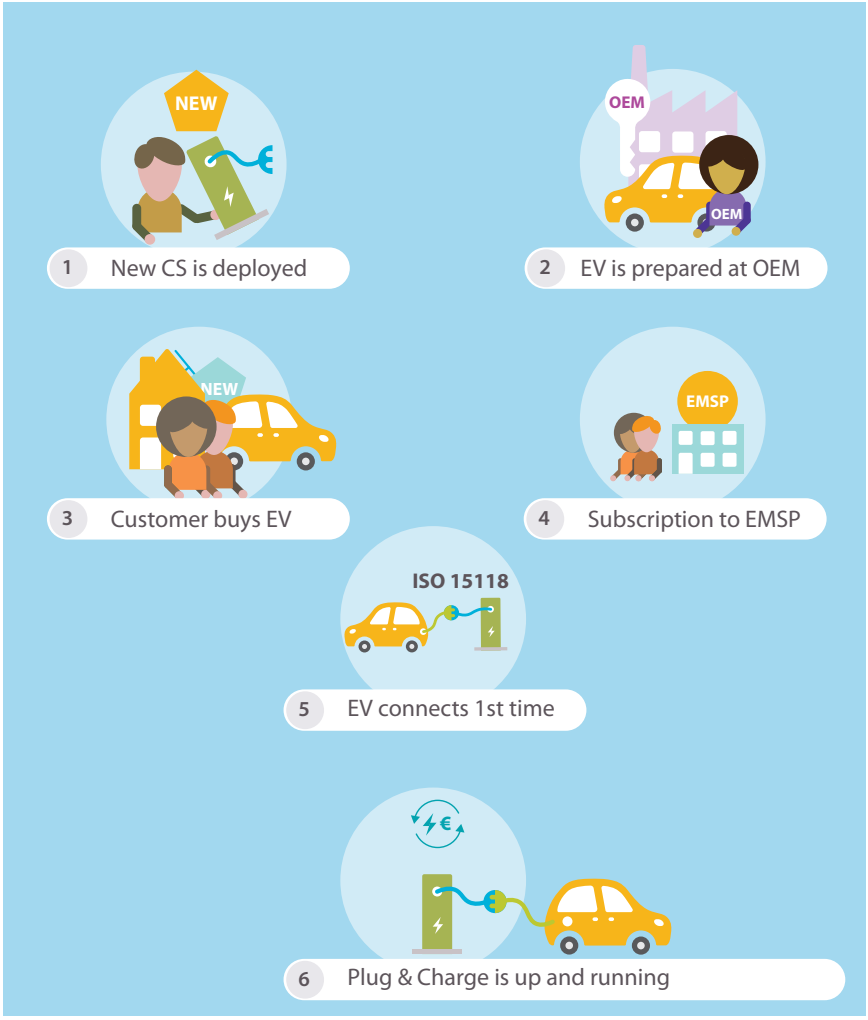
When the Contract Certificate of an EV is about to expire or already expired, that EV will request a new Contract Certificate from the Charging Station that in turn will forward the request to the CSO, and the CSO to the EMSP and back to the EV.

If the EMSP has a new certificate ready for an EV, there are different possibilities to get that contract installed inside the EV:

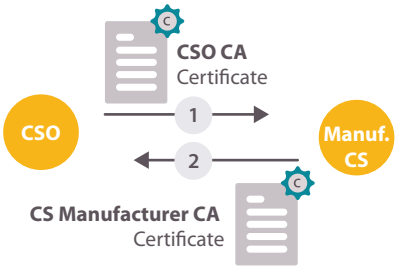
- The EMSP waits for the old contract to expire (the EV will automatically search for a new certificate)
- The EMSP revokes the old certificate.
- The EMSP informs its customer that it should trigger a certificate update from an EV display. This last option is not further specified in the ISO 15118, but besides the user input is the same as the certificate expiry scenario.

3.5. CERTIFICATES EXPLAINED STEP BY STEP

To explain the various applicable certificates, this paragraph describes a scenario starting at setting up a Charging Station until charging the EV is ready for using the Plug and Charge (PnC) functionality described by ISO 15118. The sequence describes the steps in the scenario for Plug and Charge authorization using ISO 15118, including preparatory steps. The various certificates are indicated with an underline.



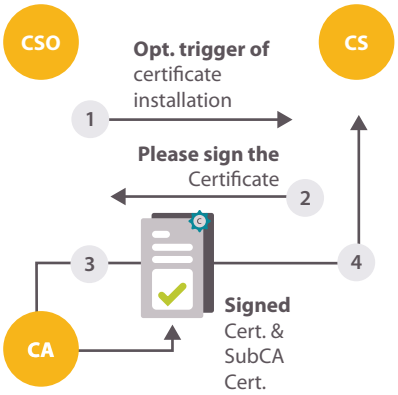
3.5.1 CHARGING STATION IS DEPLOYED IN THE FIELD



Initial connection

1 The CSO provides the CSO CA certificate for provisioning to the Manufacturer of the Charging Station

2 The Manufacturer of a Charging Station provides its CS Manufacturer CA certificate for provisioning the Charging Station to the CSO



Install new certificate in Charging Station (OCPP use cases A02/A03)

1 CSO (optionally) triggers the Charging Station to install a new certificate

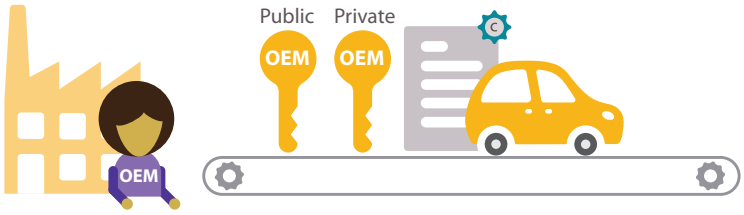
2 Charging Station sends a certificate signing request to the CSO.

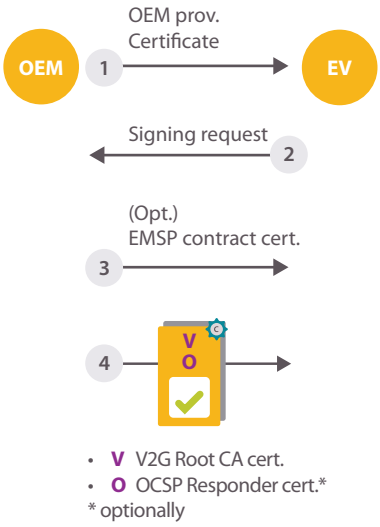
3 CSO forwards the request to a Certificate Authority or signs the certificate itself (if the CSO fullfils the role of Certificate Authority)

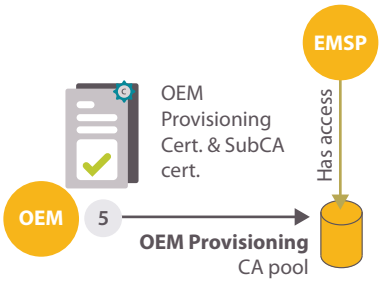
4 The signed Charging Station certificate including sub CA certificates is sent back to the Charging Station

CSO installs the V2G Root CA certificate in the trust store of the Charging Station

3.5.2 EV IS PREPARED AT THE OEM







1 OEM of the EV puts the OEM provisioning certificate in the EV.

2 This could be done by letting the EV generate a private and public key and then send a certificate signing request to the OEM backend.

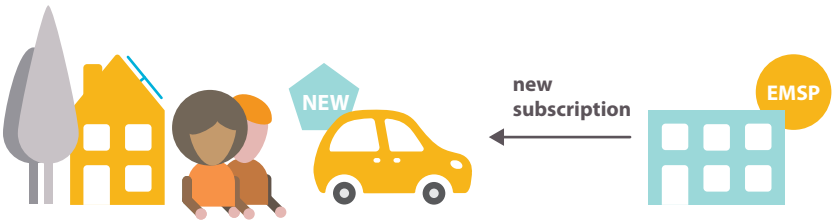
3 OEM of the EV can put a Contract Certificate of an EMSP in the EV if the EMSP is known, which could be the case when the OEM also fulfils the role of EMSP.

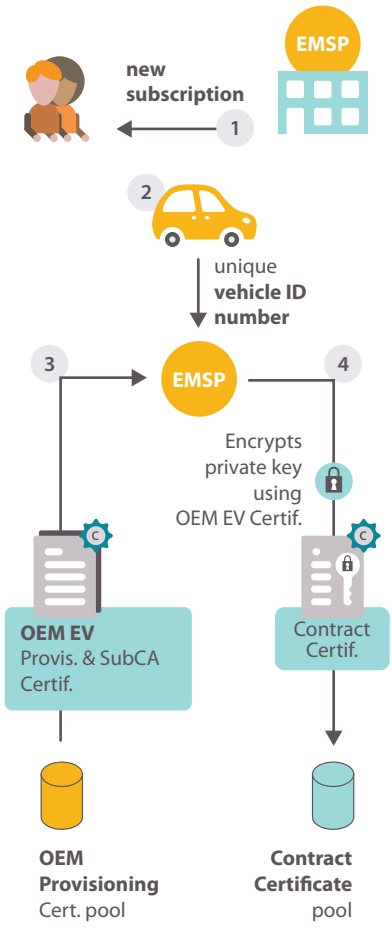
4 OEM of the EV puts the following certificates in the trust store of the EV:

- V2GRoot CA Certificates (that according to ISO 15118 must be used by Charging Station Operators, can be used by EMSPs and must be used by Certificate Provisioning Services (CPS, explained in 4.1.1)
- (optionally) OCSP Responder Certificates used by the OCSP responders that provide information concerning Charging Station certificates (explained in 4.1.2)

5 OEM of the EV puts the OEM provisioning certificate including SubCA certificates of the OEM in the 'OEM Provisioning Certificate Pool' that is accessible by the EMSP

3.5.3 USER ACQUIRES AN EV & SUBSCRIBES TO EMSP





Customer buys an EV

Customer subscribes to an EMSP

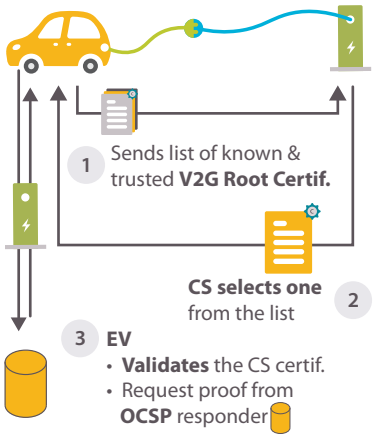
1 Customer subscribes to an EMSP for Charging Services

2 Customer sends its unique EV identifier to the EMSP (called PCID, see 4.2.2)

3 EMSP gets the 'OEM Provisioning Certificate' including SubCA certificates of the OEM from the 'OEM Provisioning Certificate Pool'

4 EMSP creates a Contract Certificate, encrypts the associated private key using the OEM Provisioning Certificate (so only the EV can read it) and puts it in the form of a specific efficient XML format ("EXIResponse") in a 'Contract Certificate Pool'.
To ensure the EV that this message containing the Contract Certificate has not changed since the EMSP created it, it is signed. If the EMSP CA certificate has been issued by the V2G Root CA, the EMSP can sign it using its own EMSP CA certificate. Using the V2G Root CA in its trust store, the EV will be able to verify the message. If the EMSP CA certificate has not been issues by the V2G Root CA, the EMSP must have its messages containing Contract Certificates signed by a Certificate Provisioning Service (a separate role, explained in 4.1.1). This CPS uses a certificate that has been issued by the V2G Root CA, so the EV will again be able to verify the signed messages from the EMSP.

3.5.4 EV CONNECTS TO AN ISO 15118 CHARGING STATION FOR THE FIRST TIME

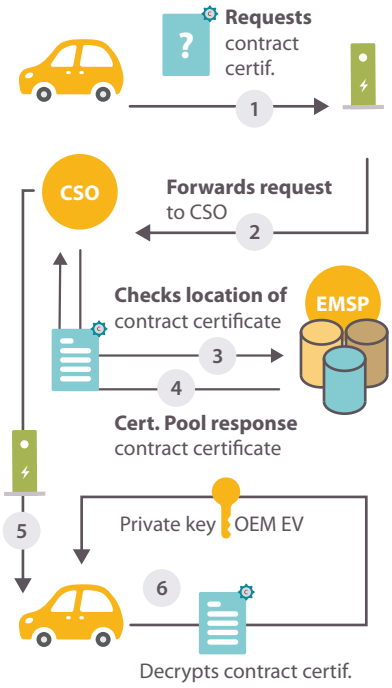


Establish EV – Charging Station connection

1 EV user plugs in the cable and the EV sends the list of V2G Root certificates it knows / trusts

2 The Charging Station selects one of its certificates that is derived from one of the V2G root certificates in the list and uses this to start a TLS handshake. This can be its previously installed Charging Station certificate or separate ISO 15118 certificate

3 The EV uses the V2G Root CA certificate to validate the certificate chain of the Charging Station and requests "proof" (that the Charging Station's Certificate is still valid) from an OCSP responder, all within the TLS handshake.



Get contract certificate

1 EV discovers it needs a contract certificate and requests a contract certificate via an EXIRequest (containing the PCID, explained in 4.2.2) to the Charging Station

2 The Charging Station forwards the request for a contract certificate to the CSO

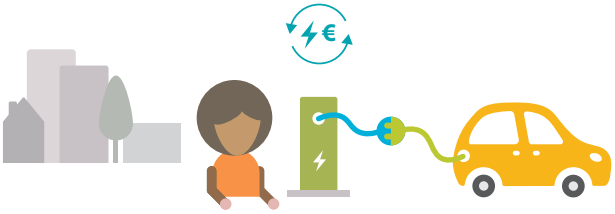
3 CSO checks where it can retrieve the contract certificate, either by checking the Directory Service (see 4.2.3) or by checking all EMSP Contract Certificate Pools

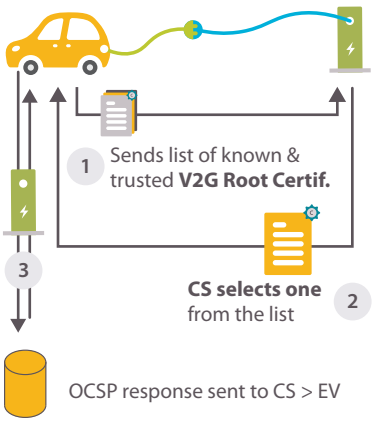
4 The CSO forwards the request for a contract certificate to the correct certificate pool. The certificate pool responds with the contract certificate in the form of an EXIResponse.

5. The CSO forwards the contract certificate to the EV via the charging station.

6 The EV retrieves and decrypts the private key using the private key associated with its OEM Provisioning certificate. Furthermore, it should validate whether it was signed by a private key associated with a certificate issued by the V2G Root CA (again, see paragraph 4.1.2)

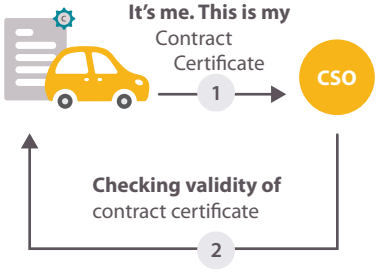
3.5.5 PLUG AND CHARGE AUTHORIZATION





Establish TLS connection

1 EV user plugs in the cable and the EV sends the list of V2G Root certificates it knows / trusts
2 The Charging Station selects one of its certificates that is derived from one of the V2G root certificates in the list and uses this to start a TLS handshake. This can be its previously installed Charging Station certificate or separate ISO 15118 certificate
3 If the EV requests an OCSP proof (regarding the validity of the Charging Station's leaf certificate), the Charging Station gets an OCSP response (via the CSO) and forwards it to the EV
4 The Charging Station sets up a connection using its previously installed Charging Station certificate or separate ISO 15118 certificate



Identification, Authentication and Authorization

1 EV identifies itself using its Contract Certificate
2 Authorization via CSO with the Contract Certificate. Before allowing charging, the certificate validity is to be checked. This can be done in multiple ways, see 4.4. When certificate validity is checked locally at the Charging Station, the (public) EMSP Root CA certificate must be known in the Charging Station. Reasons for this can be that the Charging Station is offline or for speeding up the validation.

Without simplifications

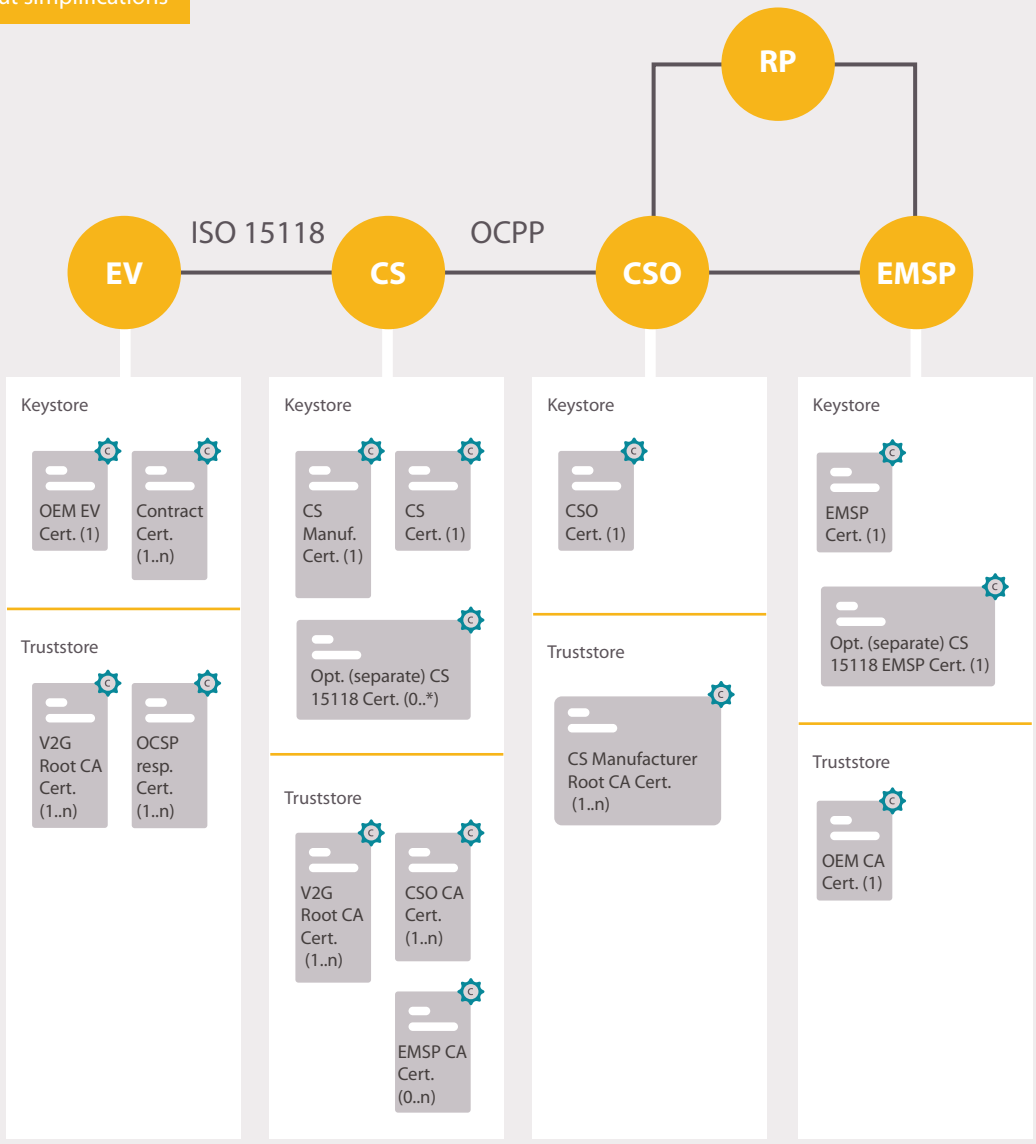


FIGURE 6: *overview of used certificates (without simplifications)*

3.6. OVERVIEW OF CERTIFICATES STORED IN THE ECOSYSTEM

In summary, the certificates that are in use are shown in **figure-6** and listed in **table 1**. The amount of instances of a certificate are included in brackets. For example, OEM EV certificate (1) means that an EV only has 1 OEM EV certificate, whereas Contract Certificate (1..n) means that each EV could have 1 to n Contract Certificates.

Please note that this figure does not contain the simplifications that are discussed later in this document.

For readability, the certificates used between the EMSP, Roaming platform, and DSO are left out of the following discussion. These certificates are used for connections between backend systems which are also important for the EV market, but less relevant for the discussion. Reason for this is that these certificates do not concern individual remote or even moving devices such as Charging Stations and EVs and thus have less technical restrictions and concern smaller numbers. However, for completeness, it would be best to consider these certificates as part of the same PKI.

Table 2 shows with the restrictions imposed by ISO 15118 that:

- All CSOs should reside under the same V2G Root CA
- All EMSPs should reside under this same V2G Root CA or must have their messages signed by a Certificate Provisioning Service (explained in 4.1.1), which in turn resides under the same V2G Root CA,

Plug and Charge functionality still involves many certificates. In the following chapter additional solutions for reducing complexity will be discussed.

	CERTIFICATE	PURPOSE	SIGNATURES	AUTHENTICATION	ENCRYPTION	#
Certificates stored in the key store: to authenticate itself						
EV	OEM EV (provisioning) certificate	Certificate installed in the EV, used for provisioning the EV with a contract certificate (first time at a Charging Station or whenever the installed contract certificate has expired).	X	X	X	1
	Contract Certificate	For authorizing an EV for charging based on a contract by an EMSP.	X	X	X	1-n Δ
C S	CS certificate	Certificate in Charging Station, used for setting up a TLS connection with the CSO and for ISO 15118 communication to the EV.	X	X	X	1
	CS 15118 certificate	Optional separate certificate for ISO 15118 communication to the EV (if CS certificate is not derived from V2G Root certificate).	X	X	X	0..n
	CS Manufacturer certificate	Certificate installed in the Charging Station, used for provisioning the Charging Station first time at a CSO.		X	X	1
CSO	CSO certificate	Certificate for setting up a connection with a Charging Station and other parties such as EMSPs.		X	X	1
EMSP	EMSP certificate	Certificate for setting up a connection with other parties such as CSOs.	X		X	1
	Op. (sep.) 15118 EMSO certificate	Certificate used for issuing contract certificates.	X		X	1

	CERTIFICATE	PURPOSE	SIGNATURES	AUTHENTICATION	ENCRYPTION	#
CA certificates – stored in the trust store to authenticate others						
EV	V2G Root certificate	Needed for trusting certificates from Charging Station.		X	X	1-n
	OCSP responder certificate	Certificate needed for checking the OCSP response for the CSO certificate(s).	X			1-n
CS	CSO CA certificate	Needed in CS to trust the CSO when connecting for the first time.		X	X	1-n$^{\pi}$
	EMSP CA certificate	For validating the contract certificates from the EV if checked locally / offline.		X		0-n$^{\partial}$
	V2G Root certificate	Needed for setting up a connection to the EV, which is done with a Charging Station certificate derived from this Root CA certificate		X	X	1-n
CSO	CS Manufacturer CA certificate	Provisioning CS when it connects for the first time.		X	X	1-n$^{\Theta}$
EMSP	OEM CA certificate	For validating the OEM certificate chain it receives from the OEM.		X		1

TABLE 2: *overview of (maximum number of) used certificates without the simplifications applicable in ISO 15118 (see chapter 4)*

$^{\Delta}$ As many EMSPs as the EV driver wants to contract

$^{\pi}$ As many as there are CSOs

$^{\partial}$ As many as there are EMSPs

$^{\Theta}$ As many as there are CS manufacturers

CHAPTER 4 IN A NUTSHELL

The constraints to the PKI infrastructure that were described in the previous chapter result in a highly complex system. Within the ISO 15118 standard a 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.

The validity check of a contract can 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.

4. SOLUTIONS FOR REDUCING COMPLEXITY

When using a PKI there are many actors and absolute number of devices (EVs, Charging Stations) and customers to consider. In order to make certificate handling workable, a number of ways to reduce complexity have been introduced or could be introduced, several proposals currently exist with different statuses. This chapter considers a number of measures from ISO 15118 and from the VDE application guide that can be taken. Furthermore, a number of options for the certificate validity checks are considered.

If any party can choose its own certificate or act as a CA, this will lead to a lot of CA certificates that should be exchanged (e.g. manually) and perhaps troubleshooting before actual communication can take place. This troubleshooting is expected to be necessary, since if a user plugs in and a connection is not established due to a failing handshake (user sees "it doesn't work"), the details of the certificates (expiration dates, fingerprints, signatures, chains) should all be checked to see what certificates are missing to allow the EV to charge. Furthermore, when new EMSPs enter the market, their (new) certificates should also be sent to all existing Charging Stations. In short, this means freedom of choice for all involved parties, but also a lot of connection problems, which will result in EV users not being able to charge everywhere.

4.1. PKI SIMPLIFICATIONS IN ISO 15118

The ISO 15118 standard introduces several means to reduce PKI complexity:

1. Certificate Provisioning Service (CPS)
2. Derive certificates from the same Root CA
3. Limit the number of V2G Root CAs in an EV
4. Limit the number of layers for a SubCA to 2
5. Limit the number of Contract Certificates in an EV to 1 »

4.1.1 CERTIFICATE PROVISIONING SERVICE

When an EMSP wants to put a contract certificate in the contract certificate pool, this has to be signed by a private key whose associated public-key certificate is trusted by the EV. This way, the EV can be sure that the certificate and private key have not been changed while being transported from EMSP to EV. The most simple way would be to let the EMSP sign the message containing the private and public key. However, to check a signature, the leaf certificate of the EMSP should be trusted by the EV. When this is derived from the V2G Root CA certificate, a trust relation can be established. However, it is not mandatory according to ISO 15118 that the EMSP certificate is derived from the V2G Root CA (see **figure-7**), since this might be experienced as too restrictive by EMSPs that might want to fulfil the role of a CA. To be able to verify the signature of the message containing the contract certificate, the EV should then store the CA certificate of every EMSP in the world, which could become a large number and might lead to a scalability issue.

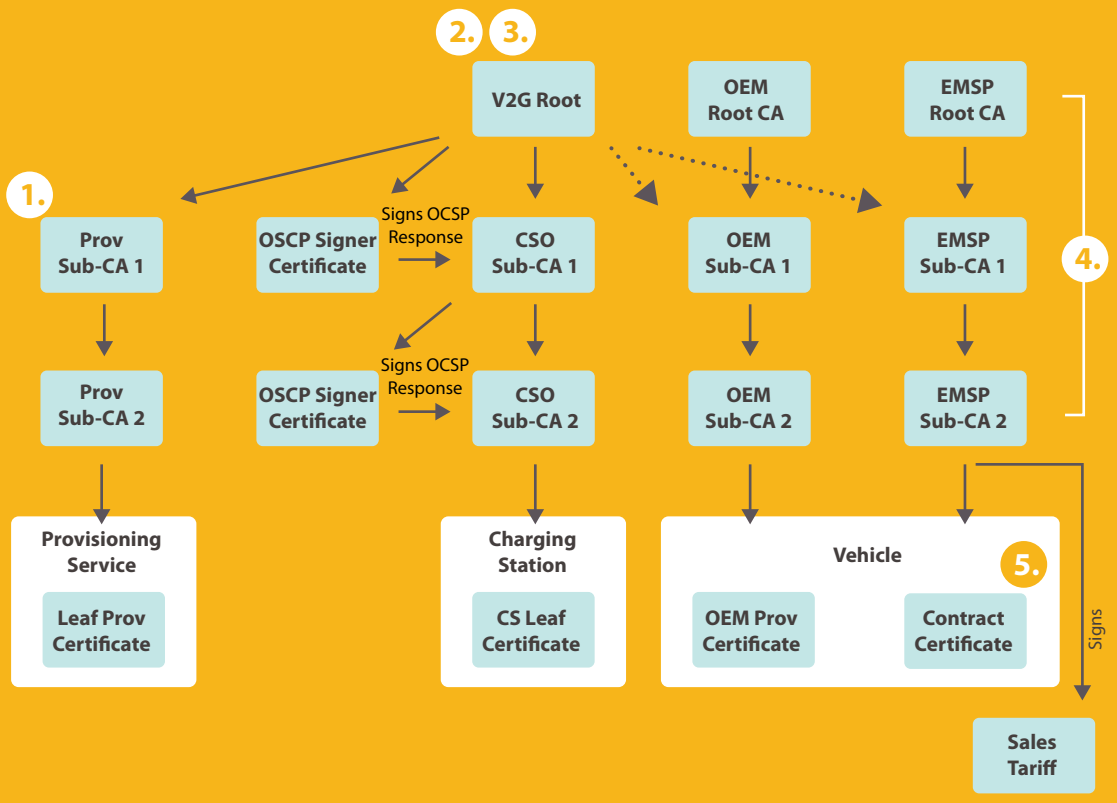


FIGURE 7: *Certificate restrictions ISO 15118*

To reduce this issue, the role of "Certification Provisioning Service" (CPS) is introduced in the ISO 15118 standard. Instead of letting each EMSP sign its own messages, a small number of CPS's (trusted parties) must sign certificates for EMSPs. Due to the certificate hierarchy in ISO 15118 as shown in the next paragraph, this CPS certificate must be derived from the V2G Root CA certificate, which reduces complexity: it is not necessary to store separate CA certificates for the CPS and this also means that no EMSP certificates have to be installed in the EV. Please note that the role of CSP can be fulfilled by the EMSP itself.

4.1.2 DERIVE CERTIFICATES FROM THE SAME ROOT CA

The ISO 15118 standards sets limitations regarding the Root Certificate Authority that are summarized in **figure-7**. The dotted lines indicate that the relation is not required. As can be seen in **figure-7**, ISO 15118 states that:

- All Charging Station Certificates must be derived from one V2G root. Reason for this is that if every CSO would use a random root CA certificate (either from an known CA or a CSO itself fulfils the CA role), each EV would have to store all these root CA certificates, which could lead to hundreds of CA certificates (that have to be managed as well).

  Please note that this implies that if the ISO 15118 standard is followed:

  - Charging Station Operators will not have the freedom to select a Root CA of their own choice for ISO 15118 communication.
  - If the certificates of an EMSP are not derived from the same V2G Root CA as the Charging Station itself, the Charging Station needs to store the CA certificates of each EMSP separately to be able to do an offline certificate validation. If the Charging Station has not stored these additional CA certificates, "High Level Communication" (among which Plug & Charge) cannot work when offline.
  - If the Charging Station selects a Root CA other than the V2G Root CA as prescribed in ISO 15118, then this Root CA should be known to every EV to make Plug & Charge work. Since it will not be possible to setup ISO 15118 communication (e.g. for installing a contract certificate) without

this certificate, this means that this should be included in the EV in factory.

- The OEM (EV) provisioning CA certificate and the EMSP (in ISO 15118 referred to as "MO") Root CA certificate are not necessarily derived from the V2G Root CA certificate. This is assumed (in the VDE application guide) to be operated by the OEM / EMSP itself. Please note that this implies that in that case OEMs and EMSPs will have the freedom to select a Root CA of their own choice.

- However, even though EMSPs have the freedom to choose the Root CA of their choice for issuing contract certificates, they are required to let a CPS sign the message containing the Contract Certificate. Because the CPS certificate is derived from the V2G Root CA the EV can then verify the CPS certificate up to the Root CA using the V2G Root CA certificate.

- When a consumer wants to use an EMSP contract, but the EMSP contract certificates are not derived from (one of the) the general V2G Root CA(s):

    - Each Charging Station will need to additionally store the CA certificates of each of these EMSPs separately into their trust store, to be able to do a local / offline contract certificate validation.

    - If the CSO does not (want to) store the EMSP CA certificate in the Charging Station, "High Level Communication" (among which Plug & Charge) will not work.

The V2G root CA and CPS are an important aspect of making the entire ecosystem interoperable, manageable and open. The V2G root CA and CPSs should therefore be carefully selected, which is explained in more detail in chapter 5.

4.1.3 LIMIT THE NUMBER OF V2G ROOT CAS IN AN EV

The EVs should store the V2G Root CA and OEMs want to limit the memory space and computational power for certificate verifications due to cost constraints. Therefore the ISO 15118 standard suggests to limit the number of V2G Root CA certificates: it requires at least 1 V2G Root CA certificate and recommends a minimum number of 5. [note: the size of an ISO 15118 V2G Root CA certificate is maximized to 800 bytes]. This number of 5 relates to the number of continents (although there are 7 continents).

4.1.4 LIMIT THE NUMBER OF LAYERS FOR (SUB)CAS TO TWO

In the ISO 15118 standard the maximum number of (Sub)CA certificates is set at two. This is a compromise between the OEMs that wanted short certificate chains since these have to be stored in the EV. Other parties ("Secondary actors") wanted to be able to sign certificates themselves, not being dependent on a central organisation and preferred more intermediates certificates as this makes it possible to manage certificates easier (i.e. more options to classify / sort certificates):

- As a consequence of these requirements, the lowest SubCA level should be the secondary actors, such as CSOs and EMSPs, to enable them to sign their own leaf certificates (for Charging Station certificates and contract certificates).
- Limiting the number of layers makes validation faster / less difficult or reduces the number of SubCA certificates to cache / store.
- Limiting the number of layers limits the freedom in certificate structure and thus in classifying / sorting certificates. Because of these limits the certificate hierarchy should be carefully chosen, since afterwards limitations cannot be handled by "just adding a new layer".

4.1.5 LIMIT THE NUMBER OF CONTRACT CERTIFICATES IN AN EV TO ONE

In the ISO 15118 standard edition one, the number of Contract Certificates in the EV is limited to one. This means that an EV user can only have one contract at one EMSP at the same time.

This ISO 15118 edition one requirement is not compatible with certain current E-Mobility services such as car sharing and using multiple EMSPs for different Charging Services, for example company cars where the EV user must charge with its own contract for private use. In the draft ISO 15118 edition 2 (69/621/CDV, date of circulation 2018-09-07) the use of multiple contract certificates in one EV is added.

4.1.6 OVERALL DESIGN INCLUDING THE SIMPLIFICATIONS IN ISO 15118

In summary, simplifications of the PKI design in ISO 15118 result in:

- A limit to the number of certificates needed for the secure installation of Contract Certificates (by introducing a CPS role).
- Reduction of the number of Root CA certificates in the ecosystem by introducing a V2G Root CA including a mandatory certificate hierarchy.
- A limit to the information exchange of Public Keys of CA during handshake by limiting the number of SubCAs to two.
- A limit to the number of contract certificates in the EV.

In the table an overview of certificates is given, including the simplifications discussed in this chapter.

TABLE 3:

Certificates needed for ISO 15118 including simplifications

π As many as there are CSO's that work with this CS Manufacturor.

ə As many as there are CS of different Manufacturers connected to the CSO

	Key Store		Number
EV	OEM EV (provisioning) certificate	Certificate installed in the EV, used for provisioning the EV with a contract certificate (first time at a Charging Station or whenever the installed contract certificate has expired).	1
	Contract Certificate(s)	For authentication and authorization an EV for charging based on a contract by an EMSP.	1
	Trust store		
	V2G Root CA certificates	Needed for trusting certificates from Charging Station and verifying signatures of the messages that contain the EMSP contract certificate	1 to 5 (suggested)

CHARGING STATION	**Key Store**		
	CS certificate	Certificate in Charging Station, used for setting up a TLS connection to the CSO and for ISO 15118 communication to the EV.	1
	CS 15118 certificate	Optional separate certificate for ISO 15118 communication to the EV (if CS certificate is not derived from V2G Root certificate).	0..5
	CS Manufacturer certificate	Certificate installed in the Charging Station, used for provisioning the Charging Station first time at a CSO.	1
	Trust Store		
	CSO CA certificate	For trusting the CSO when connecting for the first time.	1 to n π
	V2G Root CA certificate	For setting up a connection to the EV, which is done with a Charging Station certificate derived from this Root CA certificate.	1 to 5
	EMSP CA certificates	For validating the contract certificates from the EV if checked locally / offline. Only needed for EMSPs not derived from the V2G Root CA.	0 to n
CSO	**Key Store**		
	CSO certificate	Certificate for setting up a connection with a Charging Station and other parties such as EMSPs.	1
	Trust Store		
	CS Manufacturer CA certificate (s)	Provisioning CS when it connects for the first time.	1 to n ə
EMSP	**Key Store**		
	EMSP certificate	Certificate for setting up a connection with other parties such as CSOs.	1
	Opt (separate) 15118 EMSP certificate	Certificate used for issuing contract certificates.	1
	Trust Store		
	OEM CA certificate(s)	For validating the OEM certificate chain it receives from the OEM.	

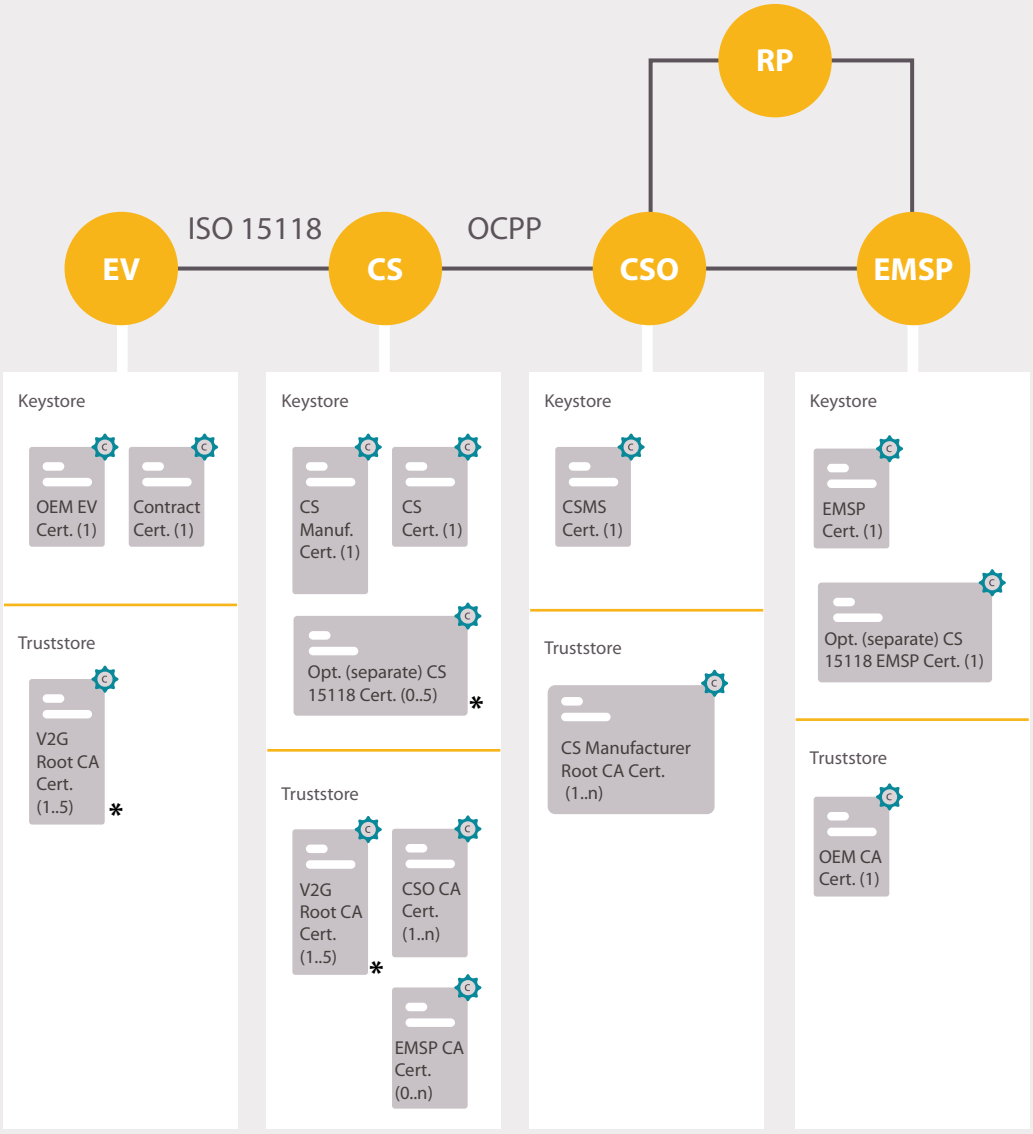


FIGURE 8: *ISO 15118 certificate overview including simplifications*

Please note that the OCSP responder certificate for checking the OCSP responses for the Charging Station certificate and the CPS certificate needed for verifying the signature of the Contract Certificate are left out of the table above. Due to certificate hierarchy (derived from V2G Root CA) it is not necessary to include these separately.

In the figure the simplifications for the numbers of certificates are represented (compare to **figure-6**).

Comparing **figure-8** with **figure-6** shows that the simplifications in ISO 15118 are aimed at reducing the amount of certificates stored in the EV. Additionally it simplifies access for EMSPs to the PKI, since they can use / become a CPS instead of having to install its EMSP CA certificate in each EV.

4.2. PROPOSALS BY THE GERMAN VDE

The German VDE (Verband der Elektrotechnik, Elektronik und Informationstechnik) is a German Association for Electrical, Electronic & Information Technologies, active in - amongst others - developing technical regulations. It has published an application guide ('Anwendungsregel') that currently only has a formal status inside Germany. It introduces the following concepts:

1. Introducing certificate pools for both OEM EV certificates and Contract Certificates and combining certificate pools at a central location, for fast access.

2. Provisioning Certificate ID. The unique ID of the OEM Provisioning Certificate that can be used for requesting certificates from the OEM Certificate Pool by EMSPs.

3. Directory Service. A lookup table to check at which location information for a specific OEM or EMSP is found when multiple certificate stores (pools) exist.

4.2.1 INTRODUCING CERTIFICATE POOL CONCEPT

The VDE application guide introduces the 'Certificate Pool' as a concept to manage the timeliness of the installation of certificates.

- **De OEM Provisioning Certificate Pool**

  This is a data store where the OEM stores all public certificates of all EVs. An EMSP can use these certificates to encrypt the Contract Certificate issued by the EMSP in such a way, that only that specific EV can read that Contract Certificate. The EV used its OEM provisioning certificate private key to decrypt the Contract Certificate. EMSPs can prepare their customer's Contract Certificates in advance and store these in the (EMSP) Contract Certificate Pool.

- **The EMSP Contract Certificate Pool**

  This is a data store where prepared Contract Certificates for specific EVs are ready and waiting for installation in that EV. A CSO can request the specific Contract Certificate that belongs to the EV that is connected to one of its Charging Stations. The installation of the Contract Certificate can be directly using such a pool, since the certificate was prepared by the EMSP in advance.

- **Combining Certificate pools at a central location**

  As explained in chapter 3, part of using the ISO 15118 standard concerns getting certificates from EMSP to the EV:

  - To enable all EMSPs to get the OEM EV public keys to encrypt the private key associated with the Contract Certificate, and
  - To enable all CSOs to access Contract Certificates of all EMSPs

  In order to prevent EMSPs to retrieve OEM Provisioning Certificates from each OEM individually, OEMs could store their OEM Provisioning Certificates in a central location. Likewise, in order to prevent CSOs to have to contact EMSPs individually to retrieve the Contract Certificates, all Contract Certificates could be stored at a central location. These are called 'Certificate Pools' for OEM certificates and Contract Certificates. Especially Contract Certificates are interesting due to the potential large amount of parties fulfilling the role of EMSP that creates these certificates.

4.2.2 PROVISIONING CERTIFICATE ID (PCID)

In a similar way as the EMAID, the VDE application guide defines an ID for the OEM Provisioning Certificate, the Provisioning Certificate ID (PCID). When using this in the OEM Provisioning Certificates, this can be used to request certificates from the OEM Certificate Pool by EMSPs. By including the OEM in this ID, it can also be used for finding the right OEM Certificate Pool, in combination with a Directory Service.

4.2.3 DIRECTORY SERVICE

When a certificate is to be fetched for an EMSP from a certificate pool and more than one certificate pool exist (that do not have copies of each other's certificates), an additional "register" is necessary to determine where the Contract Certificates of a specific EMSP are stored. From the PCID that a CSO receives via a Charging Station, it can determine which OEM EV is involved (for Certificate Installation).In a similar way it can, from the EMAID that it receives via a Charging Station determine which EMSP is involved (for Certificate Update). Using this register, the CSO can determine where it can find the Contract Certificate that is to be installed in the EV. This register is called a Directory Service.

4.3. USE OF TELEMATICS FOR UPLOADING CERTIFICATES

Another simplification could be the use of telematics for uploading certificates directly from the OEM system to the EV. This could provide a more robust, efficient and certain channel for OEM related EMSPs. If, for example, an additional V2G Root CA should be added, this could be done as soon as possible by an OEM, the EV does not have to be plugged in at a Charging Station for the ISO 15118 "route".

Please note that this only works for OEM affiliated EMSP, it is uncertain whether it will practically be possible that EMSPs can get access to this telematics route.

4.4. CERTIFICATE VALIDITY CHECK

The ISO 15118 standard requires an OCSP responder for setting up the TLS connection from EV to Charging Station, because the EV requires an OCSP response, i.e. proof that the Charging Station certificate is valid. The ISO 15118 standard does not specify in detail in what way the validity of a leaf certificate (i.e. Charging Station and Contract Certificate) should be checked. This is detailed in the VDE appliction guide. It states that certificates are valid if they have not been altered after issuing, the signature up to the root CA level has not been compromised, it is within the validity period, X.509 certificate attributes are syntactically correct and the subject is ok.

Besides checking the technical validity of a certificate itself (including or excluding revocation), for Plug and Charge authorization a check can also be done to the EMSP that has created the Contract Certificate to check whether the contract is indeed valid. This is out of scope of the ISO 15118 standard and the VDE application guide, but needs to be decided on for a correctly functioning EV ecosystem. The table below lists a number of options for validating Contract Certificates. Please note that this table also has the option of using a CRL. Besides using the CRL to register compromised ("hacked") certificates as explained in 2.5, it can also be used to register contracts that are revoked for other reasons (e.g. defaulters, contracts ended by the customer).

Every option has its advantages and disadvantages and since an offline option seems only useful as a "backup" option, a trade-off has to be made which is the desired option within the EV market.

TABLE 4: *Authorization options when using ISO 15118*

Δ Depending on the EMSP, this could be between 1 month and 2 years

NO	OPTION	PRO'S	CON'S
1	Offline	• Simplicity • No online communication necessary • Faster authorization, so better customer experience	• Takes some time until discovering that a certificate is no longer valid (non-billable electricity) Δ • EMSP CA certificates that are not derived from a V2G Root CA have to be available in Charging Stations.
2	Online OCSP check	• Generic, existing standards	• Every EMSP must maintain a list of invalid certificates for the OCSP responder. • Additional (per session) communication costs. • Scalability might become an issue.
3	Online CRL check	• Generic, existing standards	• Every EMSP must maintain a CRL. • Additional (per session) communication costs. • CRL checking can become slow when checking multiple lists. • Scalability might become an issue.
4	Offline CRL check	• Generic, existing standard • Offline authorization possible • Faster authorization, so better customer experience	• (Telco) costs for sending CRL to Charging Stations (every x time). • Scalability might become an issue. • EV-specific, existing standards to be adjusted for sending CRLs.
5	CSO » EMSP direct	• Similar mechanism for (current) RFID charging card can be used. • Only EMAID can be used.	• EV-specific, existing standards to be adjusted. • Scalability might become an issue.
6	CSO » EMSP via Roaming Platform	• Similar mechanism for (current) RFID charging card can be used. • Only EMAID can be used. • Scalable solution	• Additional RP functionality necessary. • EV-specific, existing standards to be adjusted.

CHAPTER 5 IN A NUTSHELL

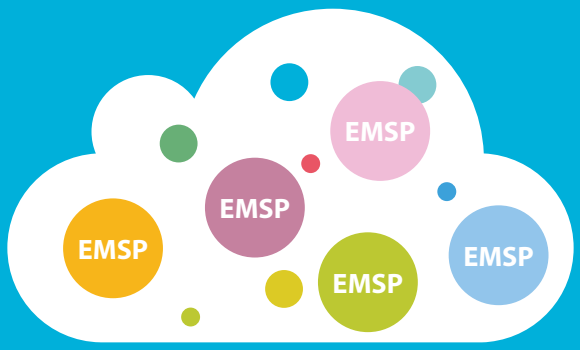
A number of different designs for a PKI for using ISO 15118 within the EV market are possible, ranging from a system managed by a single party or a consortium of parties, to an open PKI that allows everybody in the EV market to participate in the PKI. The design determines what agreements must be made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

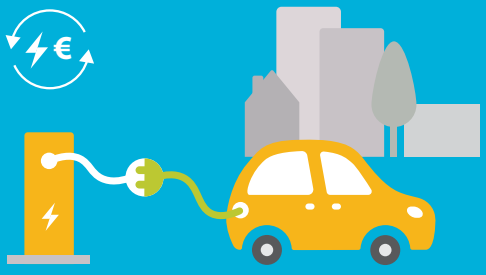
5. DESIGNING A PKI IN A SYSTEM

In the previous chapters we have explained the basics of how certificates work, how certificates are applied when using ISO 15118 for EV charging and what (technical) choices and simplifications are applied to make it a workable solution for the EV market.

In this chapter we will show a number of design options for a PKI within a market, starting in paragraph 5.1 with a Single Party System in which one party fulfils all roles needed for charging. In paragraph 5.2 we describe a system servicing a consortium, which consists of a limited amount of parties that co-operate. Some measures need to be taken to make sure that all systems are interoperable and work together to ensure that the targeted EV users can use the infrastructure. In paragraph 5.3 we describe an open PKI system that can be used by any EV user and which any party can access. The measures that have to be taken for a consortium are then no longer limited to the consortium parties, but are extended to any party.



EMSP
Subscription



EMSP
Subscription

EMSP
Subscription

5.1. SINGLE PARTY SYSTEM

In its simplest form, a Public Key Infrastructure can be set up as a Single Party System: one party manages the Certificates of the EV, the Charging Stations and the E-Mobility Contracts. This could be the case if an OEM also provides the Charging Infrastructure and acts as the E-Mobility Service Provider. When the entire ecosystem is in the hands of one party, by definition all certificates are trusted and derived from the same Root CA. It is a simple system, but excludes customers with other EV brands, customers with other EMSPs and other Charging Infrastructure Providers. This way of implementing a PKI will not be discussed further in this document.

5.2. CONSORTIUM PKI REQUIRED MEASURES

When several companies decide to set up an ecosystem that will allow EVs of multiple brands to charge at charging infrastructure of multiple providers using the E-Mobility services of multiple parties, they can decide to share a PKI. This PKI will be set up as a consortium. Examples of a consortium PKI are:

- A Public Transport Concession, where an EMSP handles the charging of busses at specific locations. Concessions may be awarded for a number of years.
- A consortium of OEMs, Charging Infrastructure Providers and EMSPs that want to offer a premium service to their customers and in that way distinguish themselves from competitors and alternative solutions.

Consumers driving EV brands and using E-Mobility Contracts, as well as Charging Station Providers that are not part of this consortium will not be able to use the Plug and Charge features and perhaps will not be able to access the information from the EV used in Smart Charging (such as the requested amount of energy and Time of Departure) via the Charging Infrastructure. The parties inside the consortium will decide if there should be a fall back service offered to non-consortium members or if charging is not possible at all.

This is a more complex system compared to the single party system, that will need a range of additional measures to reduce complexity and increase manageability (as explained in chapter 4).

A consortium PKI is a manageable way of implementing ISO 15118, arranging fees and access regulation. This PKI consortium will of course be – as is any consortium – subject to competition policy to make sure companies compete fairly with each other. Fair competition encourages enterprise and efficiency, creates a wider choice for consumers and helps reduce prices and improve quality. In case of the European Commission, an effective enforcement of competition rules is pursued, maintaining competition instruments aligned with market developments, as well as promoting a competition culture in the EU and world-wide. For more information, see European Commission Competition Directorate (http://ec.europa.eu/competition).

To setup a **consortium PKI**, for each role a number of measures should be taken.

CSO

- The V2G Root Certificate of all CSOs will have to originate from the designated party in the consortium.
- In the consortium, the CSOs need to agree on sending all the (V2G) Root CA Certificates of all EMSPs in that consortium, into the Charging Stations for enabling local / offline validations.

OEM

- All OEMs should store the V2G Root CA Certificates of the consortium into the EV at the factory (or use telematics to send these to all EVs later). Because of certificate hierarchy, CPS certificates are then also trusted by the EV.
- All OEMs should share their OEM Provisioning Certificates into a 'OEM Provisioning Certificate Pool' that can be accessed by all EMSPs in that consortium, either at each OEM separately or at a central platform (e.g. a Roaming Platform).

EMSP

- All EMSPs should store all their 'EMSP Contract Certificates' into a 'Contract Certificate Pool' that can be accessed by all CSOs in that consortium.
- The certificates of the EMSPs in the consortium should be derived from the V2G Root CA in the consortium. If not, the messages containing EMSP Contract Certificates should be signed by a CPS certificate which is derived from the V2G Root CA and thus trusted in the consortium.

Central platform **Cert. Pools**

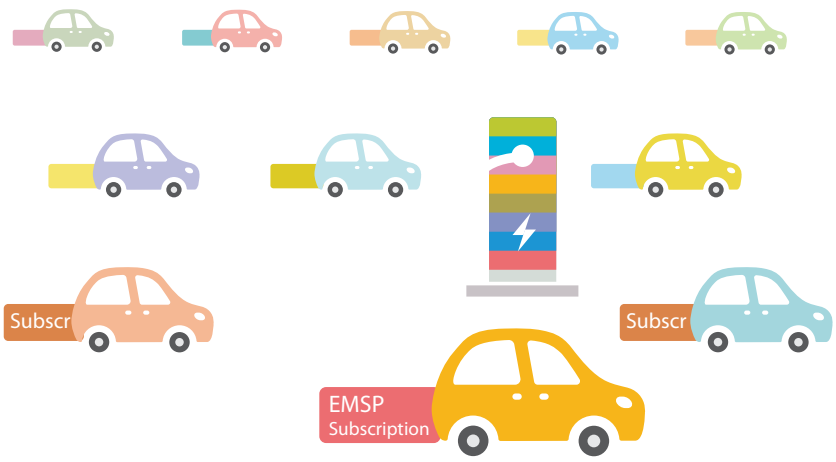
- The platform should be accessible for all OEMs in the consortium to provide their OEM provisioning certificates.
- The platform should be accessible for all EMSPs to provide their Contract Certificates.
- If the platform has the role of CPS, it should be accessible to all EMSPs in the consortium.

V2G Root CA

- It should sign all certificates of all CSOs and CPSs and optionally of EMSPs and OEMs in the consortium.

5.3. OPEN PKI REQUIRED MEASURES

An Open PKI calls for a system where any customer with any brand of EV supporting Plug & Charge can charge on any Plug & Charge enabled Charging Station using any Plug & Charge EMSP contract. This is the most complex form of PKI, that will need - in addition to the measures needed in a consortium PKI – regulation to ensure inclusion and a level playing field.



When compared to a consortium PKI, the **required measures are similar**, **but** access to the different platforms, Charging Stations and EVs is **not limited to the consortium**, but is provided to all parties in the EV ecosystem in order to have **access for all consumers.**

To setup a **open PKI**, for each role
a number of measures should be taken.

CSO

- Multiple V2G Root CA certificates should be installed in its Charging Stations.
- All EMSP Root CA certificates of EMSPs who's certificates are not derived from a V2G Root CA, should be installed into its Charging Stations for enabling local / offline validations.

OEM

- All OEMs should store all relevant V2G Root CA Certificates in the EV at the factory (or use telematics to send these to all EVs later).
- All OEMs should share their OEM Provisioning Certificates with a 'OEM Provisioning Certificate Pool' that can be accessed by all EMSPs. This can be done either at the OEM or at one or more central platforms (e.g. a Roaming Platforms).

EMSP

- All EMSPs should store all their 'EMSP Contract Certificates' with a 'Contract Certificate Pool' that can be accessed by all CSOs.
- The certificates of EMSPs should be derived from the V2G Root CA. If not, the messages containing EMSP Contract Certificates should be signed by a CPS certificate which is derived from the V2G Root CA and is thus trusted. All EMSPs should have access to a CPS.
- All EMSPs should update the Directory Service(s) to indicate where its certificates can be found.

Central platform **Cert. Pools**

- All EMSPs should have access to the Directory Service(s) for OEM provisioning certificates pools.
- All CSOs should have access to the Directory Service(s) for EMSP Contract Certificates pools.
- All CSOs should have access to all Contract Certificate Pools
- The platform(s) should be accessible for all OEMs to provide their OEM provisioning certificates.
- The platform(s) should be accessible for all EMSPs to provide theirContract Certificates.
- If the platform has the role of CPS, it should be accessible to all EMSPs.

V2G Root CA

- It should sign all certificates of all CSOs and CPSs and optionally of EMSPs and OEMs

In addition to the required measures for an open PKI as described above, more market agreements should be in place to guarantee openness for all parties in the EV ecosystem and the EV user.

When all certificates are derived from one V2G Root CA certificate, this means that all involved parties agree on trusting this one Root CA. Assigning this V2G Root CA is a political issue, since:

- The V2G Root CA has a powerful position (a monopoly for selling EV related certificates, has the possibility to deny CSOs access to the EV charging infrastructure, is dominant in disputes)

- All parties greatly depend on this one party, since it creates a single point of failure (for example when the V2G Root CA certificate would be 'compromised').

For all parties to accept this V2G Root CA it is essential to assign this role to a neutral and independent organization and to address terms, costs and quality aspects. When this V2G Root CA is a neutral and trusted party, this will also result in EMSPs being more inclined on getting a certificate from this V2G Root CA, which in turn could eliminate a separate role of Certificate Provisioning Service.

Certificate Pools provide essential information for all players that participate in the EV ecosystem. Therefore it is essential that all Certificate Pools allow open access for all parties that want to participate.

A process should be in place to facilitate revoking an existing EMSP contract, in case the customer contracts a new EMSP or when an EV driver purchases a second hand EV. This does not only concern consumer protection regarding EMSP contract duration and cancellation, but also involves agreement in the market on how this situation is handled. Especially when using more than one Certificate Pool, it should be very clear how this process works in order to have interoperability between different CSOs, Contract Certificate pools and EMSPs.

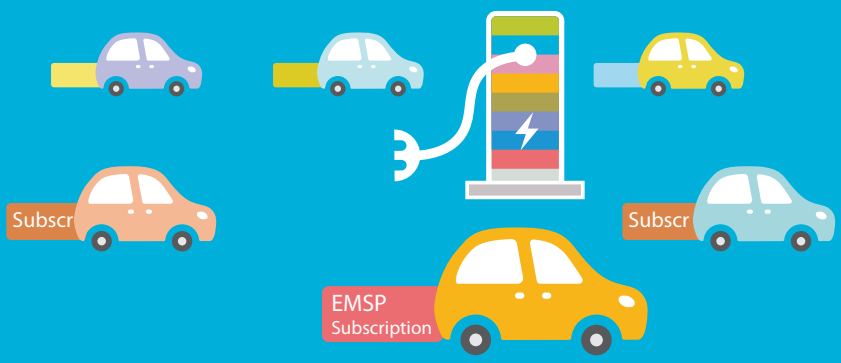
In an **open PKI** additional **market agreements** should be in place regarding the **V2G Root CA** and **Certificate Pools**.

V2G Root CA

- The neutral V2G Root CA provides certificates to all players in the EV market on equal terms.
- The costs of the certificate services and procedures of issuing should be regulated.
- Due to the critical nature of the Root CA, quality audits should be in place.
- There should be a market wide process in place that addresses the access and acceptance of new V2G Root CAs and SubCAs.

Central platform Cert. Pools

- Governance should be in place to ensure that all CSOs are allowed access to all Contract Certificate Pools and that all EMSPs are allowed access to all OEM Certificate Pools. In case multiple pools exist, access to Directory Services should also be allowed for all parties.
- A process should be in place to facilitate revoking an existing EMSP contract.
- When using more than one Certificate Pool, it should be very clear how market processes work in order to have interoperability between different CSOs, Contract Certificate pools and EMSPs.
- Fees for certificate pool services might need to be benchmarked.



CHAPTER 6 IN A NUTSHELL

As made clear in previous chapters, when using ISO 15118 in the EV market, many dependencies between market players exist and need to be addressed.

By awarding the V2G Root CA role to a neutral party, an open system is created that is supported by all market players. This broad market support will in itself accelerate the adoption of ISO 15118. Additionally, this central and neutral V2G Root CA architecture enables a hybrid system architecture of central platforms and peer to peer information exchange. Central platforms (such as roaming hubs) can host certificate pools and manage connections in an efficient way and will enable all players to join in.

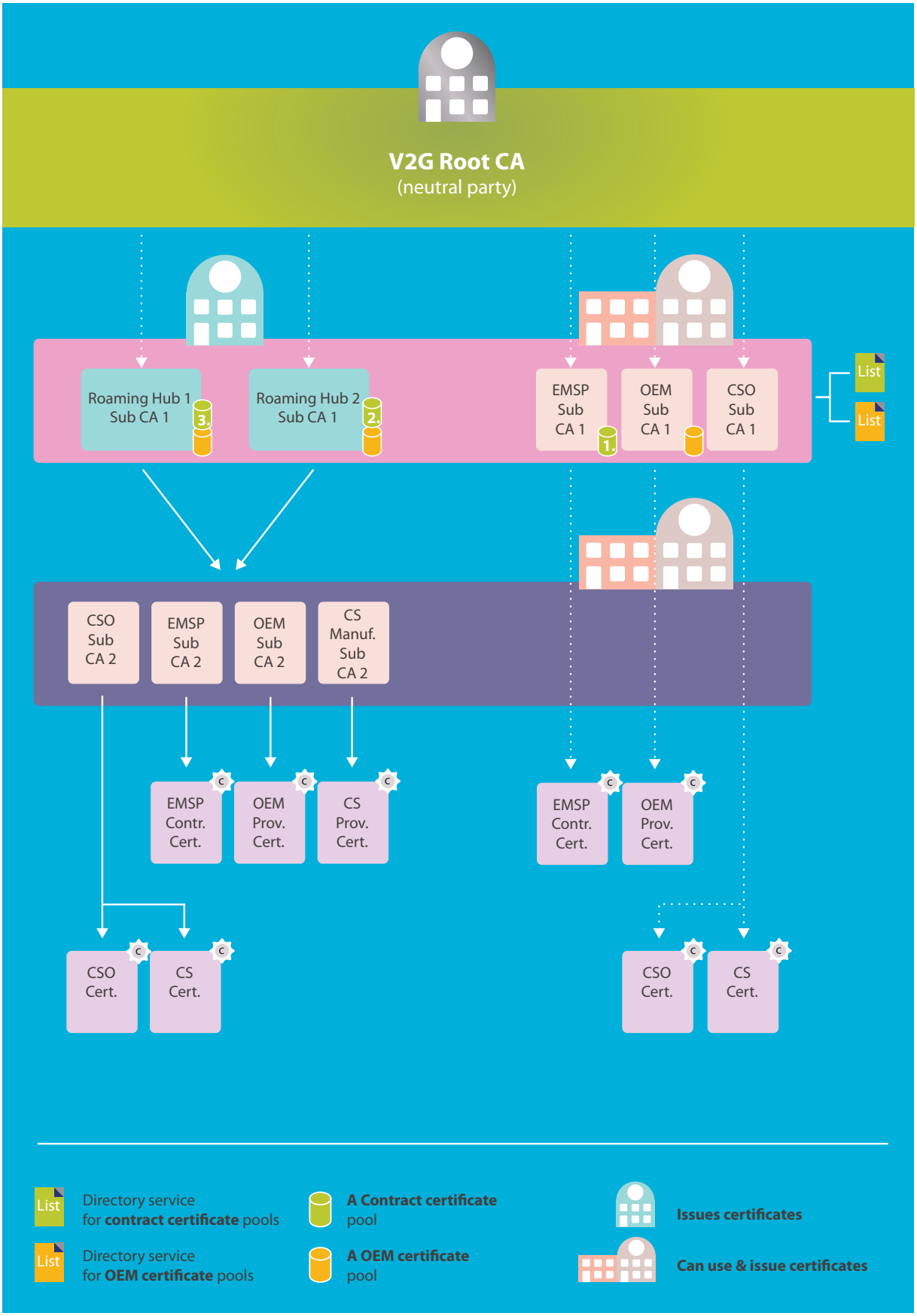
Peer to peer information exchange can be a preferred solution for large players. However, if these parties want to be part of the overall open PKI and thus reside under the same V2G Root CA, they should comply with the market agreements within the PKI.

6. DESIGN FOR AN OPEN PKI

Based on the discussion on this document so far, it can be expected that in some form certificate pools will become part of the EV market, to facilitate ISO 15118 based charging. In an earlier report by ENCS a number of PKI structures were proposed. Based on these assumptions and the discussion in this document, an additional PKI design option is proposed for an environment that includes ISO 15118. This option is a combination of a centralized design and a peer to peer design. This is schematically represented in **figure-9**. For readability, Certificate Provisioning Services and OCSP responders are left out of the figure.

This design consists of:

- Certificate Authorities
- PKI structure
- Certificate Pools and a Directory Service


V2G Root CA
(neutral party)
Roaming Hub 1
Sub CA 1
3.
Roaming Hub 2
Sub CA 1
2.
EMSP
Sub
CA 1
1.
OEM
Sub
CA 1
CSO
Sub
CA 1
List
List
CSO
Sub
CA 2
EMSP
Sub
CA 2
OEM
Sub
CA 2
CS
Manuf.
Sub
CA 2
EMSP
Contr.
Cert.
OEM
Prov.
Cert.
CS
Prov.
Cert.
EMSP
Contr.
Cert.
OEM
Prov.
Cert.
CSO
Cert.
CS
Cert.
CSO
Cert.
CS
Cert.
List
Directory service
for contract certificate pools
List
Directory service
for OEM certificate pools
A Contract certificate
pool
A OEM certificate
pool
Issues certificates
Can use & issue certificates

6.1. CENTRALIZED DESIGN

In this PKI design, one overall V2G Root CA is used (e.g. per continent as proposed in ISO 15118). In the centralized part of the design, on the left side of the figure, the Sub CA1 layer consists of Roaming hub based CA's, whereas the Sub CA2 layer consists of the individual organisations that can distribute their own certificates.

Please note that, as discussed in chapter 5, to keep the market easily accessible for new market participants, having at least one V2G Root CA from a neutral CA is required. This way, when a new roaming hub wants to enter the market, it only needs to get a SubCA certificate from that neutral V2G Root CA and its certificates can be used in the existing market. This setup thus provides a fair and open system in which new parties can access the market and makes it possible for parties in the EV market to switch from one roaming hub to another hub.

In the design in **figure-9**, the roaming hubs also fulfil the role of OEM Certificate pool and Contract Certificate pool since these are central functions. In this setup, parties on the SubCA 1 level can also fulfil the role of Certificate Provisioning Service, which works out well since roaming hubs are currently already trusted parties for EMSPs and CSOs.

One could imagine that roaming hubs might even provide a service for EMSPs to create certificates, so that EMSPs can choose not having to deal with this complexity ("outsourcing" of Contract Certificate creation).

6.2. PEER TO PEER DESIGN

In specific situations it could be possible that (e.g. larger) EMSPs, OEMs and CSOs do not want to be dependent on a roaming hubs. This option is drawn on the right side of **figure-9**, where the EMSPs, OEMs and CSOs are on the same level in the hierarchy as the roaming hubs. Due to the fact that Contract and OEM Certificates shall still be exchanged, this will result in a more peer to peer market.

FIGURE 9: design for an open PKI

6.3. OPEN PKI & PEER TO PEER - REQUIRED MEASURES

In an Open PKI where individual parties want to join as a separate SubCA, additional measures are needed to ensure inclusion and a level playing field.

EMSP

- Create and maintain their own Contract Certificate Pools
- Fulfil the role of CPS
- Setup a real-time connection to every CSO to give them access to this certificate pool
- Setup a connection to every OEM Certificate pool

OEM

- Create their own OEM certificate pools
- Make this OEM certificate pool accessible to all EMSPs

CSO

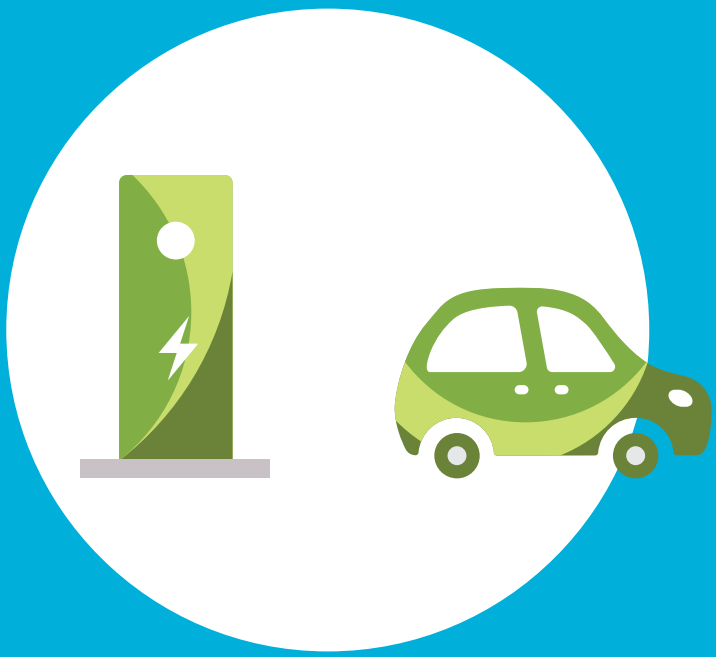
- CSOs should setup a connection to each EMSP Contract Certificate pool

---

This setup thus leads to peer to peer connections between:

- Each EMSP and OEM in the market and
- Each EMSP and CSO in the market.

Since maintaining a peer to peer connection will imply costs, it is up to the market parties to make a decision whether they choose a peer to peer setup or a centralized setup which also brings costs (e.g. subscription costs and / or transaction costs).



We invite **all stakeholders** to participate in the discussion and **co-create** an open and secure **smart charging system** for **all customers**.

7. KEY TAKEAWAYS

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. ElaadNL's 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.

KEY TAKEAWAYS

1. A Public Key Infrastructure (PKI) is a system for managing digital certificates that are used for securing digital communication.

2. The ISO 15118 model as discussed in this report adds EV user information to the EV charging ecosystem and can in this way be an enabler for Smart Charging. Even though providing this smart charging information is not mandatory for all scenarios in the ISO 15118 standard, this information should be made available to the EV ecosystem.

3. To be able to provide its functionality while remaining secure, ISO 15118 introduces some inevitable complexity to the EV charging ecosystem. One of the key elements of the security is a PKI.

4. Multiple PKI designs are possible, in this report we have presented an open PKI design, with the aim that industry players and market authorities engage in a discussion on the way forward.

5

A well-designed, open PKI can benefit all involved parties using ISO 15118:

- 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.

6

For an open PKI based EV ecosystem with ISO 15118:

- A neutral V2G Root CA is essential.
- Certificate pools need to be in place and accessible to all relevant parties. It is up to the market to decide whether a centralized of decentralized setup is preferable.

7

For an EV ecosystem including ISO 15118, additional market agreements are necessary for EV user related processes such as switching between EMSPs.

8

We invite all stakeholders to participate in the discussion and co-create an open and secure smart charging system for all customers.

APPENDIX

APPENDIX

REFERENCES

NO.	TITLE	AUTHOR
1	User Authentication for Electric Vehicle charging systems	ENCS
2	Stimulating the use of a PKI for the EV charging ecosystem	ENCS
3	VDE-AR-E 2802-100-1: 2017-10	VDE
4	ISO 15118 manual: mastering the Vehicle-2-Grid (V2G) Communication Interface	Dr. Marc Müllin
5	EV related protocol study	ElaadNL
6	15118-2: Road vehicles – Vehicle to grid communication interface – Part 2: Technical protocol description and Open Systems Interconnection (OSI) layer requirements	ISO
7	European Commission Competition Directorate (http://ec.europa.eu/competition).	European Commis-sion

TERMS & ABBREVIATIONS

TERMS	DEFINITION
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. (Source: Wikipedia)
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.

OCPP	Open Charge Point Protocol. Protocol between Charging Station and Charging Station Management System
OCSP	Online Certificate Status Protocol. A (Internet) protocol used for obtaining the revocation status of digital certificates (source: Wikipedia)
OICP	Open InterCharge Protocol. Roaming protocol of Hubject
OpenADR	Open Automated Demand Response. Protocol aimed at automating demand response communication, supporting a system and/or device to change power consumption or production of demand-side resources.
OSCP	Open Smart Charging Protocol. Protocol between DSO and CSO (or EMSP) for distributing available capacity.
PCID	Provisioning Certificate ID. ID of the OEM EV certificate.
PKI	Public Key Infrastructure
Roaming platform (RP)	Platform that allows EMSPs and CSO exchange information, among others for authorization.
Trust store	A repository of trusted (public) root-CA certificates that help to decide which certificates to trust when receiving data from a communicating device

We invite **all stakeholders** to participate in the discussion and **co-create** an open and secure **smart charging system** for **all customers**.

Contact
Utrechtseweg 310 B42
6812 AR Arnhem, The Netherlands
+31(0)26 31 20 223

info@elaad.nl
TW @ElaadNL
www.elaad.nl