

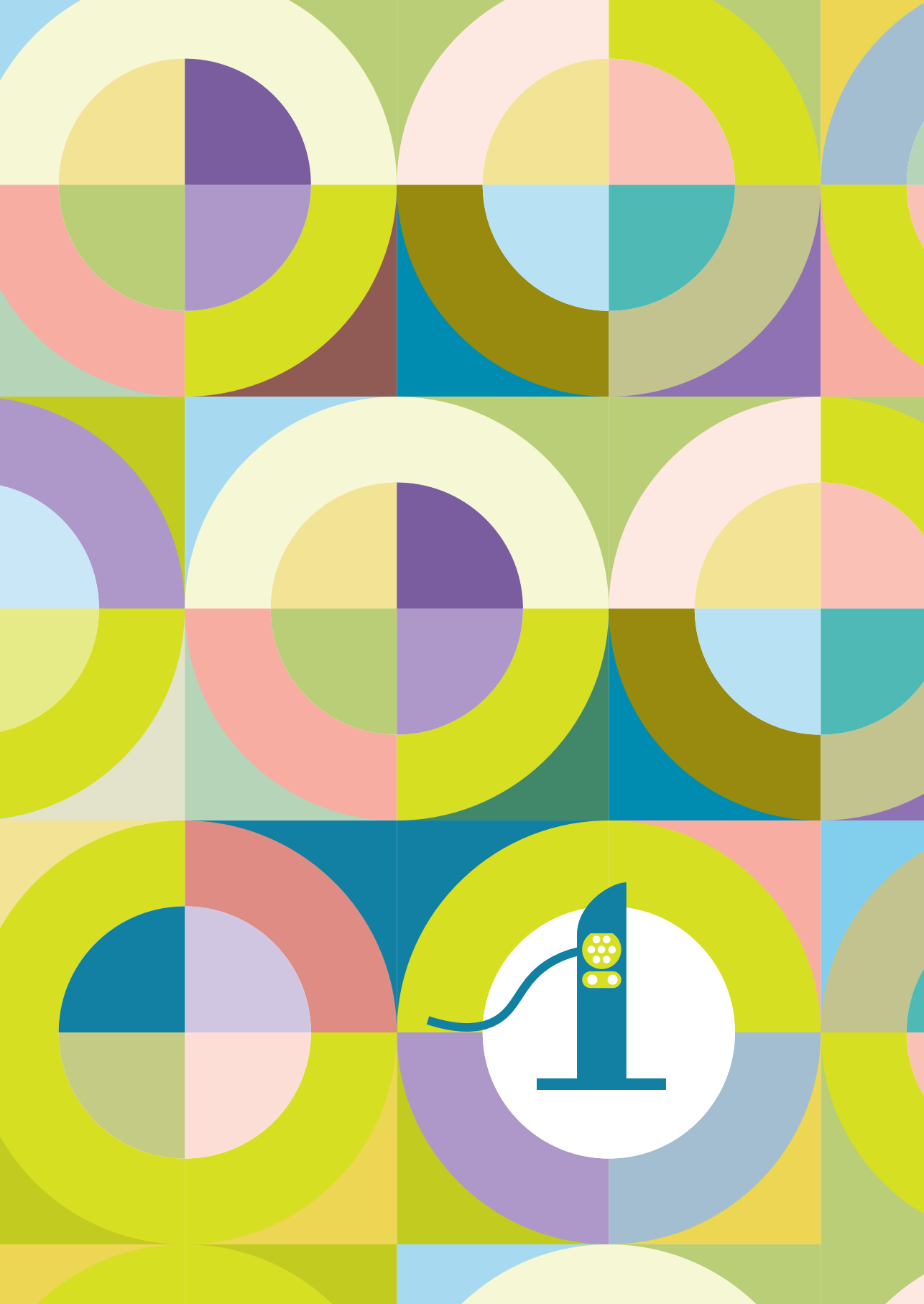
PUBLIC KEY INFRASTRUCTURE

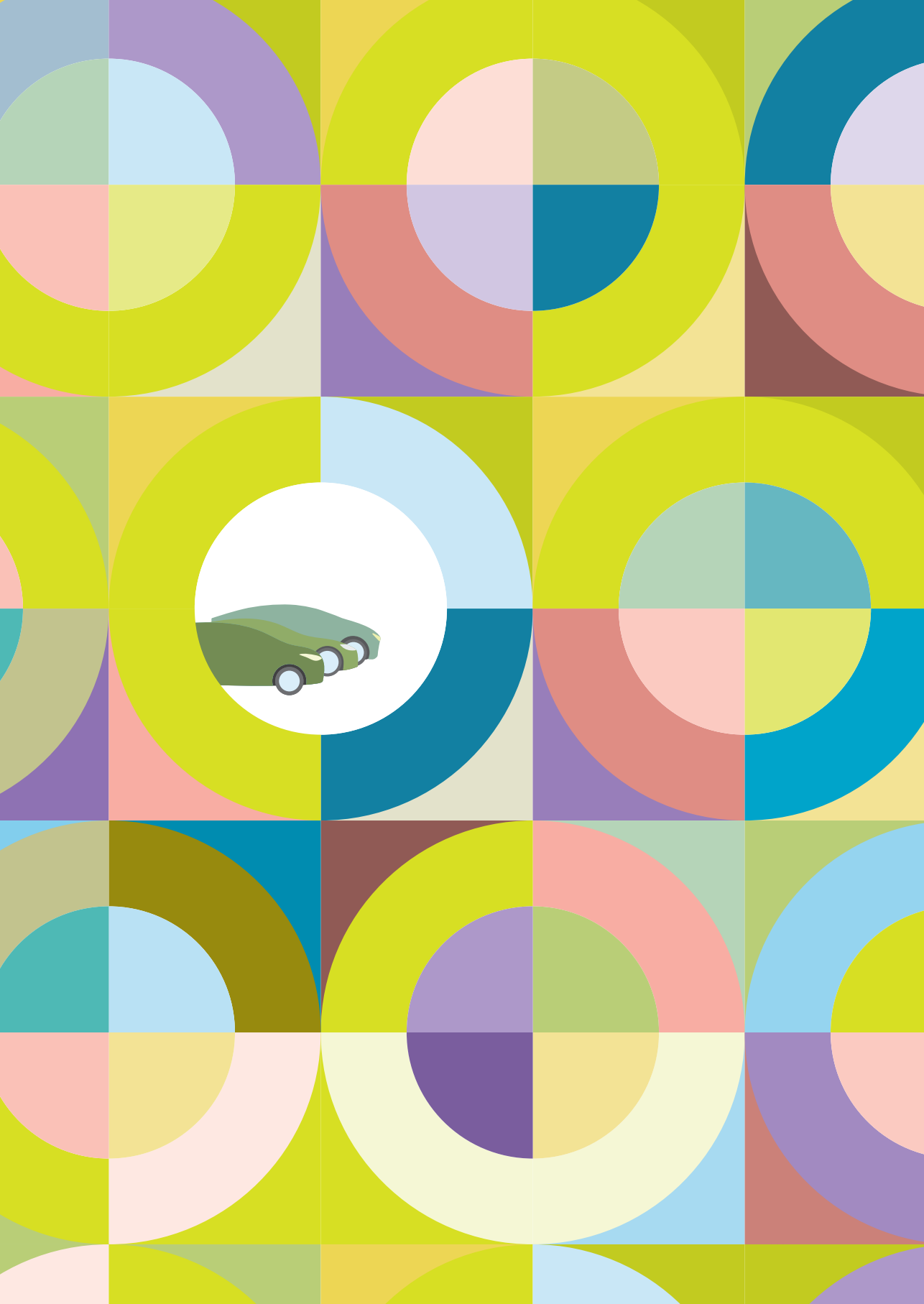
FOR ISO 15118

FREEDOM OF CHOICE FOR
CONSUMERS & AN OPEN
ACCESS MARKET

Elaadnl

The logo for Elaadnl is a teal circle containing the text 'Elaadnl' in white, with a yellow lightning bolt graphic under the 'nl'. The background of the entire page is a close-up photograph of an electric vehicle charging station, showing a black charging handle and a yellow charging cable. A network diagram is overlaid on the image, consisting of white circles connected by dashed white lines, with one teal circle at the top right containing the Elaadnl logo.







COLOFON

AUTHORS

Lonneke Driessen	ElaadNL
Paul Klapwijk	ElaadNL

PUBLICATION

Title	Public Key Infrastructure for ISO15118 Freedom of choice for consumer & an open access market
Date	May 1st 2022
Publisher	ElaadNL
Version	1.0
Copyright	ElaadNL, 2022

DESIGN & ILLUSTRATIONS

Marcel Nahapiet, nahapiet.com

CONTACT

ElaadNL
Westervoortsedijk 73
Gebouw KB, Industriepark Kleefse Waard (IPKW)
6827 AV Arnhem
+31(0)26 31 20 223

 info@elaad.nl

 [@ElaadNL](https://twitter.com/ElaadNL)

 www.elaad.nl



TABLE OF CONTENTS

PREFACE	XI
MANAGEMENT SUMMARY	XII
1. INTRODUCTION	3
2. FREEDOM OF CHOICE FOR CONSUMERS AND AN OPEN ACCES MARKET	9
3. MARKET DESIGN: ONE PKI OR MULTIPLE PKIs	12
3.1. Single PKI Design	12
3.2. A Multiple, interoperable PKI design	14
3.3. Relation with roaming	16
4. PURPOSE OF THIS PUBLICATION	18
PART-1	
5. INTRODUCTION	23
6. A LEVEL PLAYING FIELD IS THE BASIS FOR SUCCESS	25
6.1. A level playing field for OEMs and CSOs	25
6.2. A level playing field for OEMs and EMSPs	26
6.3. ISO 15118 - premium service or essential standard?	27
6.4. Freedom of consumer choice vs a monopoly	28
6.5. Involvement of the European Commission	28

7.	MARKET RULES FOR THE PKI ECOSYSTEM	31
7.1.	Market Rules for V2G Root CAs	33
7.2.	Market Rules for using Certificate Trust Lists	35
8.	MARKET RULES FOR A PKI	37
8.1.	Market Rules regarding an individual V2G Root CA	37
8.2.	Market Rules for PKI Pool Operators	40
9.	MARKET RULES FOR PKI PARTICIPANTS	43
9.1.	Market rules for CSOs	45
9.2.	Market Rules for EMSPs	46
9.3.	Market Rules for OEMs	48
10.	MARKET RULES FOR INTEROPERABILTY BETWEEN PKIs	51
10.1.	Cross Certification in combination with Pool Interoperability	54
10.2.	Trust List Mechanism in combination with Pool interoperability	55
10.3.	CSOs (and possibly EMSPs) join all PKIs in combination with Pool interoperability	57
11.	RECOMMENDATIONS	60
11.1.	Governance by an Independent European Authority	60
11.2.	Market Initiatives for V2G Root CAs	62

PART-2

12.	INTRODUCTION	69
13.	PKI INTEROPERABILITY FOR ISO 15118	72
13.1.	One V2G Root CA	72
13.2.	Multiple V2G Root CAs with Cross recognition	74
13.3.	Multiple V2G Root CAs with Cross certification	76
13.4.	Multiple V2G Root CAs with Certificate Trust List	77
14.	CROSS CERTIFICATION IN PRACTICE	79
14.1.	Cross certification explained	79
14.2.	Impact on existing implementations	90
14.3.	Technical issues encountered	108
14.4.	Impact of Cross Certification on hardware requirements	109
14.5.	Contract certificate chain verification	111
14.6.	Summary	112
14.7.	Recommendations	113
15.	CERTIFICATE TRUST LISTS IN PRACTICE	114
15.1.	Certificate Trust Lists explained	114
15.2.	Impact of the CTL on existing implementations	123
15.3.	Impact of the CTL on hardware requirements	129
15.4.	Summary	130
15.5.	Recommendations	131

16.	INTEROPERABILITY DISCUSSION	133
16.1.	PKI Interoperability using cross certificates	133
16.2.	PKI Interoperability using a Certificate Trust List	134
16.3.	Other PKI interoperability findings / further research	135
16.4.	PKI Pool Interoperability	137
16.5.	Topics besides providing interoperability	138
16.6.	Co-existing interoperability options	140
16.7.	Conclusion	142
16.8.	Recommendations	143

PART-3

17.	INTRODUCTION	149
18.	PKI QUALITY RULES	151
18.1.	Quality aspects of a PKI	151
18.2.	Requirements for applying quality rules	152
18.3.	Work in progress at CharIN	154
18.4.	Recommendations	154
	Terminology	158
	References	160
	Other publications in this series	162
	Appendix A: CTL ASN.1 format	166
	Appendix B: CTL Value Added Service	172



“

A succesful Public
Key Infrastructure
means a succesfull
roll out of ISO
15118



PREFACE

In 2018, ElaadNL published “[Exploring the PKI for ISO 15118 in the EV charging ecosystem](#)”. In this publication we had our first look at the ISO 15118 standard and shared our thought process on finding out how the standard works and how it could be incorporated in the EV market.

We also had a first look at the Public Key Infrastructure that is needed for digital security, and the consequences for the various roles in the EV ecosystem.

This new publication can be considered a follow-up, based on new developments in the market and new ideas that have come up over the last years since our previous publication. We have again attempted to explain our findings and shared our thoughts on how to successfully implement the ISO 15118 standard in the market, allowing all market players to participate, looking not only at the technological solutions for PKI interoperability, but also at the consequences for market governance and quality rules.

We have done our utmost, together with the participants of our demonstration projects, to give an accurate and complete overview of what we have learned. If the reader would find anything in this publication that could be further clarified or improved, please let us know, so we can improve future versions of this document or future publications around this topic. Please also do not hesitate to contact us and join the discussion on this topic!

MANAGEMENT SUMMARY

ISO 15118 is the upcoming standard for secure information exchange between electric vehicles, charging stations and Mobility Service Providers. With industry adoption increasing and legislators recommending and even considering mandating ISO 15118, it is very important to understand the implications of this standard.

ISO 15118 operates inside a Public Key Infrastructure (PKI) ecosystem, where market parties agree to work together. A PKI governing organization sets the terms of access, pricing, information exchange formats and audit procedures.

Therefore, the PKI that operates ISO 15118 not only handles the technical aspects, it also holds a powerful position in the market.



Canon of the PKI assessment

- 2018 ElaadNL's first demonstration of Charging using ISO 15118 & OCPP at the Global EV Charging Test in Arnhem. Publication "Exploring the PKI for ISO15118 the EV charging ecosystem V1.0"
- 2019 PKI conference in the Amsterdam Arena Second demonstration of charging using ISO 15118 at the CharIN Festival in Arnhem Interoperability testing of ISO 15118 at the Joint Research Centre (JRC) of the European Commission in Petten
- 2020 PKI interoperability demonstration using Cross Certification
- 2021 PKI interoperability demonstration using a Certificate Trust List
- 2022 Publication of this study " Public Key Infrastructure for ISO 15118 Freedom of choice for consumer & an open access market." Fall 2022: PKI interoperability demonstration on PKI Certificate Pool level

We would like to thank all our partners without whom we would not have learned what we know today.



There is a lot at stake in this strategic, growing market

The European Commission and many European Countries want to accelerate adoption of zero emission transport, want to protect consumers' freedom of choice and uphold fair and open access to the European market.

Large industries, such as Oil Companies, Utility Companies and OEMs, want to protect and expand their position in the energy and transport domain.

European, American and Asian industries are competing for the best starting point at home and abroad.

Startups and newcomers to the Energy and Mobility industry are highly motivated by the opportunities offered by this fundamental change.

Cooperation between all these stakeholders is paramount for successful transition to electric mobility that is centered around the European consumers.



This publication addresses **three main topics** related to a PKI, keeping in mind the expeditious transition to E-mobility, information security, consumer freedom and a level playing field for the industry.

Market Rules and Governance to ensure freedom for consumers

To ensure freedom for consumers, Market Rules and Governance must be put in place.

- **Consumers' freedom to select and change their E-Mobility Service Provider (EMSP)** at any time, regardless of their vehicle brand
- **Consumers' freedom to charge at any Charging Station**, regardless of their vehicle brand or their E-mobility Service Provider



Since 2015, Dutch EV drivers have enjoyed this freedom, being able to charge at any charging station, regardless of their Service Provider or vehicle brand. The open protocols OCPP and OCPI are the norm. This open approach was a key success factor in bringing the Netherlands where they are today: the country with the highest number of charging stations per inhabitant. It is clear that for Dutch EV drivers, there is no going back to closed systems.



Securing this consumer freedom whilst introducing ISO 15118 is possible and requires the effort and commitment of both industry and legislators. Part 1 of this publication describes the market rules that are needed to make this happen.

Market Rules and Governance to ensure a fair and open market for all market parties

Today the RFID card is the main method of EMSP contract identification. What will change with ISO 15118, is that the OEM needs to agree to the EMSP that a consumer selects. OEMs could themselves be in competition with these EMSPs, since OEMs are setting up EMSP services themselves (moving up the value chain).

This aspect of ISO 15118 means that non-OEM EMSPs are at a disadvantage. This is a market imbalance that can only be addressed through market rules and governance.

All in all, the market will enter a very competitive phase, where market players will venture up and down the value chain and where the size of a company matters when it comes to negotiations.

A market dictated by large companies or companies that operate - directly or indirectly - in multiple market roles is unlikely to provide the needed innovation, service and price pressure unless there are clear rules.

Ultimately, it is to be expected that OEMs and possible also large CSOs (owned by Utility Companies and Energy Companies that have direct access to prime locations, such as fueling stations) may become too dominant in the development of the e-mobility market which will in turn lead to a slower transition of the transport sector.

Again, introducing ISO 15118 in a level playing field is possible and also requires the effort and commitment of both industry and legislators. The market rules as described in part 1 of this publication will make this a reality.



Technical Interoperability

In this strategic, growing and international market, multiple PKIs will emerge. Not addressing PKI interoperability will result in multiple inoperable EV charging ecosystems, leading to compartmentalization of charging services. This is inefficient and frustrating for consumers.

For the technical solutions to work together there needs to be a standard way to implement the digital secure communication, both inside a PKI, as well as between separate PKIs. The technical options resulting in PKI interoperability are presented in part 2 of this publication and are the result of joint discussions, development and testing with many leading companies in the EV charging industry during the past 2 years.

Commitment of the EV Charging Industry and legislators to this technical part of PKI interoperability is needed for the sake of consumer freedom and a competitive market.



Quality Rules

For market parties to trust different PKIs and for PKIs to trust each other, there needs to be agreement on the individual PKI's Quality rules. These Quality Rules need to be defined clearly in the Certificate Policy and underlying audit requirements. This way, interoperability is achieved, whilst safeguarding consumer privacy, safety and digital security.

The topic of concrete and detailed PKI Quality Rules should be addressed at European Level, facilitating the cooperation between independent PKIs. Part 3 of this publication addresses the Quality Rules required for independent PKIs to trust each other.

Inclusivity of ISO 15118

ISO 15118 and the surrounding PKI technology is complex. Test events, test equipment and participation in PKI projects are expensive. To keep this technology inclusive, it is important to allow anyone to learn, develop, test and build ISO 15118 systems. ISO 15118 should not be a premium technology for an elite group of companies. Let ISO 15118 be accessible for everyone.

The way the PKI ecosystem for ISO 15118 will be defined, will determine the success and competitiveness of the European EV charging industry as well as the speed of the E-mobility transition. Shaping this PKI ecosystem is a joint effort of the industry and legislators and calls for investments on both sides.



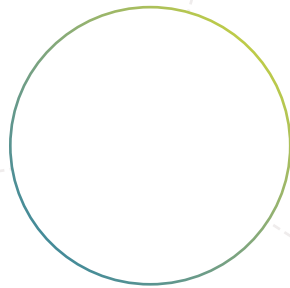


Inspired by: "Un dimanche après-midi à l'île de la Grande Jatte." Georges Seurat.

At the start of La Belle Epoque and the second wave of the industrial revolution. Redefining society, just like the energy transition today.

INTRODUCTION







1. INTRODUCTION

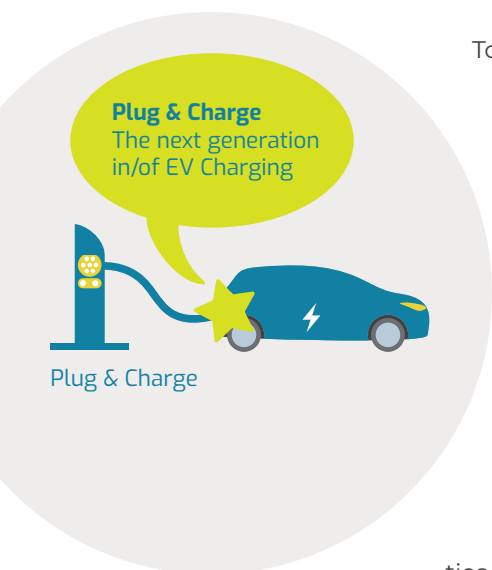
ElaadNL is the knowledge and innovation center in the field of smart charging infrastructure in the Netherlands. ElaadNL is a partnership of the Dutch grid operators who manage the Dutch electricity and gas networks. Through their mutual involvement in ElaadNL, the Dutch grid operators prepare for a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

Since 2011, The International Standards Organization (ISO) has worked on a new way of secure digital authentication and authorization for charging of electric vehicles (EVs), popularly called 'Plug & Charge' (PnC). By simply plugging in, EV drivers can identify themselves and start a charging session without the need of an RFID card or an app on their phone. The underlying technology is defined in the standard ISO 15118.

A 'digital certificate' is embedded inside the vehicle and takes over the function of the physical RFID card or other external identification means. When an EV driver plugs in at a Charging Station that is equipped to read these digital certificates, information exchange will be automatic and secure. The digital certificates are used to authenticate the contracting party, i.e. the owner or driver of the EV, to encrypt the information exchange and to digitally sign the data. But ISO 15118 is not only about

digital security and 'Plug&Charge', it also describes the way to exchange information between the EV and the Charging Station, enabling smart charging. This is very important with regard to energy management or demand response in the electricity grid.

This ISO 15118 standard is, at the time of writing of this publication, recommended by the **European Commission** (EC) to use in public tenders (see reference [STF-RECOMM]) and is recommended/mandated in some states in the US.



To enable this new method of authentication and transaction handling as defined in ISO 15118, a Public Key Infrastructure (PKI) is needed. A PKI is a set of roles, policies, and procedures needed to manage digital certificates and public-key encryption. All par-

“ Digital certificates enable authentication & smart charging

ties that participate in the PKI trust each other and can exchange digital information in a secure way. In 2017 the first EV came to the market that is equipped with 'Plug&Charge' technology based on ISO 15118 and there is already one PKI in operation for production EVs. It is expected that more PKIs will enter the market, given the developing nature of the EV charging industry, the multitude of players and the competitive and cross border nature of the industry.

Multiple independent PKIs

When there are multiple independent PKIs, by their very nature they will not be interoperable unless all PKIs mutually agree to 'trust' each other and agree on technical, operational and governance aspects of interoperation.

When these PKIs, their respective owners and participants are each other's competitors, they may be reluctant to cooperate, resulting in a plethora of independent, non-interoperable PKIs. This will lead to:

- **Consumer lock-in:** consumers can only use Charging Stations or only select E-Mobility Service Providers (EMSPs) that are part of the PKI of choice of their vehicle manufacturer
- **Competition lock-out:** PKI governing organizations have the power to exclude parties and new entrants from participating in the PKI or allow them to participate under unfavorable terms.

A neutral PKI system, that guarantees fairness, openness and a level playing field will require additional effort and commitment from the side of legislators and the industry. This is a joint effort between OEMs, Charging Station Operators (CSOs) and E-Mobility Service Providers (EMSPs) but also the Utility Industry (Grid Operators, Energy Suppliers and Balance Responsible Parties).

It is of course important that OEMs can trust the Charging Stations and Contract Certificates, but their dependency on the PKI is relatively limited compared to CSOs and EMSPs. CSOs and EMSPs are required to join the PKI, adhere to its rules, submit to its audits, pay the PKI fees and work with the systems performance.

What is sometimes overlooked, is that for Utilities, an open PKI infrastructure is essential too. Utilities operate critical infrastructure and the grid integration of electric vehicles in a secure manner is their top priority. Load balancing and bidirectional power flow (or V2X) are key to the transition to e-mobility. With the upcoming new version of ISO 15118, called ISO 15118-20, securing all communication to the vehicle with digital certificates is mandatory^a. When Utilities would want to access information needed for smart charging or Vehicle to Grid services (Energy Requested, Time of Departure, State of Charge, etc.) they need access to the PKI ecosystem.



A neutral PKI system, that guarantees fairness, openness and a level playing field will require effort and commitment

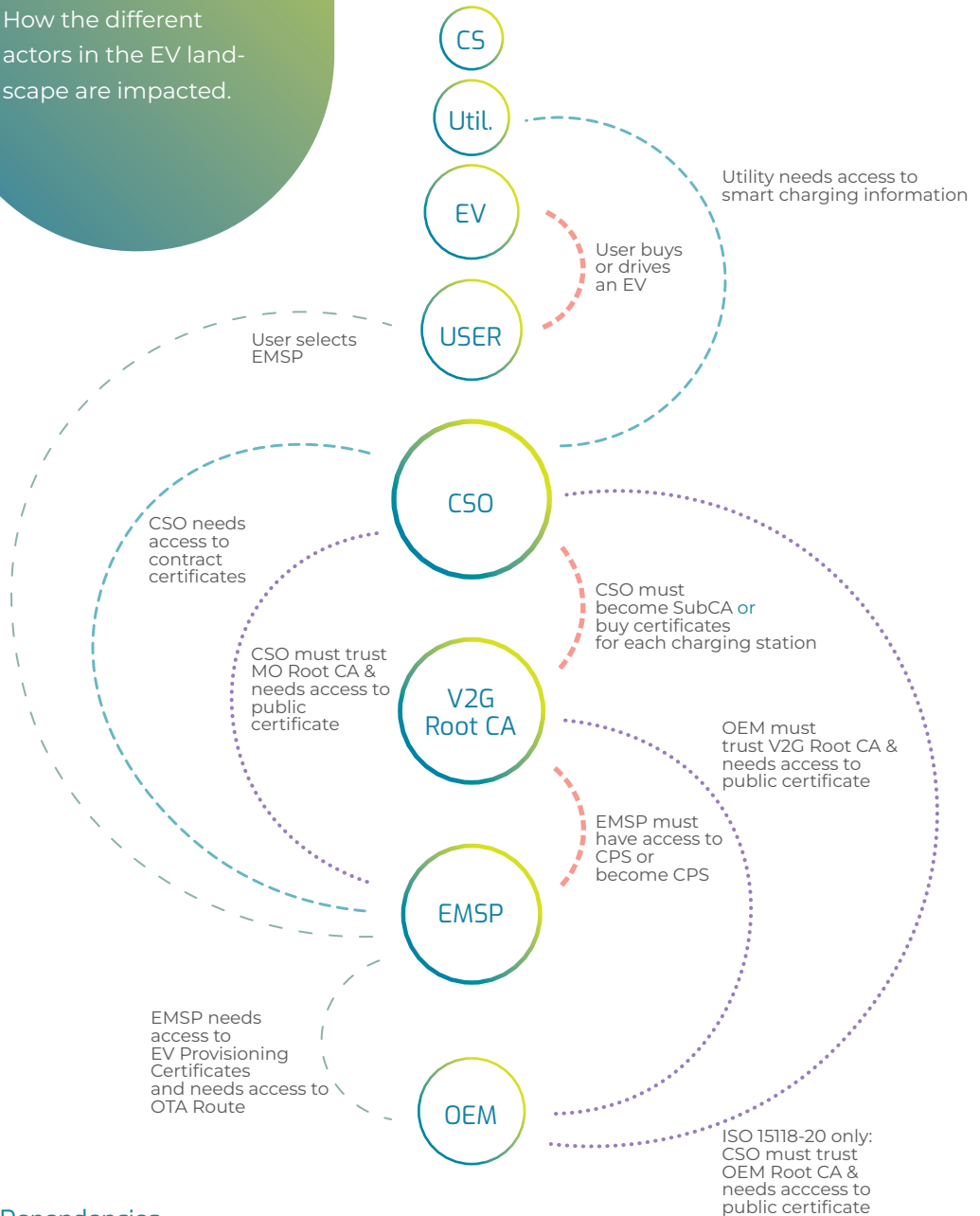
To illustrate the importance of a neutral PKI system for the different stakeholders in the EV market, the figure illustrates the dependencies.

Introducing ISO 15118 into the European e-mobility system affects all players and requires broad understanding of the matter and inclusive discussions on the best way to define the implementation in the market.

^a: In ISO 15118-2, the usage of digital certificates (Transport Layer Security (TLS)) was not mandatory for all functionality, in the ISO 15118-20 it is changed to be mandatory for all messaging.

Dependencies

How the different actors in the EV landscape are impacted.



Dependencies

Relative weight

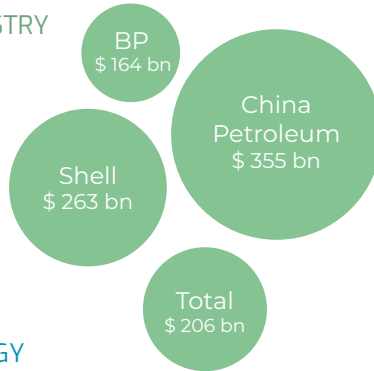
- - - - - Required to JOIN PKI / heavy dependency
- Required to TRUST PKI
- - - - - Access information
- - - - - Other dependencies

Landscape

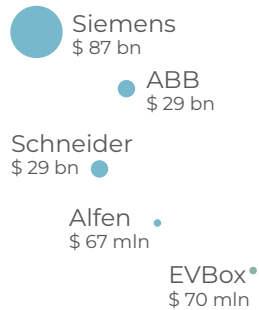
EV charging infrastructure

Some of the relevant actors, indication of annual revenue

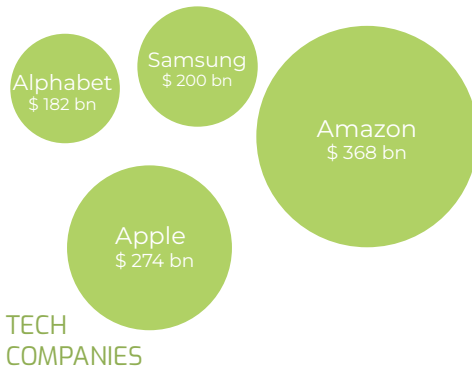
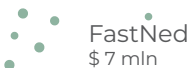
OIL INDUSTRY



ENERGY MANAGEMENT



STARTUPS UNICORNS DISRUPTERS

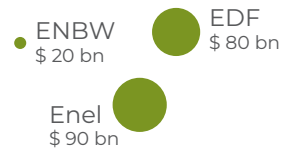


TECH COMPANIES

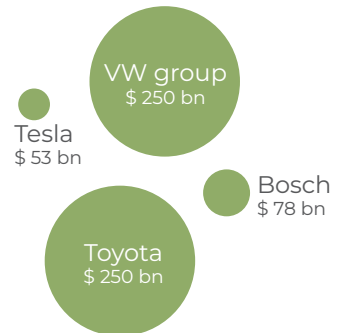
Many industries see business opportunities in this new EV charging market.

It is yet to be seen how this will play out between familiar faces from the different corners of the landscape & new entries and disruptors in the market.

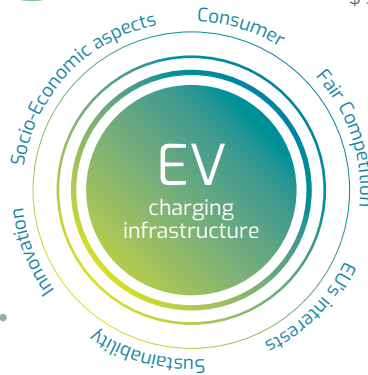
UTILITIES



FINANCIAL INSTITUTIONS




AUTOMOTIVE



2. FREEDOM OF CHOICE FOR CONSUMERS AND AN OPEN ACCESS MARKET

While the technical framework for a PKI is described in the ISO 15118 standard, complemented by the VDE application rule^p, further measures are needed in order to achieve interoperability, freedom of choice for consumers and a level playing field for market actors like EMSPs, CSOs, Utilities and OEMs:



A collaborative business ecosystem will benefit all

Market Rules and Governance. Part-1

To protect consumers and to protect the open access market, market rules need to be put in place and the market needs to be monitored by a regulatory body. Part 1 of this publication describes in detail the proposed approach for Market Rules and Governance of an Open PKI system.

^p: The VDE Application Rule describes a number of technical topics are not described in the ISO 15118 standard itself, but are needed to setup an ISO 15118 ecosystem.

Technical interoperability between PKI's. Part-2

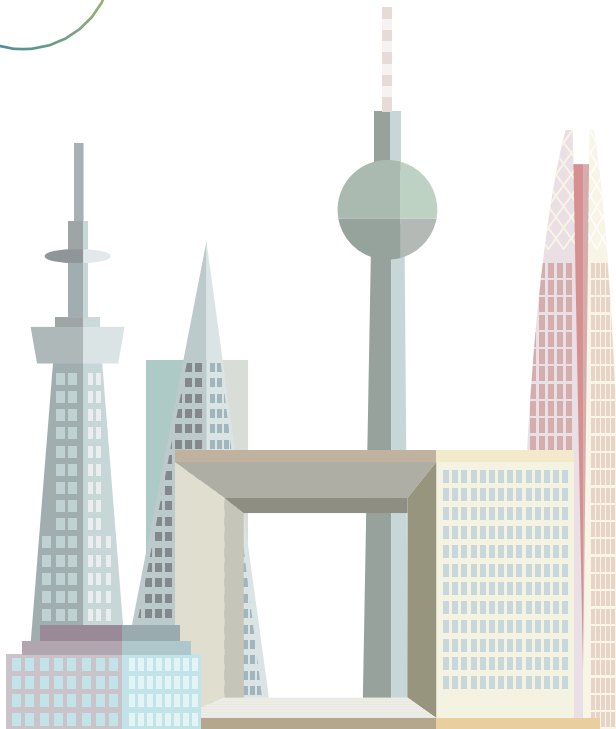
For the technical solutions to work together there needs to be a standard way to implement the digital secure communication. This applies to the interoperability inside a PKI, as well as interoperability between separate PKIs. Part 2 of this publication describes in detail the results of the ElaadNL project and proposed approach for 'Intra-PKI'- and 'Inter-PKI' interoperability for an Open PKI system.

Detailing Quality rules for PKIs. Part-3

For market parties to trust different PKIs and for PKIs to trust each other, there needs to be agreement on the individual PKI's Quality rules, stated in the Certificate Policy and underlying audit requirements. Part 3 of this publication describes in more detail the proposed Quality Rules for an Open PKI system and the ongoing work to date. These rules need to be in place and accepted by all market participants.

Regardless of the way the market is organized - one PKI or multiple PKIs - in all cases quality rules, interoperability rules, market rules and independent governance are essential to ensure freedom of choice for consumers as well as open access and a level playing field for market actors.

Regardless of the way the market is organized, in all cases quality rules, interoperability rules, market rules and independent governance are essential



3. MARKET DESIGN: ONE PKI OR MULTIPLE PKIs

The interoperable Public Key Infrastructure for E-mobility can be designed as a single PKI system or as a multiple PKI ecosystem. This market design can evolve over time; for example the market can start off with only one PKI and new PKIs can emerge at a later stage. The market design can also differ in different regions in the world, for example in Europe, in North America or Asia.

It is important to note that this document does not address the market design with multiple, non-interoperable PKIs: while this design is not unrealistic, it does not ensure freedom of choice for consumers, nor open access and a level playing field for market actors. It is therefore not an acceptable market design, particularly in the European context of free movement of services, goods, money and people.

3.1. Single PKI Design



In this set-up, all market players (CSOs, EMSPs, OEMs) join one and the same PKI, that enables interoperability by default. If market players do not join this PKI, they are not interoperable with the rest of the market with regards to the ISO 15118 functionalities.

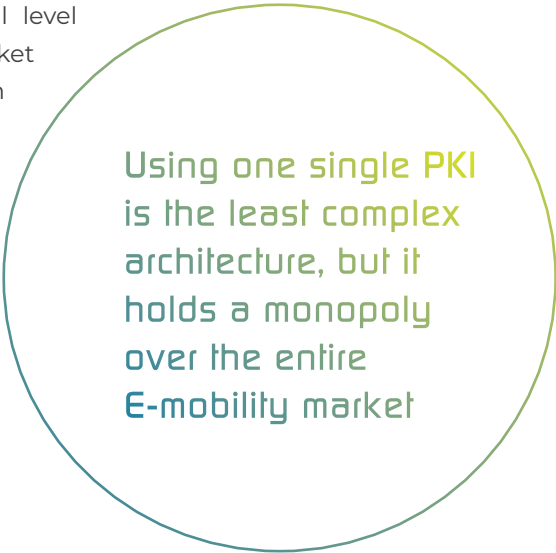
A distinction can be made between owning, governing the PKI and operating the PKI. In this document, the definitions are:

- **Owning** – company owning the actual Root CA private key and certificate.
- **Governing** - deciding on the procedures, conditions for operating and allowing access to the PKI, e.g. participant determining audit requirements
- **Operating** – doing the actual technical work for creating and distributing certificates, auditing participants and, in the case of ISO 15118, hosting certificate pools.

Within this single PKI design, there are several nuances regarding:

- A** One single PKI that is owned, governed and operated by a **commercial organization** (owned by market parties)
- B** One single PKI that is owned, governed and operated by an **industry association** (a non-profit organization that consists of a subset of the market parties)
- C** One single PKI that is owned, governed and operated by a **governmental agency** (that answers to for example the European Commission)

Using one single PKI is the least complex architecture on a technical and organizational level and in that respect is an attractive market design. The issue with this market design is that the single PKI holds a monopoly over the entire E-mobility market. It holds disproportionate power regarding for example participation contract terms, prices, operational performance, technical aspects and dispute resolution. Additionally, it makes the PKI vulnerable to accusations and legal action with regards to market power abuse.



This monopoly position will need to be surrounded by a framework of Market Rules and Governance by a Governmental Agency, addressing industry and governmental unease. Still, it is unlikely that all market players and legislators will agree on one PKI and additional PKIs are bound to surface. At the time of publication of this document, already 4 V2G Root CAs were aiming to operate in the European market. To ensure freedom of choice for consumers and open access and a level playing field for market actors, interoperability between these PKIs is needed.

3.2. A Multiple, interoperable PKI design

In a market where several PKIs are active, it is still possible to achieve interoperability through one of **three mechanisms**:

- 1 Cross Recognition:** multiple PKI's exist in the market. Everybody agrees that all PKIs are "trusted". A design for an ISO 15118 ecosystem based on this mechanism could require a subset of the market players to join all PKIs, whereas the rest of the market could only join one PKI. More details of this interoperable design are explained in Part 2.

There are two additional designs that do allow market parties to only join one PKI and still be interoperable with the market parties that join other PKIs:

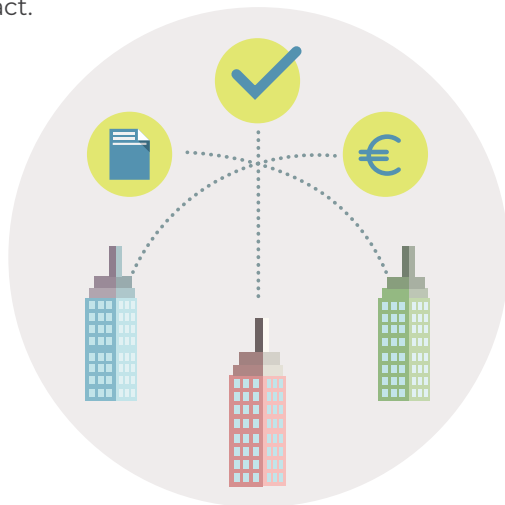
- 2 Cross Certification:** Multiple PKI's agree to cooperate, using the interoperability mechanism of 'cross certification' (see Part 2). Interoperability is handled by a technical mechanism where parties from different PKIs (often the Root CAs) set-up a technical trust relation.

- 3 Certificate Trust List:** Multiple PKI's agree to cooperate, using the interoperability mechanism of a 'certificate trust list' (see Part 2)



All of these multi PKI market designs introduce more complexity on the technical and organizational level. In Part 2 of this publication we will show the technical impact.

In all cases, when multiple PKIs work together, market rules and governance to ensure an open and fair market (see Part 1) and quality rules for PKIs to trust each other (see Part 3) are required.



3.3. Relation with roaming

In the current EV market, information exchange is needed between CSOs and EMSPs to authorize and (financially) settle charging sessions. This “roaming” is currently done peer to peer and via roaming hubs. The discussion of the open and interoperable PKI is an independent topic of the freedom of EMSPs and CSOs to engage in roaming agreements. A more detailed explanation is given below.

Authentication and authorization

Authentication is currently based on the identifier of the contract, often the contract id or the identifier of the RFID card of an EV user that belongs to the contract. When using the Plug & Charge functionality from the ISO 15118 standard, the RFID card is replaced by a digital certificate.

When using ISO 15118, the following complementary methods for authorizing the contract in case of roaming are possible:

1. Check the ISO 15118 **E-Mobility Account Identifier** (EMAID) that is included in the digital certificate.
2. Check the **entire contract certificate** from the EV

The most logical option seems to use the first option at the CSMS, using the EMAID or contract identifier, making the actual roaming setup similar to the current roaming market (and the second option preferably already in the Charging Station). When a contract for an EV user is created by an EMSP, it should prepare the contract certificate, send it to one or more contract certificate pools and add the contract identifier to one or more roaming hubs or make this contract identifier available via the EMSP peer to peer roaming connections.

Exchanging metering information from the EV

The ISO 15118 standard has a “metering receipt (ISO15118-2) / confirmation (ISO15118-20)”: a signed message related to metering. The purpose of the

standard is to use this message for billing, implying that this message should also be exchanged with the EMSP. Therefore, this message could lead to an extension of the current roaming functionality of roaming hubs or additions to peer to peer roaming protocols. Since this ISO 15118 message is signed by the EV using the private key belonging to the Contract Certificate (that the EMSP originally created), the EMSP can validate this message without further exchange of certificates.

This metering receipt thus boils down to additional information that has to be sent from the CSO to the EMSP and can therefore be combined with the currently exchanged data between these roles for settling a charging session, a charge detail record.

Both the authorization as well as the exchange of additional metering information could impact existing roaming solutions, but do not add a dependency between the roaming hub and the PKI infrastructure. CSO's and EMSPs are can choose a PKI and roaming solution independent of each other, provided that the roaming solution supports the ISO 15118 related information described above. Of course, central roaming hub solutions and solutions for ISO 15118 certificate pools could be combined as a "one stop shop" for EMSPs and CSOs (as a commercial proposition).



4. PURPOSE OF THIS PUBLICATION

This publication addresses the three main issues related to a PKI that must be resolved to enable a competitive e-mobility market that serves the European consumers:

- Part 1** **Market Rules and Governance** to ensure a fair and open market
- Part 2** **Technical Interoperability** within a performant system
- Part 3** **Quality standards** to safeguard consumer privacy, safety and digital security.

At the time of writing of this publication, several initiatives have addressed or are addressing the topic of an open, fair and consumer-centric PKI ecosystem for E-Mobility:

- The European Commission has set up a Sustainable Transport Forum sub-group on governance and standards for communication exchange in the electromobility ecosystem. *“The main focus of the sub-group shall be the development of a governance structure and, to propose an implementation strategy for the operation of a public key infrastructure (PKI), or similar IT solution, that allows an open, single, secure and economically efficient management of the digital communications between the electric vehicle and the recharging infrastructure.”*
- A CharIN[®] PKI Task Force has developed a “Recommendation for a Certificate Policy for an ISO15118 PKI (2020-08-06)”.

[®] CharIN is an Industry association dedicated to promote interoperability based on the Combined Charging System (CCS) as the global standard for charging vehicles of all kinds, supporting ISO 15118 as the standard between EV and Charging Station.

- A CharIN PKI Task Force is developing a Use Case based interoperability document: *“The interoperability document will describe use cases of the communication flow from all actors involved in the PnC environment. On this baseline requirements will be defined in order to manage multiple Root CA’s and certificate distribution and data exchange.”*
- CharIN has started a project for a new PnC Market Implementation *“The goal of project “Plug and Charge Europe” is to set up the Public Key Infrastructure (PKI), a technology needed to enable secure authentication and authorization via digital certificates in accordance to ISO 15118, with CharIN as operator and provider of required services. CharIN as neutral and international authority shall ensure the fair, open and non-discriminatory operation of the PKI across all stakeholders and thus successfully overcome previous hurdles in the Plug and Charge implementation.”* Charin has published its Terms *“CharIN PnC Terms & Conditions”*, describing the Market Rules for it’s V2G Root CA and its PKI participants.

ElaadNL is contributing to all these initiatives and aims with this publication to support the discussions:

- Provide an overview and update regarding the Open PKI for ISO 15118 to all e-Mobility Stakeholders, including the hundreds of Legislators, Policy Makers, Security Experts, CSOs, EMSPs, Utilities and many more that are not active inside the above mentioned initiatives
- Share the findings of the PKI Interoperability Project of Korean, German, French, Israeli and Dutch market parties
- Share the recommendations we have identified

We have learnt that there is already broad consensus that an open and interoperable PKI ecosystem is the way forward. We hope that the next three parts of this publication, describing Market Rules and Governance, Technical Interoperability and Quality Rules, will assist legislators and the industry in their discussions and implementations.



Inspired by: "Bauhaustreppe", Oskar Schlemmer.

The Bauhaus school of design gave birth to the modernist movement and had an profound impact on design as a whole and society world wide. Perhaps much like the energy transition can have in bringing forth the new.



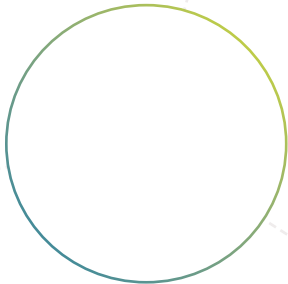
PART I

MARKET RULES

Ensuring freedom of choice for consumers as well as open access and a level playing field for market actors.



A proposed draft of
European market
rules and governance
for an open PKI





5. INTRODUCTION

The purpose of this part of this document is to present a first draft of European market rules and governance for an open PKI, ensuring freedom of choice for consumers as well as open access and a level playing field for market actors.

General legislation regarding consumer protection and industry competition is already in place in Europe. In the emerging field of e-mobility this could be translated to:

- **Consumer freedom to select and change the E-mobility Service Provider** (EMSP) at any time, regardless of the brand, origin or original destination of the vehicle
- **Consumer freedom to charge at any Charging Station**, regardless of the vehicle brand or the E-mobility Service Provider

- **Consumers are informed upfront about the tariff of charging** at any charging station. This is the tariff the E-mobility Service Provider will bill towards the EV driver. All tariffs shown towards the consumer must be understandable and without hidden cost.
- **Market access under fair, reasonable and non-discriminatory** conditions for all market parties

Given the specific nature of the PKI for ISO 15118, the above mentioned general rules can be made more explicit.

In this document, a first summary of market rules is outlined. Before we go to the proposed market rules, the next paragraph gives an additional explanation on the need of these market rules.

6. A LEVEL PLAYING FIELD IS THE BASIS FOR SUCCESS

ElaadNL believes there are several important reasons why – with the introduction of ISO 15118 - market rules and governance are of the utmost importance.



6.1. A level playing field for OEMs and CSOs

In the current ISO 15118 setup OEMs determine what PKI a Charging Infrastructure Provider must join before their drivers can charge at that Charging Station. It can be expected that OEMs will want the maximum availability of Charging Stations for their drivers (lack of charging facilities is an impediment to e-mobility adoption). However, at the same time the OEM selects the PKI and determines its terms and conditions. Since OEMs are always larger companies than Charging Station Operators (CSOs), most CSOs have no negotiating power.

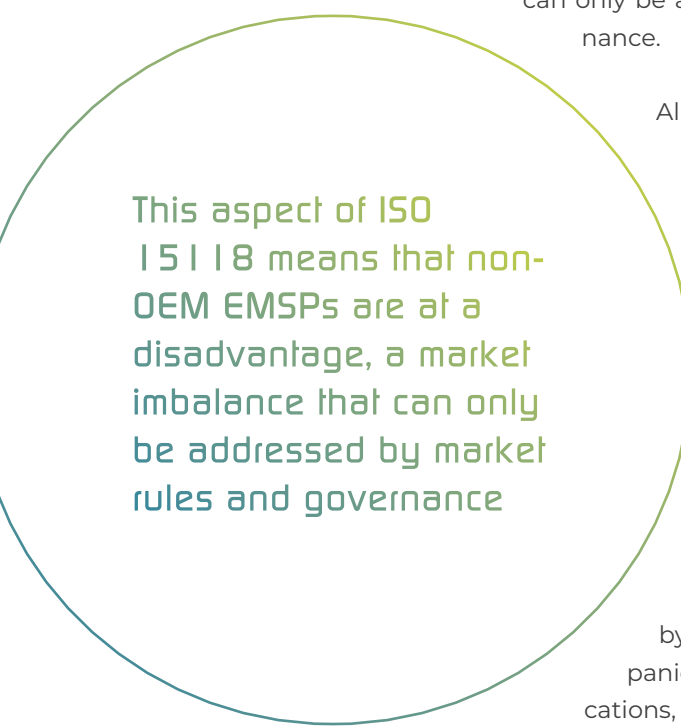
OEMs are investing in their own Charging Infrastructure (moving up the value chain) and play the role of CSO. They may want to give discounts and privileges to consumers that drive their vehicle brand by means of favoring a certain EMSP that is owned or preferred by the OEM (e.g. cheap Plug & Charge (PnC) service from this EMSP combined with uncompetitive pricing for direct payments). Consumers that want to

charge with a competing vehicle brand should have access under fair and reasonable conditions, particularly when the infrastructure is in the public space and concessions are involved. What is fair and reasonable can be neutrally agreed in market rules and governance.

6.2. A level playing field for OEMs and EMSPs

Unlike today, with the RFID card being the main method of EMSP contract identification, when using ISO 15118 the OEM will need to agree to the EMSP that a consumer selects (by providing the OEM provisioning certificate to that EMSP). OEMs could themselves be in competition with these EMSPs, since OEMs are setting up EMSP services themselves (moving up the value chain). This aspect of ISO 15118 means that non-

OEM EMSPs are at a disadvantage, a market imbalance that can only be addressed by market rules and governance.



This aspect of ISO 15118 means that non-OEM EMSPs are at a disadvantage, a market imbalance that can only be addressed by market rules and governance

All in all, the market will enter a very competitive phase, where market players will venture up and down the value chain and where the size of a company matters when it comes to negotiations. A market dictated by large companies or companies that operate - directly or indirectly - multiple market roles will, without clear rules, very likely not provide the needed innovation, service and price pressure. Ultimately, most probably the OEMs and possible also large CSOs (owned by Utility Companies and Energy Companies that have direct access to prime locations, such as fueling stations) may become

too dominant in the development of the e-mobility market which will in turn lead to a slower transition of the transport sector.

6.3. ISO 15118 - premium service or essential standard?

Some parties could argue that ISO 15118 should be regarded as a premium service and therefore does not have to adhere to open access for all market parties. This position is however incompatible with the position by parties that ISO 15118 should be mandated as a European standard in the Alternative Fuels Infrastructure Regulation, and the fact that it is included in the European Commission Sustainable Transport Forum recommendations for public tenders for charging infrastructure.

ISO 15118 is regarded by ElaadNL as an essential standard, not only because it offers improvements regarding digital security and information needed for smart charging. It also provides – with the upcoming ISO 15118-20 version, which is to be released in 2022, the basis for interoperable Vehicle to Grid systems, energy management and wireless charging systems. We believe those services are not premium, but basic. Therefore, the ISO 15118 functionality of EVs should not be regarded as a premium service that may be used by the OEMs to their competitive advantage.



6.4. Freedom of consumer choice vs a monopoly

One could argue that it is eventually in the interest of all parties to operate in an open market, since consumers will favor companies that offer them freedom of choice.

In the Netherlands, an EV driver owns a specific vehicle for an average of four years. Therefore, during those four years the EV driver is dependent on the OEM's choices regarding the PKIs it connects to. During those four years, if no market rules are put in place, the OEM controls which EMSPs (if any) and what Charging Stations the customer can select. In that sense the OEM has a monopoly.

6.5. Involvement of the European Commission

As mentioned in the introduction to this document, the European Commission has set up a Sustainable Transport Forum sub-group on governance and standards for communication exchange in the electromobility ecosystem. The purpose of this sub group is to advise on a governance framework that allows an open and secure management of the digital communications between the electric vehicle and the charging infrastructure.



EC sub group to create a governance framework

To support this work, the next chapter introduces the market rules that we think are needed for an open and secure EV ecosystem incorporating the ISO 15118 standard.



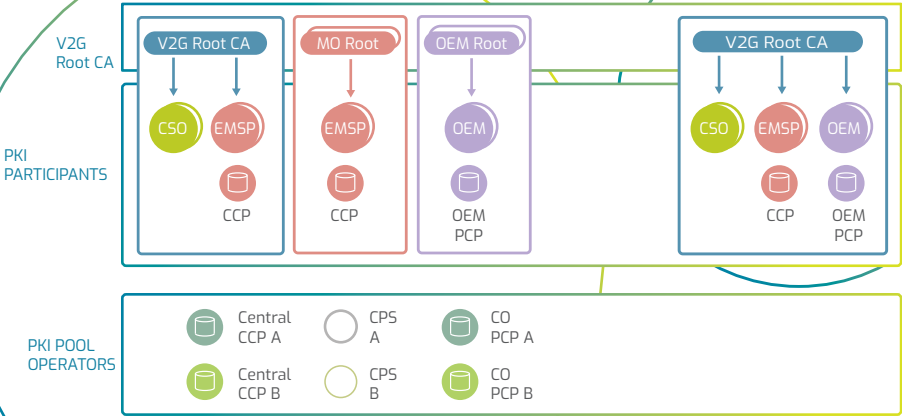
PKI ECOSYSTEM

Trust List manager



PKI

PKI



CCP: Contract Certificate Pool
 PCP: Provisioning Certificate Pool
 CO PCP: Central OEM PCP

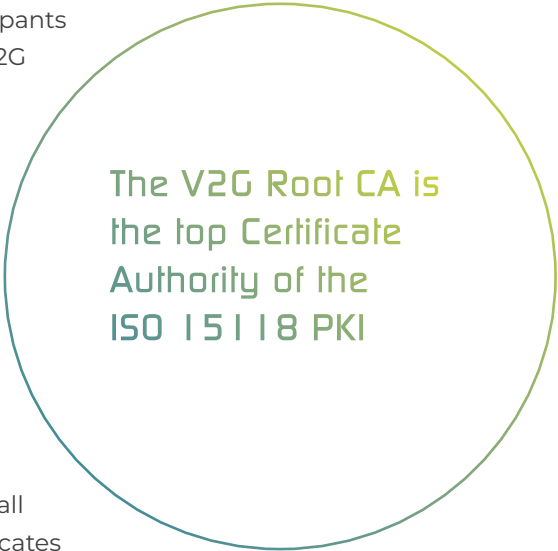
ISO 15118
 operates inside
 a Public Key
 Infrastructure
 ecosystem

7. MARKET RULES FOR THE PKI ECOSYSTEM

ISO 15118 operates inside a Public Key Infrastructure ecosystem, as shown in the figure on the previous page. A PKI ecosystem consists of multiple PKIs that interoperate using either a cross certification- or a Trust List mechanism.

A PKI consists of one V2G Root CA, PKI participants that use/accept certificates derived from this V2G Root CAs and one or more Pool Operators that assist with central pools and a CPS service and optionally directory service(s).

The V2G Root CA is the top Certificate Authority of the ISO 15118 PKI and the trust anchor for most certificates in the ecosystem.



PKI participants include:

- **CSOs**, that are mandated to either be a Sub CA to a V2G Root CA or purchase all their individual Charging Station Certificates from a Sub CA.
- **EMSPs** that can choose to be:
 - **A Sub CA** to a V2G Root CA or purchase all their individual Charging Station Certificates from a Sub CA

- Or function as an **independent Certificate Authority** (MO Root CA). In the latter case, the individual Contract Certificate bundles need signing by a CPS that is derived from the V2G Root CA.
- **OEMs**, that can choose what V2G Root CA s to trust and therefor can choose which CSOs and EMSPs to trust

PKI Pool Operators support the V2G Root CA by offering Central Pools:

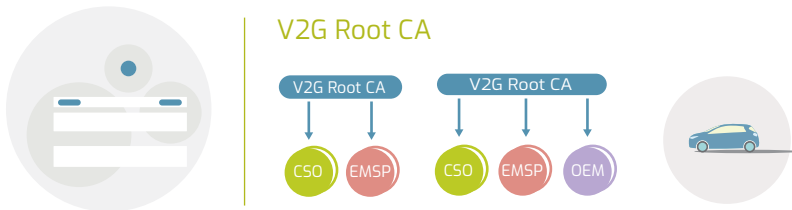
- Central Contract Certificate Pools that enable CSOs to check for Certificate updates **more efficiently**
- **Central OEM Provisioning Certificate Pools** to enable EMSPs to construct Contract Certificates more efficiently

PKI Pools can be operated collectively (Collective Pools) by independent parties (such as Roaming Platforms) or they can be operated by individual EMSPs or OEMs (Market Party Pools).

The nature of the ISO 15118 standard dictates some specific requirements, that in turn require specific market rules: regarding consumer choice, EMSP access, CSO access and access of new V2G Root CAs. In order to have an open ISO 15118 ecosystem, the paragraphs below describe rules that we think are essential and should be introduced market wide.

7.1. Market Rules for V2G Root CAs

In the European market there could be one V2G Root CA or there could be several V2G Root CAs that interoperate. A Trust List Manager governs the list of trusted V2G Root CAs, trusted by all parties within the individual PKIs.



Multiple V2G Root CAs that do not interoperate will limit the freedom of choice for consumers to charge where they like, using the EMSP of their choice and regardless of their vehicle brand.

A single or dominant V2G Root CA holds the monopoly over all European CSOs, regarding for example participation contract terms, prices, operational performance, technical aspects, and dispute resolution.

Accreditation and monitoring of V2G Root CAs at a central European Level will guarantee V2G Root CAs Quality Standards and a fair, open and interoperable PKI ecosystem.

Multiple V2G Root CAs that do not interoperate will limit the freedom of choice for consumers

The following market rules should therefore be set at the EU level

- 1 **Accreditation of a V2G Root CA** is done by an independent authority (such as the EU Agency for cybersecurity (ENISA), mandated by the EU Cybersecurity Act (CSA))
- 2 All eligible V2G Root CAs must comply with **European Standard Quality Requirements** for PKI implementations. ♦
- 3 These requirements are:
 - Transparent (public)
 - Based on security standards that are mandated by law
 - Set by an independent authority (such as the EU Agency for cybersecurity (ENISA), mandated by the EU Cybersecurity Act (CSA))
- 4 This conformity declaration is provided by an **independent auditor**
- 5 The accreditation of this auditor is **independent at EU level**

Since it is to be expected that more V2G Root CAs will be set up in future, there should also be Market Rules in place that guarantee a fair treatment for these new V2G Root CAs that want to interoperate with another (dominant or established) V2G Root CA.

- 6 All eligible **V2G Root CAs must support interoperability** mechanisms, if multiple V2G Root CAs emerge in the European market, ♦
 - By participating in the European Trust List
 - By facilitating Cross Certification

7.2. Market Rules for using Certificate Trust Lists

When using a Certificate Trust list, a number of specific market rules are applicable concerning the processing of this list. In short, once a Certificate Trust List is accepted in the market, all Root CA certificates on the list should be considered as the Root CA of trusted PKIs. More specifically, the following rules apply:

- 7 The Trust List Manager is **governed by an independent authority** (such as the EU Agency for cybersecurity (ENISA), mandated by the EU Cybersecurity Act (CSA))
- 8 There are **uniform** Trust List **Admission** Rules for V2G Root CAs
- 9 The Trust List Manager must make the Certificate Trust List (CTL) **available to all** market parties participating in one of the PKIs.

◆ Rule is part of CharIN PnC Terms & Conditions 2022-02-08.
All relevant rules on the subsequent pages are indicated with the same icon



8. MARKET RULES FOR A PKI

A PKI consists of a V2G Root CA, PKI participants (OEM, EMSP and CSO) and PKI Pool operators (either centralised or operated by Individual OEMs and EMSPs). The market rules a PKI should set to offer an open and fair PKI.



8.1. Market Rules regarding an individual V2G Root CA

Any V2G Root CA has a dominant position towards market parties. The V2G Root CA decides who can become a Sub CA, what the qualification criteria are and what fees need to be paid. Therefore, the following market rules should apply:

- 10** V2G Root CAs may **only demand reasonable security requirements** and no additional non-security related requirements which are defined in its Certificate Policy (CP) to candidate Sub Cas. ♦

- 11 These requirements stated in the **Certificate Policy** are:
- Transparent (public)
 - Based on security standards that are mandated by law
 - Monitored by an independent authority (such as the EU Agency for cybersecurity (ENISA), mandated by the EU Cybersecurity Act (CSA))
- 12 V2G Root CAs can only ask Sub CAs for **demonstrable** conformity to acceptance criteria
- 13 This conformity declaration is provided by an **independent auditor**. ♦

To ensure a level playing field for all market parties (established and new, large and small) all market parties should be granted access to any PKI.

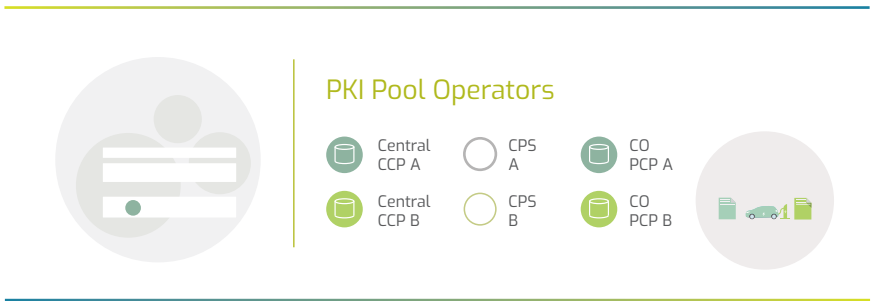
- The EMSPs need to have access to the consumers' specific EV certificate that is generated by the OEM (the OEM EV Provisioning Certificate). An EV will only accept the EMSP contract when the private key of the EMSP contract is encrypted with this specific EV certificate. Since OEMs store their OEM EV Provisioning Certificates into a 'Pool' that is part of the PKI, any PKI should provide open access to all EMSPs that want to join.
 - The consumer will only be able to charge its EV and use its EMSP contract when a CSO has embedded the PKI's V2G Root Certificate on its Charging Stations and installs a certificate derived from that V2G Root CA. Therefore, any PKI should provide open access to all CSOs that want to join.
- 14 The V2G Root CA shall **provide the V2G Root CA Certificate service** upon request to any CSO, EMSP and OEM as long as they meet the Certificate Policy requirements. ♦

- 15 The V2G Root CA shall **ensure access** to the Certificate Provisioning Service for any EMSP. ♦
- 16 To enable all parties to validate certificates from the PKI, PKI Participants must **provide certificate status** information with the OCSP responder or Certificate Revocation List to all other PKI Participants without any restriction.

8.2. Market Rules for PKI Pool Operators

As a service to the PKI ecosystem, PKI Pool operators (e.g., Roaming Platforms) can collect contract certificates and OEM provisioning certificates in central ‘pools’, where market parties can access them efficiently. Some market parties however will keep their certificates in their own, individual Pool.

Since access to these ‘Collective’ and ‘Individual’ pools is conditional to offer ISO 15118, Market Rules apply to both.



8.2.1. Access to the PKI's OEM EV Provisioning Certificate Pools

EMSPs need to have access to the consumers' specific EV certificate that is generated by the OEM. Only when the private key of the EMSP contract is encrypted with this specific EV certificate, will the EV accept the EMSP contract. In a market with many EMSPs (currently hundreds in Europe), it may be more efficient for OEMs to transfer their OEM EV Provisioning Certificates to a “Central Pool” and outsource the information exchange to a central hub (a Collective Pool). This will also reduce the number of connections to all individual OEM Pools (tens) an EMSP has to manage. Since the PKI Pool Operator is responsible for this central Collective Pool, the following rules should apply:

17 All OEMs and EMSPs must have equal access to **Collective OEM Provisioning Certificate Pools**

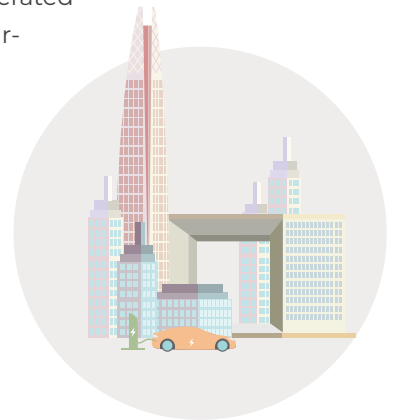
There are OEMs that prefer to store their OEM Provisioning Certificates in their own 'Individual' Pool. In that case, the following shall apply:

18 All EMSPs must have equal access to the **Individual OEM Provisioning Certificate Pool**

8.2.2. Access to the PKI's Contract Certificate Pools

Only when a Charging Station is trusted by the EV and has access to the consumers' EMSP contract, the consumer will be able to use the charging services at the Charging Station of its choice.

EMSPs and CSOs must exchange Contract Certificates. These are created by the EMSPs and are installed by Charging Stations operated by the CSO. In a market with many EMSPs and CSOs (currently hundreds in Europe), it may be more efficient for EMSPs to transfer their Contract Certificates to a "Central Pool" and outsource the information exchange to a central hub. This will also reduce the number of connections to all individual Contract Certificate Pools a CSO has to manage. Another reason to store Contract Certificates in a centralized pool is to ensure fast enough response times. OEMs also may want access to Contract Certificate Pools, in case they want to offer EMSP Contract Certificate Installation via their Telematics connection to the EV.



Although OEMs, EMSPs and CSOs are different market roles, many companies will be active in multiple roles. To ensure fair competition, open

access for OEMs, EMSPs and CSOs to each other's services must be addressed. Since the PKI Pool Operator is responsible for this central Collective Pool, the following rules should apply:

To ensure fair competition, open access for OEMs, EMSPs & CSOs to each other's services must be addressed

19 All OEMs, CSOs and EMSPs must have equal access to **Collective Contract Certificate Pools**

There are EMSPs that prefer to store their Contract Certificates in their own 'Individual' Pool. This way, they have maximum control

over the EMSP – CSO connection on their own Charging Network. However, denying access to these Contracts to other CSOs limit EV drivers to fetch new contract certificates at any Charging Station. In that case, the following shall apply:

20 All OEMs and CSOs must have equal access to the **Individual Contract Certificate Pools**

8.2.3. Pool interoperability / Central Pool Synchronisation

PKI Pool Operators can facilitate the market by connecting their Central Contract Certificate Pool and their Central OEM Provisioning Certificate Pool with other Pool Operators. This will allow CSOs, EMSPs and OEMs to only connect to one of the Pool Operators.

21 PKI Pool Operators must **ensure Pool Interoperability** with all other PKI Pool Operators. ♦

9. MARKET RULES FOR PKI PARTICIPANTS

CSOs can only offer ISO 15118 services to customers that have a vehicle that trusts the PKI the CSO is part of. When CSOs want to offer ISO 15118 services to their customers, they will need to become a Sub CA themselves and generate their own Charging Station leaf certificates or acquire Charging Station leaf certificates from a Sub CA.



At this point in time in Europe there are already more than 500 CPOs and many more are expected to join as European Countries become more active in EV charging. When they want to or must (according to EU regulation) offer ISO 15118 charging services will have to join a PKI. This PKI determines the participation contract terms, prices, operational performance, technical aspects and dispute resolution for PKI services. It is therefore stands to reason that CSOs will want the freedom to choose a PKI.

- When there is only one (dominant) PKI/V2G Root CA operational in Europe, all CSOs have no choice but to join this PKI. This PKI is a monopoly that should be regulated and monitored.
- When there are more than one V2G Root CAs active in Europe, to ensure a level playing field between V2G Root CAs and hence CSO freedom of choice of V2G Root CA, market rules should be put in place.

At this point in time in Europe there are already more than 400 EMSPs and many more are expected to join as European Countries become more active in EV charging. EMSPs that want to offer ISO 15118 charging services will have to join a PKI, either by becoming a Sub CA to generate contract certificates or by setting up an own MO Root CA and getting access to the Certificate Provisioning Service of a PKI. This PKI determines the participation contract terms, prices, operational performance, technical aspects and dispute resolution. It therefore stands to reason that EMSPs will want the freedom to choose a PKI.

All EMSPs in the market should have an equal opportunity to offers services enabled by ISO 15118 technology (such as Plug&Charge, Smart Charging or V2X) to their customers.

- When there is only one (dominant) PKI/V2G Root CA operational in Europe, all EMSPs have no choice but to join this PKI. This PKI is a **monopoly that should be regulated** and monitored
- When there are more than one V2G Root CAs active in Europe, to ensure a level playing field between V2G Root CAs and hence EMSP freedom of choice of V2G Root CA, **market rules** should be put in place

PKI participants are CSOs, EMSPs and OEMs, that can be independent and complementary (not overlapping). In this case market rules may not be needed. However, when companies take one and / or multiple roles, they can be each other's competitors, in which case market rules come into play.



Market parties that want to offer ISO 15118 charging services will have to join a PKI

9.1. Market rules for CSOs



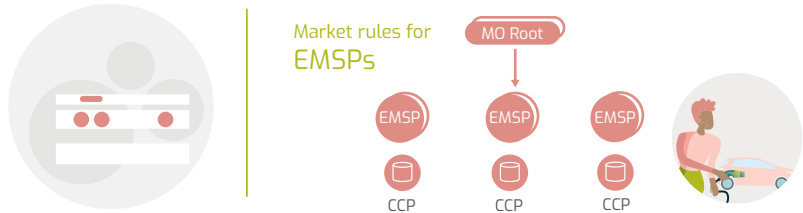
The consumer will be able to use and update its EMSP contract, only when a CSO has access to the Contract Certificate Pool to fetch a contract certificate by the request of the consumer.

Although EMSPs and CSOs are different market roles, many companies will be active in both roles. To ensure fair competition, open access for EMSPs to charging infrastructure within reasonable costs should be addressed.

- 22** CSOs, which support contract certificate installation/ update, **must offer connection to all** Contract Certificate Pools participating in the PKI, either via direct connection or via Pool Interoperability. ♦

No additional market rules are needed for CSOs, since the ISO 15118 PKI structure and technical operation already impose requirements on the CSO.

9.2. Market Rules for EMSPs



Only when a Charging Station is trusted by the EV and has access to the consumers' EMSP contract, the consumer will be able to use the charging services at the Charging Station of its choice. Although EMSPs and CSOs are different market roles, many companies will be active in both roles. To ensure fair competition, open access for EMSPs and CSOs to each other's services must be addressed.

- 23** EMSPs must make **contract certificates accessible to all** CSOs to install contract certificates in EVs via the charging infrastructure. Alternatively, EMSPs transfer the responsibility for enabling access to a third party, e.g., Central Collective Contract Certificate Pool Operator.

According to ISO 15118, EMSPs can choose to use the V2G Root CA or operate their own MO Root CA. The EMSP contract certificates should be signed by an MO Sub CA certificate that is derived from the V2G Root CA or by an MO Root CA.

- 24** EMSPs that operate their own MO Root CAs must **publish their MO Root CA certificates.** ♦

To ensure fast enough response times, the EMSP can contribute their Contract Certificate to one or more “Contract Certificate Pools” (CCP).

- 25 EMSPs must indicate the **contract certificates' location** to the OEMs and CSOs. ♦
- 26 EMSPs must make contract certificates **accessible** to the customer's EV OEM to install contract certificates in EVs via the OTA/ vehicle telematics interface and OEM backend. Alternatively, EMSPs transfer the responsibility for enabling access to a third party, e.g., Contract Certificate Pool Operator. ♦
- 27 EMSP contract certificate **bundles must be signed** by a CPS certificate chain derived from the V2G Root CA. ♦

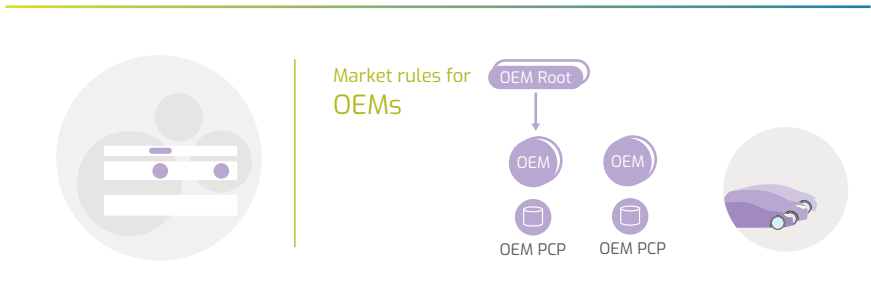
A consumer and EMSP agree on the contract duration and on terms for contract termination (e.g., a three-year contract with an option to cancel after the first year).

The EMSP contract that is embedded in the EV has a validity date. If a consumer switches between EMSPs, the existing EMSP contract should be technically revoked from the system without regard of the validity date. This revocation should be done by the old EMSP (who may not be inclined to do so) or should be done by the party that manages the Customer Contract Certificate Pool (CCCP) (assuming this party is neutral). The selection of the EMSP by the consumer must be respected by all parties. There should be clear market rules on this consumer switch, keeping into consideration contract terms.

- 28 To ensure freedom of consumers to change their EMSP contract, market rules for **customer switching** need to be published for each PKI.



9.3. Market Rules for OEMs



OEMs will only trust V2G Root CAs that adhere to a minimum level of security, stated in the Quality Rules of a PKI (often stated in a Certificate Policy and Certificate Practice Statement).

- 29** Only V2G Root CAs that minimally **adhere to European Standard** Quality Requirements will be included in the EV trust store

In ISO 15118-2 and in the ISO 15118-20 draft version the Certificate Installation via the Charging Station is an optional part of the specification. There are OEMs that prefer contract certificates to be installed in their vehicles via 'Telematics' or 'Over the Air' (OTA). If this is the case, then this route should be open to the EMSP of the consumers' choice.

- 30** OEMs **must enable the installation/update** of an EMSP contract that was chosen freely by the consumer; either by allowing access via the OEM Telematics connection or by enabling EMSP Contract Certificate Installation via the Charging Infrastructure. ♦

The EMSP a consumer selects will create a Contract Certificate for this specific customer and will install it into the customer's EV. When buying EVs, consumers shall be free to select the EMSP of their choice.

- 31 The technical and commercial **terms** defined by OEMs for installing an EMSP contract in the vehicle **must be equal for all** EMSPs. ♦
- 32 EVs shall only be sold or delivered with a pre-selected EMSP contract with the **consumer's explicit consent**. ♦
- 33 In case of multiple EMSP contracts installed in the EV, the consumer must have the **freedom to switch** to the contract of choice. ♦

The PCID of the EV is the common EV identifier between the EMSP and OEM.

- 34 OEMs must provide a simple and secure way for the consumer to **access the PCID** of the EV. Additionally, OEMs must offer a consumer-friendly way for the replacement in case of loss or change of the PCID. ♦
- 35 OEMs must inform consumers of the **PCID changes** of their EVs. Alternatively, OEMs can transfer the responsibility for informing of PCID changes to a third party. ♦



The EMSPs need to have access to the consumers' specific EV certificate that is generated by the OEM. An EV will only accept the EMSP contract when the private key of the EMSP contract is encrypted with this specific EV certificate. OEMs store their OEM EV Provisioning Certificates into a 'Pool'.

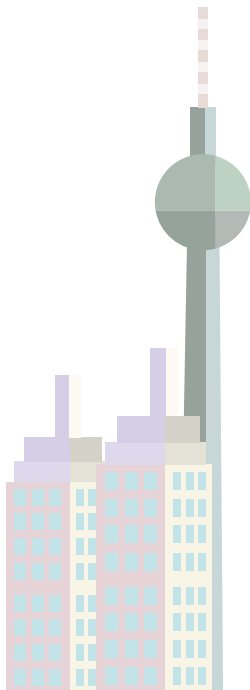
- 36 OEMs must ensure that the consumers' EVs **always have valid OEM provisioning certificates** in case of an existing telematics route. If the OEM does not offer telematics services, the certificate must be updated at the next workshop visit at an OEM service partner before the expiration of the installed certificate. ♦

- 37** OEMs must ensure a way for **EMSPs to have access to the EV's OEM provisioning certificates** (e.g., indicating the location of OEM provisioning certificates directly or via a third party or OEM pushes OEM provisioning certificates at EMSP request). ♦

In a market with many EMSPs (currently hundreds in Europe), it will be more efficient for OEMs to transfer their OEM EV Provisioning Certificates to a “Collective Central Pool” and outsource the information exchange to a central hub. For EMSPs this reduces the number of connections to all individual OEM Pools (tens) an EMSP must manage.

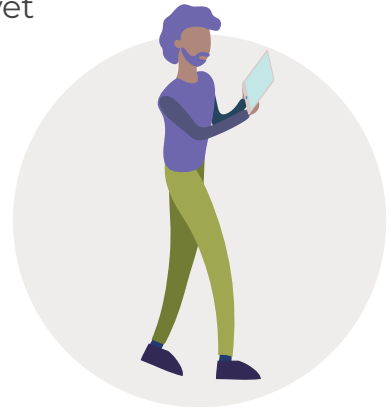
For access to these OEM EV Provisioning Certificates the following market rules should apply:

- 38** **OEMs must publish all relevant EV information** for the EMSPs to ensure the functionality of the Plug and Charge contract in the EV: ISO 15118 version (-2 vs -20), schema version, if needed, cryptographic information and installed V2G Root CAs in the EV trust store). ♦



10. MARKET RULES FOR INTEROPERABILITY BETWEEN PKIs

When each individual PKI sets up market rules for their participants, the fair and open access within that PKI is dealt with. This does not yet guarantee that market players have the freedom to choose a PKI, nor does it guarantee interoperability for EV drivers.



For freedom of choice for market participants and EV drivers, PKI interoperability must also be addressed. PKIs are in competition with each other, offering the same services to the market and oftentimes

controlled by market competitors. That is why market rules for PKI interoperability cannot be left to the market but should be addressed at the European Governmental level.

Broadly speaking, there are three options to achieve PKI interoperability.

For freedom of choice for market participants and EV drivers, PKI interoperability must also be addressed

PKI Interoperability resulting in EV drivers to charge at any Charging Station using the contract of their choice can be achieved by the following three options :

1

Cross Certification & Pool Interoperability

- V2G Root CAs can **cross sign each other's certificates** so that interoperability does not specifically depend on OEMs / CSOs / EMSPs, but is handled on PKI level.
- PKI Pool Operators must **ensure Pool Interoperability** with all other PKI Pool Operators.

The technical details regarding Cross Certification and the impact on PKI participants are described in part 2. This interoperability solution requires investment by V2G Root CAs and PKI Participants in maintaining Cross Certificates and investments by CSO regarding the hardware requirements of the charging stations. The main burden for PKI interoperability is shared between V2G Root CAs and CSOs.

2

A Trust List Mechanism & Pool interoperability

- All V2G Root CAs **join** the Certificate Trust List
- OEMs store **all V2G Root CAs** on the CTL in the trust stores of their **Vehicles**
- CSO store **all V2G Root CAs** (and OEM Root CAs in case of ISO 15118-20) on the CTL on all **charging stations**
- PKI Pool Operators must **ensure Pool Interoperability** with all other PKI Pool Operators.

The technical details regarding the Trust List Mechanism and the impact on PKI participants are described in part 2. This interoperability solution requires investment in setting up and running a Trust List Manager, investments by OEMs in the size of the Trust Stores in the EVs and investments by CSO regarding the hardware requirements of the charging stations. The main burden for PKI interoperability lies with the OEMs.

CSOs (and possibly EMSPs) join all PKIs & Pool interoperability

3

- **CSOs join all PKIs** by becoming a Sub CA or by buying leaf certificates for all their charging stations
- PKI Pool Operators must **ensure Pool Interoperability** with all other PKI Pool Operators.
- **Whether EMSPs should join** all PKIs depends on the extent of the Pool Interoperability.

This interoperability solution requires investment by all individual CSOs in joining all PKIs. This results in an increase in operating costs for CSOs (and possibly EMSPs). The main burden for PKI interoperability lies with the CSOs.

The technical details regarding PKI Pool Interoperability is not yet part of this document. Work has started in 2022 with our project partners. Results of this cooperation are expected in the second half of 2022.

The interoperability solution requires investment by market parties

Depending on the chosen option, market parties could together assure PKI interoperability, but this comes at a financial cost and some individual market parties oppose interoperability, claiming that it is conflicting with their companies' interests.

For the sake of consumer freedom and a fair and level playing field for market parties, PKI interoperability should be addressed at the European Governmental level.



10.1. Cross Certification in combination with Pool Interoperability

When PKI interoperability is achieved by Cross Certification and Pool interoperability, additional market rules are needed. The already defined market rules also still apply..

- 39** All eligible **V2G Root CAs must support interoperability mechanisms**, if multiple V2G Root CAs emerge in the European market, by facilitating Cross Certification (see also market rule 6) ♦
- 40** **PKI Pool Operators** must ensure Pool Interoperability with all other PKI Pool Operators. (see also market rule 21) ♦

Additionally market rules are needed for cross certificates.

- 41** All cross certificates that are used in the market should be **made available** to all market parties participating in one of the PKIs.
- 42** A CSOs should **install all Cross Certificates** of the V2G Root CA in all their Charging Stations.

10.2. Trust List Mechanism in combination with Pool interoperability

When PKI interoperability is achieved by a Trust List mechanism with Pool interoperability, additional market rules are needed. The already defined market rules also still apply.

- 43 All eligible V2G Root CAs must support interoperability mechanisms, if multiple V2G Root CAs emerge in the European market, by participating in the European Trust List (see also market rule 21) ♦
- 44 PKI **Pool Operators** must ensure Pool Interoperability with all other PKI Pool Operators. (see also market rule 21) ♦

Additionally, market rules are needed for OEMs and CSOs.

To allow open access for Certificate Authorities that want to join the ecosystem in future, existing EVs should be able to get an update of a Root Certificate of a new CA joining the market.

- 45 Any OEM should support the **addition of new V2G Root CA Certificates in the EV** by either using the 'Over the Air' (OTA) connection or using a dealership infrastructure.

When using a Certificate Trust List as an interoperability mechanism, the interoperability for installing contract certificates is arranged by installing V2G Root CAs in the EV. It is important that all V2G Root CAs on the CTL are installed in the EVs trust store.

- 46 OEMs should **add additional V2G Root CA Certificates** in the EV, either by using the OTA connection or by using the dealership infrastructure.
- 47 OEMs should accommodate PKI interoperability by providing sufficient **support for multiple V2G Root CAs** in the EVs Trust Store (e.g., 100+ V2G Root CAs).

The EMSP contract certificates should be signed by an MO Sub CA certificate that is derived from the V2G Root CA or by an MO Root CA. According to ISO 15118, the MO Sub CA can be derived from the V2G Root CA or EMSPs can operate their own MO Root CA. In a market with many EMSPs (currently hundreds in Europe), and all these EMSPs should decide to become their own MO Root CA, the impact of managing hundreds of MO Root CA certificates is on the CSO is too great. For certificate management reasons for CSOs, it therefore seems more practical to derive MO Sub CA certificates from the V2G Root CA.

PKIs have an important role to play in protecting CSOs from this development. They can state that contract certificates that are not derived from the V2G Root CA cannot use the CPS.

- 48 A V2G Root CA **shall only allow an EMSP access** to the CPS if the MO Root CA is derived from the V2G Root CA.

However, if the market would develop towards a setup with many MO Root CA certificate, it may be more efficient to introduce a European MO Root CA Trust List (MO-CTL). In that case:

49 The CSO should provide the **MO-CTL to all** Charging Stations:

- Either by forwarding the list in its entirety to the Charging Station and the Charging Station should install all MO Root CA certificates on the MO-CTL in the Charging Station for validating contract certificates
- Or the CSO should send each certificate on the MO-CTL to the Charging Station for installation and the Charging Station should install each certificate for validating contract certificates.

10.3. CSOs (and possibly EMSPs) join all PKIs in combination with Pool interoperability



When PKI interoperability is achieved by CSOs joining alle PKIs in combination with Pool interoperability, additional market rules are needed. The already defined market rules also still apply.

50 PKI Pool Operators must **ensure Pool Interoperability** with all other PKI Pool Operators. (see also market rule 21) ♦

Additionally, market rules are needed for EMSPs and CSOs.

51 All EMSPs should **participate in all European PKIs**, by joining all PKIs that are on the European V2G Root CA Trust List depending on how the Pool interoperability is setup.

Only when a CSO has embedded the V2G Root Certificate on its Charging Stations and installs a certificate derived from that V2G Root CA, the consumer will be able to use its EV that is equipped with the V2G Root CA and use its EMSP contract.

52 A CSOs **should participate** in all European PKIs

- For each V2G Root CA in the market, the CSO must install a Charging Station certificate derived from that V2G Root CA
- By installing all V2G Root CA certificates on the CTL on the charging stations for contract certificate verification.
- By installing all OEM Root CAs (ISO 15118-20)

53 CSOs should **install all MO Root CA certificates** for contract certificate verification.

Please note that on a business level CSOs and EMSPs make separate roaming agreements. These agreements are independent of the technical certificates that are installed in Charging Stations.

11. RECOMMENDATIONS

11.1. Governance by an Independent European Authority

Regardless of whether all European parties join one PKI – that will result in a monopoly that requires strict regulation, or whether there will be multiple PKIs that will co-exist and interoperate, we believe that at a European Legislative level, detailed market rules and governance will need to be put in place.

Independent governance of the market rules would benefit the acceptance of these rules and will help dispute resolution.



An independent European Authority should be put in place to:

- Guarantee interoperability for consumers
- Monitor PKIs and the fair, reasonable and non-discriminatory access to a PKI
- Monitor the terms, fees charged, and Quality of Service Level (response times, availability)
- Monitor the Independent Quality Auditors
- Act as an intermediary in case of conflict
- Organize the acceptance of new V2G Root CAs
- Set and / or Monitor the Quality rules V2G Root CAs and Sub CAs should adhere to
- Monitor the Cross Certification process and the fair, reasonable and non-discriminatory access to Cross Certification
- Monitor the Certificate Trust List Manager and the fair, reasonable and non-discriminatory access to a Certificate Trust List

Independent governance is needed regardless of the number of PKIs in the market, the owners/operators of the PKI (commercial, industry association or National Cooperative) or the chosen interoperability mechanism.

Today, ISO 15118 vehicles are in production, Public Tenders are requiring ISO 15118 and the European Commission, as well as National authorities, are recommending the use of ISO 15118. With this long-awaited roll out of ISO 15118, now is the time to act and set up an independent, neutral European Governance Authority to ensure a secure, open and consumer centered PKI ecosystem.

11.2. Market Initiatives for V2G Root CAs

At the time of writing this publication, several market initiatives were developing a V2G Root CA for the European market, in addition to the already existing V2G Root CA operated by Hubject.

TERMS & CONDITIONS



We recommend all V2G Root CA initiatives to follow the example of CharIN and establish and publish PnC Terms & Conditions

The CharIN PnC Europe initiative has discussed internally what market rules (or Terms and Conditions) should be put in place. These are published as “CharIN PnC Terms & Conditions - 2022-02-08” . These Terms and Conditions cover to a very large extent the market rules in this document, with the exception of the market rules for the Trust List Manager and interoperability between PKIs (chapter 10).

The V2G Root CA initiatives by SAE and Gireve have not yet published their T&C.

We recommend all V2G Root CA initiatives to follow the example of CharIN and establish and publish PnC Terms & Conditions.

MARKET PARTIES JOINING DISCUSSION

The recently formed STF Sub-group on “governance and standards for communication exchange in the electromobility ecosystem” addresses the topic of market rules and governance. The STF Subgroup 1 started in 2021 discussing this topic and will remain to do so in 2022. We recommend the STF to discuss market rules and governance with a great level of detail (so not high level requirements). We recommend that the STF Subgroup broadens the participation in the discussion with the market parties that are affected most, the hundreds of active EMSPs and CSOs in the diverse European market. Companies at the table currently are mainly large corporations and are therefore not a balanced representation of the current EV charging market.

EUROPEAN COMMISSION

Lastly, this STF Sub-group is merely an advisory body, where the final decision lies somewhere else. We call upon the European Commission to be transparent about the decision making process regarding this important topic. The outcome will determine the fair and open access, freedom of choice for market players and interoperability for EV drivers. And therefore it will determine the success and competitiveness of the European EV charging industry.



We recommend that the STF Subgroup broadens the participation in the discussion with the hundreds of active EMSPs and CSOs in the European market



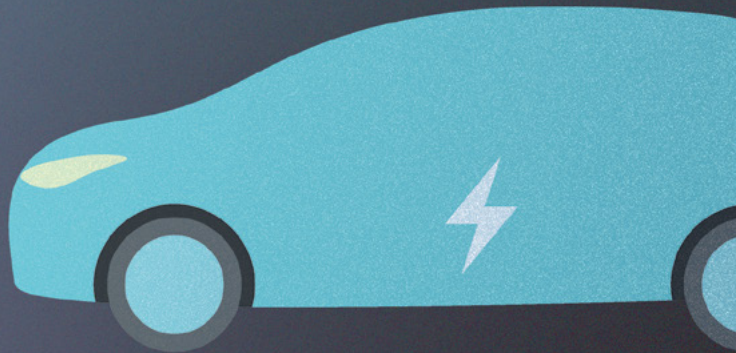
Public Key

Private Key

PART 2

Technical PKI Interoperability

Developing an interoperable PKI
ecosystem for ISO15118



CO-AUTHOR:

Eric Baumann	Hager Group
Jerome Benoit	SAP Labs
Olivier Chalier	VEDECOM
Olivier Clerc	Thales Group
Moritz Dickehage	e-clearing.net
Dimitri Doutriaux	Trialog
Roch El Khoury	VEDECOM
Pierre Girard	Thales Group
Christian Hahn	Hubject
Michel d' Hooge	VEDECOM
Teddy Hyunwoong Kim	Gridwiz
Wayles Hyunsoo Kim	Gridwiz
Ricardo Jover	VEDECOM
Jesse Kerkhoven	ElaadNL
Jacques Kraemer	Hager Group
Olivier Maridat	Trialog
Joe Matta	VEDECOM
Anas Munir	e-clearing.net
Steffen Rhinow	Hubject
Gerald Seiler	SAP Labs
Jaeson Yoo	Penta Security Systems Inc.



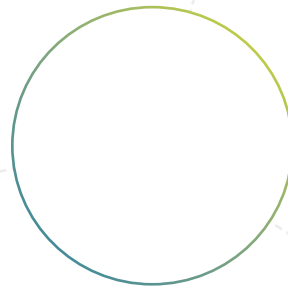
Technical PKI Interoperability PART 2

SPECIAL THANKS TO:

Francois Colet	Renault
Thomas Fousse	Gireve
Joseph Levy	Driivz
Daniel Navrotsky	Driivz
Ashkan Nazary	NewMotion
Jean-Marc Rives	Gireve
Saber Omrani	Renault
Jean-Rémy Oudin	Freshmile
Oscar Rodriguez Infante	EDF
Damien Pierre Sainflou	Stellantis
Maxime Roux	Freshmile
Stefan Scheubner	EnBW
Marco Stiegelmaier	Volkswagen
Mourad Tiguercha	Concentus
Baran Yalcin	tinqplus
Christoph Zwirello	NewMotion



A technical solution
is needed to connect
different PKIs into one
interoperable solution





12. INTRODUCTION

For the technical solutions to work together, there needs to be a standard way to implement the digital secure communication. The basis is currently governed by the ISO 15118 working group.

However, in order to get the entire system to work, additional work has been undertaken by the German VDE (Verband der Elektrotechnik, Elektronik und Informationstechnik) in the working group DKE AK 901.0.115. This group provided the VDE AR 2802-100-1.

For further reference, please see [Exploring the PKI for ISO 15118 in the EV charging Ecosystem](#) [ElaadNL-PKI].

Since the VDE is operating in Germany with German parties and ISO 15118 is a global standard, CharIN has started a task group on PKI interoperability. This group is developing a use case based interoperability doc-

One V2G Root CA



There is one Root CA that is the top Certificate Authority / Trust Anchor of the entire PKI ecosystem

Cross Recognition



Multiple PKI's exist in the ecosystem. Everybody agrees that all PKIs are "trusted" or "cross-recognized"

Cross Certification



"Bilateral" trust relations between pairs of CAs

Certificate Trust List



There is one entity that keeps a list of all trusted CA certificates. All PKI participants can access and use this central trust list

Figure 3: ISO 15118 PKI options

ument (reference [CharIN-IOP]) aligning with and building on the VDE application guide (reference [VDE-AR]).

Additionally, for the various PKIs to technically work together, a technical solution is needed to connect different PKIs into one interoperable solution. A group of American, Dutch, German, French, Korean and Israeli companies, have come together to build and test an interoperable PKI solution. Based on this joint work, Part 2 of this publication elaborates on the topic of technical PKI interoperability.

The group aims, through sharing the findings and technical details of PKI interoperability, to assist the market in developing an interoperable PKI ecosystem for ISO 15118. In turn it will assist a successful adoption by EV drivers and legislators.

There are multiple options for implementing an interoperable Public Key Infrastructure (PKI) for an ISO 15118 EV ecosystem, which are visualized in the figure.

Three out of these four options are approaches assuming a market organization in which multiple V2G Root CA PKIs coexist: cross recognition, cross certification and certificate trust list. In these scenarios, requirements are needed for PKI interoperability, that are to this date not yet described in the ISO 15118 standard itself, nor in other related publications (e.g. the “VDE Anwendungsregel”, reference [VDE-AR] or the draft CharIN PKI interoperability document, reference [CharIN-IOP]). These publications do not consider this topic, since – at this point in time - these all assume only one V2G Root CA per continent.

This part describes technical details for achieving PKI interoperability for cross recognition, cross certification and certificate trust list. All options from Figure 3 are discussed shortly in chapter 13. Cross certification and certificate trust lists are discussed more elaborately. These have been implemented in a field test, of which the results are presented in chapter 14 for Cross Certification in Practice and in chapter 15 for Certificate Trust lists in Practice.



13. PKI INTEROPERABILITY FOR ISO 15118

The PKI structure for ISO 15118 is part of the specification of ISO 15118, having its own trust anchor, the V2G Root CA. This structure can be applied as such, but when used on a European level, more than one trust anchors are likely to emerge.



This chapter describes different options for setting up a PKI for an ISO 15118 ecosystem. The first option describes having one V2G Root CA (paragraph 13.1). Three options describe scenarios where multiple V2G Root CAs co-exist and are interoperable with each other (paragraphs 13.2, 13.3 and 13.4).

13.1. One V2G Root CA

In general, the first option for setting up a PKI is to have only one V2G Root CA, operated by either a market participant, an industry association or a neutral, governmental level organisation. This would imply that the entire industry would join in one PKI, by either becoming a Sub CA or by acquiring the leaf certificates of this PKI.

In this case only one V2G Root CA certificate is needed in every EV and in every Charging Station in Europe for example, so the technical impact would be small^o. When the technology was first introduced, this simplistic market model was a logical first step.

The advantage of this approach is that it is simple. Certificate maintenance is easy, since all CSOs, CPSs and every Charging Station would be part of the same PKI. Although the ISO 15118 specification is prepared for having more than one V2G Root CA, this approach would fit perfectly in the ISO 15118 specification and thus would not require any changes to the ISO 15118 specification.

The disadvantage of this approach is that in case of one party fulfilling the role of the central (worldwide or European) V2G Root CA, this would create a powerful position (a monopoly for appointing Sub CAs and contract certificate provisioning). This would force all companies to use or trust the certificates from this PKI, making the position disproportionately powerful and dominant in disputes and could in theory allow for the possibility that some companies (particularly CSOs and EMSPs) are denied access to the EV charging infrastructure. OEMs are much less affected by this PKI monopoly, since they can operate their own OEM PKI independently. They do not have to join this PKI, but only need to trust the V2G Root PKI and acquire the V2G Root CA's public certificate. This monopoly position is in itself not enforceable by any industry group (commercial or non-profit). Furthermore, it introduces a single point of failure.



^o Please note that based on the validity requirements of ISO 15118, the number of certificates for one V2G Root CA will over the years be greater than one, since at least both the old and new certificate must be stored.

In order to agree to one central (European) Governmental Governing Organization, there must be awareness and willingness at a central (global and European) level. Given the fact that various countries and governments are at various stages of the transition to e-mobility, it is unlikely that this option will materialize soon.

In any case, particularly in this situation, PKI quality rules, interoperability rules (between parties inside the PKI) and market governance (strict market regulation on pricing and “FRAND” terms) are of the utmost importance to ensure fair competition. Please refer to part 1 for more information about market rules and governance.

13.2. Multiple V2G Root CAs with Cross recognition

There are currently several independent PKIs emerging. The technically simplest way to achieve PKI interoperability is that EVs recognise all certificates from all PKIs as trusted and all certificates are shared between PKIs. Practically this means that all EVs store all V2G Root CAs in their trust store and all charging stations store all V2G Root CA certificates in their trust store.

There are currently already several independent PKIs emerging in Europe

The ISO 15118 standard already takes into account the possibility to store multiple V2G Root CA certificates in the vehicle as a way to implement cross recognition. No changes are needed to the ISO 15118 specification.

The downside is that OEM must be willing to install the V2G Root CA certificate of all PKIs and of new entrants inside the EV, using the “over the air” connection (or during service appointments). Similarly, charging infrastructure operators must also be willing to install / allow certificates from all PKIs. This gives some actors in the EV ecosystem the power to either refuse new market participants (for commercial reasons), or set unreasonable terms and fees for this ser-

vice. Additionally, at this point in time, statements from OEMs about the number of available “slots” in the EV trust store for installing V2G Root CAs are mixed / not always consistent . This means that at this moment it is uncertain whether OEMs can and will support ‘Cross Recognition’.

The alternative is that market parties join all existing PKIs. Practically these options mean that all EV manufacturers, all charging infrastructure providers and all e-mobility service providers adopt and accept all the various certificates. This option, where any participant should consider any PKI of any other participant as trustworthy, is called cross recognition. For this alternative where Charging Station Operators (CSOs) and E-Mobility Service Providers (EMSPs) join multiple PKIs, the downside is that PKIs must work in an aligned way and that joining multiple PKIs means to setup multiple B2B agreements and paying multiple PKIs, what could become a very costly option. These costs will be borne by the consumer.



For both options, storing multiple certificates impacts the hardware requirements of EVs and Charging Stations and therefore there is a limit to the number of PKIs that can enter the market. Additionally, future market entrants face the situation where the existing infrastructure is saturated, putting them at a disadvantage to the existing industry. This could disincentivise e-mobility market growth and competition.

In any case, also in this situation, PKI quality rules, interoperability rules and market governance (strict market regulation on pricing and Fair, Reasonable and Non-Discriminatory (“FRAND”) terms) are of the utmost importance to ensure accepting other V2G Root CAs is not misused for unfair competition. Please refer to part 1 for more information about market rules and governance.

13.3. Multiple V2G Root CAs with Cross certification

A second option for creating interoperability between PKIs is to use a technical solution called cross certification. This solution is technically more complex than the previous options described. To better understand the impact of this solution, the consequences for different standards and implementations, this mechanism has been tested in practice. This is further elaborated in chapter 14 “Cross Certification in Practice”.

The main advantage of this approach is that once the mechanisms to support cross certification are in place, interoperability can be arranged outside of the EV at the charging infrastructure. OEMs do not have to install all V2G Root CA certificates in all their EVs and Charging Station do not need to join multiple PKIs. EMSPs can offer contracts independent of the EV PKI if cross certification is implemented in the entire market.



The disadvantage of cross certification is that the maintenance effort becomes high with a larger number of Root certificates.

Cross certification can achieve that no role in the ecosystems has unnatural power over others, provided that quality rules and PKI interoperability rules and market governance (strict market regulation on pricing and “FRAND” terms) are in place. Please refer to part 1 for market rules and governance and part 3 for more information about quality rules.

13.4. Multiple V2G Root CAs with Certificate Trust List

A third option that is described in this document is the use of Certificate Trust Lists. Similar to Cross Certification, this solution is more complex than the first option described. To better understand the impact of this solution, the consequences for different standards and implementations, this mechanism has also been tried in practice. This is further elaborated in chapter 15 Certificate Trust lists in Practice.

The main advantage of this option is that, as with the cross certification, once the mechanisms to support Certificate Trust Lists are in place, the interoperability can be arranged by adding more V2G Root CA certificates to EVs and charging infrastructure. This does not solve the scalability on the EV and Charging Station side since all V2G Root CAs from the Certificate Trust List must be stored in memory. It does however make the approach more maintainable, since the list is maintained centrally and updates can be done by replacing the list. This solution is usually considered better suited for interoperability for larger amounts of PKIs (compared to cross certification) because of its maintainability. However, as stated in the paragraph describing Cross Recognition, at this point in time, statements from OEMs about the number of available “slots” in the EV trust store for installing V2G Root CAs are mixed / not always consistent . This means that at this moment it is uncertain whether OEMs can and will support a ‘Certificate Trust List’ with more than one V2G Root CA.



The disadvantage of Certificate Trust List is that it requires a new authority to emerge and manage the list of trusted V2G Root CAs. Such authority needs to be trusted by all e-mobility players.

The Certificate Trust List is an option to achieve interoperability between PKIs, provided that quality rules and PKI interoperability rules and market governance (strict market regulation on pricing and “FRAND” terms) are in place, especially to ensure that e-Mobility players do in fact trust the CTL and install its content to their devices. Please refer to part 1 for market rules and governance and part 3 for more information about quality rules.



14. CROSS CERTIFICATION IN PRACTICE

14.1. Cross certification explained

Please note that this chapter requires some knowledge of certificates and the ISO 15118 specification. Please refer to “Exploring the PKI for ISO 15118 in the EV charging Ecosystem” for the necessary information.

PUBLICATION

"Exploring the
Public Key Infrastructure
for
ISO 15118
in the
EV charging Ecosystem"

ElaadNL, Arnhem,
The Netherlands,
November 2018

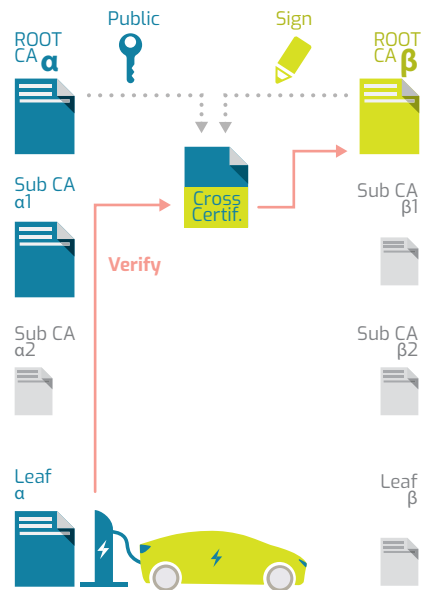


Download: https://www.elaad.nl/uploads/files/Exploring_the_PKI_for_ISO_15118_in_the_EV_charging_ecoystem_V1.0s2.pdf

14.1.1. General explanation

PKI interoperability using cross certificates, makes use of the mechanism of signing certificates, as it is normally done in PKIs, with the difference that in this case certificates from different PKIs are signed by each other's certificate authorities (actually: signed by the private keys belonging to the certificates of these certificates authorities). This can be done between any two certificates authorities from two PKIs. The following explanation will consider Root CAs that sign each other's certificate.

In the simplest terms, a certificate consists of a public key, certificate information (validity, subject and issuer) and a signature. The idea of cross certification is that it is used to create interoperability between PKIs, without changing the original certificates, but by adding additional certificates that can be used to verify a chain of certificates leading to a different Root CA.



How it works in more detail is that Root CA α sends a "certificate signing request" (csr) containing the public key of Root CA α to another Root CA, Root CA β . Root CA β in turn creates a cross certificate by:

- Signing it using the private key of Root CA β
- Using the same subject,
- But using a different issuer, namely Root CA β .

When verifying a certificate chain, the first step is to put together a correct / valid chain, based on the certificate subjects and issuers. The certificate information is used for finding a correct / valid chain by using the same subject for a cross certificate, but a different issuer. This way, a second path upwards in the chain is created, towards the other Root CA, in this example, Root CA **β**.

The verification of certificate chains is executed by verifying signatures using the public keys of the parent certificates. By using the same public key for the cross certificate, the validation of the chain with the alternative path is successful. Since the issuer of the cross certificate is not the Root CA **α**, the path leads to Root CA **β**.

Note: for the normal situation, the path leads to Root CA **α** self-signed certificate. The Cross-signed certificate is only used by systems only trusting Root CA **β** and not Root CA **α**.

When verifying a chain of certificates when the Root CA **β** is installed, but Root CA **α** is not, a cross certificate can be used that has been derived from Root CA **β**, which can then be traced back to a trusted Root CA **β**, as illustrated in figure above:



If Leaf **α** is to be validated, but Root CA **α** is an unknown CA, without cross-certification, it would not be possible to execute this validation. Reason is that it cannot be validated that Root CA **α** is a “trusted” certificate.

When using cross certification, a cross-certificate (Blue / Green in the figure) is created between the PKIs. This certificate has the same public key as Root CA **α**, but is not self-signed (as usually with Root CA certificates), but it is signed by Root CA **β**. Technically, the issuer (DN) should contain Root CA **β** and the subject (CN) should refer to Root CA **α**.

During the validation of a certificate chain, the path should be constructed from bottom to top and the signatures on the certificates should be validated using the public key of the certificate “above” it. Without cross-certification, the certificate of Sub CA **a1** would only be checked on its issuer Root CA **a**, of which in this example the certificate is not available. Path: Leaf **a**-> Sub CA **a2** -> Sub CA **a1** -> Root CA **a**†.

cross certification
can be done
between
any two certificates
of two PKIs.

When using cross-certification, by looking at the Subject DN, the path to the cross-certificate is an alternative path. Because it is created using the same public key as the public key of Root CA **a**, it can be validated that Sub CA **a1** is valid. In turn, the validity of the cross certificate can be determined using Root CA **b**, that in this example is available. So the path for validation is: Leaf **a**-> Sub CA **a2** -> Sub CA **a1** -> Cross certificate -> Root CA **b**.

The explanation above shows how to verify Leaf **a** with Root CA **b** using a cross certificate. If two PKIs trust each other, this would imply that it would also be possible for a Leaf **b** to be verified with Root CA **a**. This would require creating a second cross certificate (CSR from Root CA **b**, signed by Root CA **a**).

14.1.2. Cross certification on different levels

As indicated in the introduction, cross certification can be done between any two certificates of two PKIs. In the case of ISO 15118, the structure of the PKI is defined in the specification, so each PKI will look similar to one another. In the following paragraphs multiple levels on which cross certification can be executed are discussed, including the consequences for the number of levels and the scalability. The ISO 15118-2 specification currently specifies a PKI structure consisting of one V2G Root, one or two Sub CA levels and a leaf certificate level. As one may have noticed in the previous paragraph, using cross certificates introduces an additional layer in the PKI.

Root CA level

The example in the introduction explained cross certification on the Root CA level. Translated to ISO 15118, this would mean that two V2G Root CAs would cross sign each other's certificates, for which two cross certificates would be necessary. The main advantage of cross certification is that an EV can charge at a PKI other than its own, without the EV belonging to the same PKI as the Charging Station and Charging Station Operator (CSO). This means that the EV can charge at the infrastructure, without requiring the CSO to possess a private key and certificate from the same PKI installed at EV side. Instead of having to be a member of the other PKI, it would suffice to have a cross certificate between certificate authorities of the two PKIs.

A second advantage of this approach is that when the number of PKIs grows, the number of cross certificates per additional PKI is smaller, compared to cross certifying on SubCA level. The scalability for this approach is therefore suitable for small or medium amounts of V2G Root CAs, for example, for 3 PKIs, 6 cross certificates are needed^Σ. Once the number of V2G Root CAs becomes very high, the number of cross certificates grows too: for each additional V2G Root CA, two cross certificates are needed per existing V2G Root CA. To connect n PKIs using cross certificates, this would mean a "full graph" x two cross certificates:

$$\frac{n(n-1)}{2} * 2 \text{ cross certificates needed}$$

▼ Not available

^Σ Please note that this is per generation and this number can be higher (e.g. old / new or if other types of certificates are used in the future)

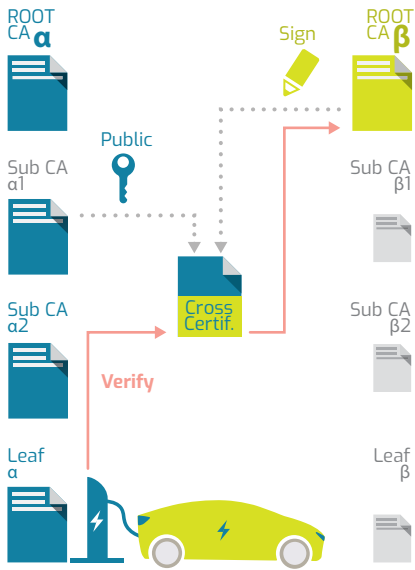
In the current ISO 15118-2 specification, the number of layers is limited^①. When cross signing on Root CA level an additional layer is necessary, therefore one Sub CA level must be sacrificed for the purpose of cross certification. In paragraph 14.2.1 we address the possible impact this has on existing ISO 15118-2 implementations. The disadvantage of this approach is that for each Sub CA (i.e. for each CSO or CPS), the Root CA is needed to sign the Sub CA. This can be considered as a security risk, as the Root CA private key is often stored offline for security reasons. Using it for signing each Sub CA would mean that it is needed during operating the PKI and cannot thus be stored offline all the time.

Whilst cross certification is currently not described in the ISO 15118 standard [ISO 15118-2], it will be included in the future ISO 15118-20 specification. Furthermore, additional documentation that describes concepts such as contract certificate pools as a complementary mechanism for an operational ISO 15118 ecosystem would need to be adjusted. Technical aspects need to be described: cross certification can, for example, either be achieved by adding the cross certificates to the client side trust store (in the case of ISO 15118-2: the EV) or by letting the server side (ISO 15118-2: Charging Station) provide the correct certificate chain during the TLS setup. In this chapter we assume that this is up to the Charging Station.

^① In the ISO 15118-2 specification, the certificate profile of the V2G Root CA does not specify a path length constraints. However, one of the ISO 15118-2 requirements states that the path length constraint of the PKI certificate tree shall be limited to 3.

Sub CA1 level

The main disadvantage of the previous approach is that an additional layer in the PKI structure of ISO 15118 would have to be introduced if two Sub CA levels are desirable. An alternative could be to do cross certification



between the V2G Root CA level of one PKI and the Sub CA 1 level of the other PKI (instead of cross signing two V2G Root CAs). This approach would not require an additional level. This approach is visually represented in the figure on the right. In this approach, for each relevant certificate on the Sub CA1 level, a cross certificate should be created, where “relevant” means that it is used by the EV or Charging Station for Transport Layer Security (TLS) connections or verifying certificates. Depending on the structure of the PKI, this could be a large amount of cross certificates, which would ultimately

need to be maintained, leading to high maintenance complexity. An estimation of the scalability for adding PKIs is as follows:

- To enable Plug and Charge using cross certificates for two PKIs would mean the following amount of cross certificates: #CSO Sub CA1 certificates PKI-1 + #CSO Sub CA1 certificates PKI-2
- For certificate installation a similar calculation can be used for two PKIs: #CPS Sub CA1 certificates PKI-1 + #CPS Sub CA1 certificates PKI-2



Please note that cross certification on a Sub CA1 level could lead to a very high number of cross certificates if there is a large number of Sub CA1 certificates. The calculation above is for the number of cross certificates between 2 V2G Root CAs. Again for interoperability between n PKIs, the above calculation would be applicable for each $n(n-1)/2$ - “full graph” – PKIs interoperability relations. Therefore this option only seems feasible and maintainable if both PKIs have very few Sub CA1 certificates, preferably only one. This would mean that the Sub CA1 level would also be used by the V2G Root CA operator.

When cross certification is applied on Sub CA2 level, the number could become very high, since the calculation would be applicable for CSO and CPS Sub CA2 certificates (and should be done for each Sub CA1 certificate). Assuming that Sub CA2 certificates are used by individual CSOs, this could potentially letting the number of cross certificates “explode”. We therefore would not advise to use cross certification on the Sub CA2 level.

Choosing level to apply cross certification

The level where cross certification is applied can be based on the number of cross certificates involved (that bring about additional maintenance[¶]) or on the number of additional layers involved. If cross certification is applied higher in the hierarchy (i.e. “closer” to the Root CA) the resulting ecosystem will involve less cross certificates and therefore reduce complexity. However, it must be taken into account that if cross

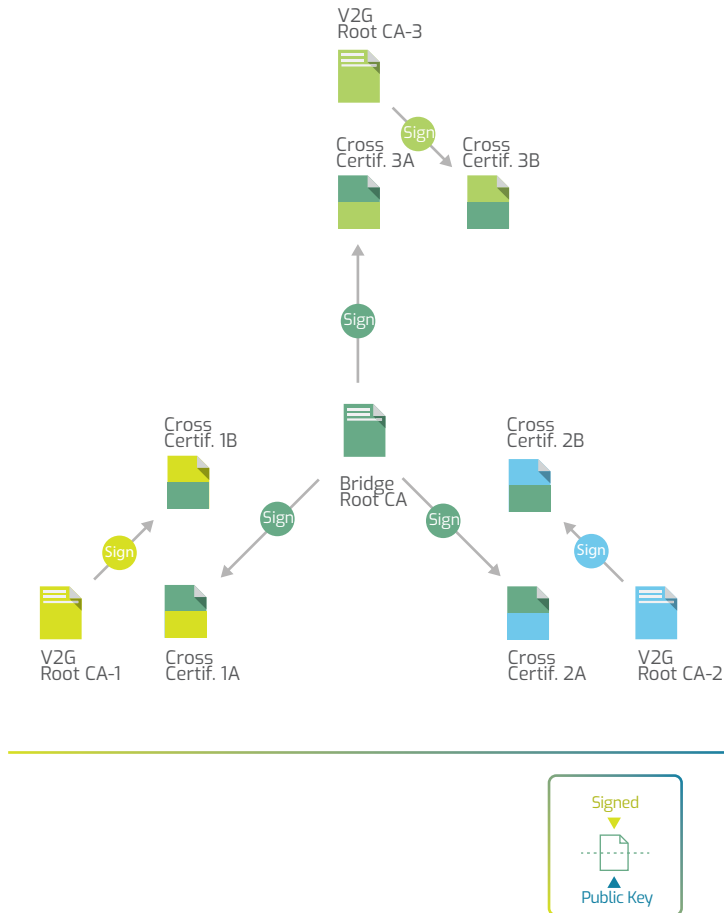
¶ Maintenance includes key ceremonies, renewing certificates and, of course, installing the right cross certificates on the right device / system.

certification is applied higher in the hierarchy, the trust relation with the other PKI entails trusting more certificates from the other PKI, since it means trusting all certificates below the certificate from the other PKI that is cross signed. When signing on Root CA level and leaving out a Sub CA level (to “compensate” the extra PKI level), it also means that the Root CA cannot be stored offline anymore. Please refer to Part 3 of this document for more information about quality rules that are needed for PKI interoperability.

In our demonstration project that is described in this chapter, we applied cross certification on Root CA level, because this seemed to be the most relevant from a research perspective and the most practical option (based on the expected maintainability) that can also already be applied with ISO 15118-2 (based on the number of layers).

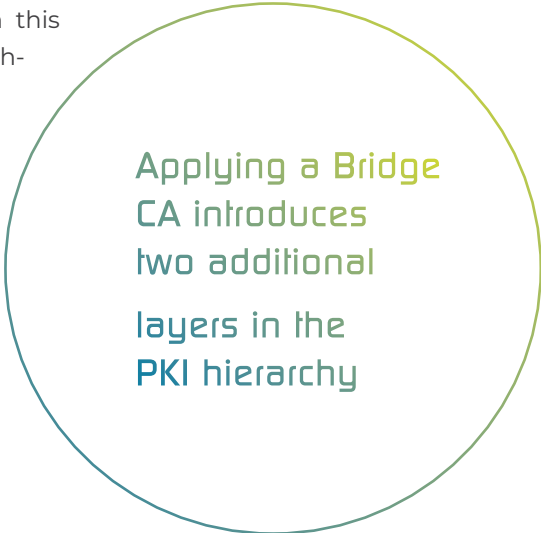
14.1.3. Bridge CA

A technical solution for the increasing amount of cross certificates could be a bridge CA. This approach is visualised in the following figure. By adding an additional “Bridge CA layer” the many to many relations between all PKIs become a relation between each PKI with the (same) Bridge root CA, keeping the amount of cross certificates needed to be interoperable relatively small. To add a V2G Root CA to the system would require two additional cross certificates, for the entire system (instead of two additional cross certificates per existing V2G Root CA when cross certifying on Root CA level).



Applying a bridge CA makes the cross certification solution more scalable and more suitable for large amounts of V2G Root CAs. Even with a small number of PKIs the scalability (amount of cross certificates) when adding a new PKI becomes clear: when using cross certificates on Root CA level without using a bridge CA, the amount of cross certificates for 2 PKIs is 2, for 3 PKIs it is 6, i.e. the number of cross certificates grows with 4. When applying a bridge CA, the amount of cross certificates would grow with 2. When the number of PKIs increases, the scalability effect is even larger. The consequence of this approach is that it would require two additional levels in the ISO 15118 PKI when used on V2G Root CA level. When looking at the schematic overview, a certificate from, for example, V2G Root CA 1 could be verified by V2G Root CA 3 by using the (additional) cross certificates “Cross Certificate 1a” and “Cross Certificate 3b”.

As mentioned, applying a Bridge CA introduces two additional layers in the PKI hierarchy. Although this option would make the cross certification mechanism more maintainable, this option cannot be applied to the existing ISO 15118-2 version and is therefore only explained here for completeness, but was not further demonstrated.



Applying a Bridge CA introduces two additional layers in the PKI hierarchy

14.2. Impact on existing implementations

When implementing cross certificates to achieve interoperability between two ISO 15118 PKIs, a number of changes to the entire chain is necessary. In the following paragraphs, these changes are listed per component or protocol that is present in the setup that was used. The setup used for this discussion, is represented in the following figure, that includes a central hub that provided the necessary certificate pools: the OEM Provisioning Certificate Pool and the Contract Certificate Pool.

Using Cross Certification in an ISO 15118 ecosystem involves:



- A** Setting up the TLS communication between an EV and Charging Station from different PKIs
- B** Using cross certification for verification of the Certificate Provisioning Service (CPS) certificate (chain)
- C** Handling additional contract certificate chain verification by the Charging Station, which is done by verifying with V2G Root CA or MO Root CA certificates

Point **c** will be addressed separately in 14.5

14.2.1. Impact on ISO 15118 implementations

Impact on the EV implementation of ISO 15118

The impact for the EV concerning the ISO 15118 communication involves three different parts:

1. Handling cross certificates in the TLS communication. The EV must be able to execute a TLS connection with a Charging Station that has a certificate derived from a V2G Root CA from another

PKI and from its own PKI. During the interoperability testing with different components, it seemed that not all EV side components were prepared for accepting a certificate chain containing an additional cross certificate (as provided by the Charging Station). This seemed to depend on the implementation on the Charging Station side and the EV side (see 14.3). Some implementations worked directly, without any changes. For some implementations, to handle both the situation that an EV connects to a Charging Station from its own PKI as well as from another PKI, the EV must send its list of currently installed V2G Root CA certificates to the Charging Station. Without this, the Charging Station was unable to form a certificate chain with the appropriate cross-certificate that can be verified by the EV. This can be done by implementing the “trusted_ca_keys” extension in the TLS ClientHello message. The current ISO 15118-2 standard requires an EV to use this extension, although it does not define which identifier type (i.e. key_sha1_hash, x509_name, cert_sha1_hash) to use for the “trusted_ca_keys” extension^Δ. Thus, the EV shall calculate the hash values of all its installed V2G Root certificates and include these with the TLS ClientHello message via “trusted_ca_keys” extension.

^Δ The upcoming version of the standard (-20) is expected to require an alternative extension for this: the “certificate_authorities” in the ‘ClientHello’ message as defined in IETF RFC 8446.

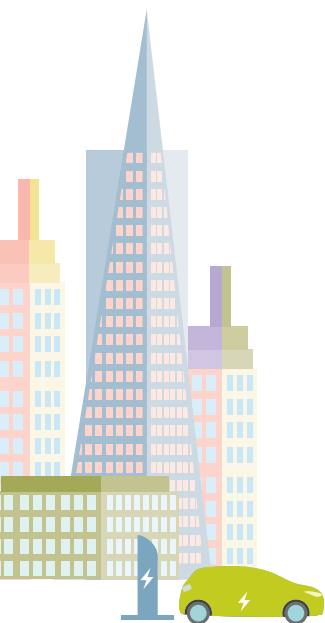
The setup was tested with 2 PKIs. When using more than 2 PKIs, more cross-certificates will be provided to the EV, meaning the TLS handshake could take more time as the TLS library on Charging Station side has to look for the correct cross-certificate. This has to be taken into account when measuring the timeout on the EV side.

2. Handling additional cross certificate layer in certificate provisioning service certificate chain.

During Certificate Installation, the EV receives an EXIResponse that contains the contract certificate to be installed. This message is signed by the Certificate Provisioning Service (CPS). The CPS certificates are also included in the certificate installation message. The EV must be able to verify this chain, which might include the cross certificate depending on the CPS and the list of Root CAs that the EV trusts. When cross signing on Root CA level, this implied that the verification of the CPS chain must allow for an additional fourth level in the PKI (for the cross certificate). Although the ISO 15118-2 message schemes allow for four certificates, existing implementations are expected not to allow for this based on ISO 15118-2 requirement validations, since these explicitly limit the number of certificates to three. See 14.2.3 for more information on the CPS role.

3. Handling additional cross certificate layer in contract certificate chain.

- a.** Certificate installation. During Certificate Installation, the EV receives an EXIResponse that contains the certificate to be installed. This message includes, besides the above mentioned CPS chain, the contract certificate chain, excluding the V2G (or MO) Root CA certificate, which is the trust anchor of the EV. To be able to use the contract certificate, at first sight it seems that a chain from the V2G Root CA of the EV to the contract certificate could be established for verification by the EV, however this is not required according to the ISO 15118-2 specification. In order to do so (and for the previous point), the EV must provide its list of Root CA IDs to the Charging Station. Based on this list, a contract certificate including a valid chain can be provided to the EV. The EV in turn must be able to handle this message containing the contract certificate, that might also include a cross certificate in the certificate chain.



- b. Plug and Charge. For Plug and Charge authentication the EV must provide its contract certificate chain in the PaymentDetailsReq message. This should not necessarily include the cross certificate, as long as the Charging Station has the correct V2G Root CA (or MO) certificate or a cross certificate to verify the chain of the contract certificate of the EV.

Impact on the Charging Station implementation of ISO 15118

On the Charging Station side, the impact consists of the following points, that are similar to EV considerations:

1. Handling cross certificates in the TLS communication. The Charging Station must, in case of cross certification on Root CA level, support an additional PKI layer and it must support TLS communication based on cross certificates. During the TLS handshake, the Charging Station must provide a chain of certificates that can be verified by a V2G Root CA certificate that is present in the EV. Depending on the V2G Root CA certificates installed in the EV the Charging Station must include the cross certificates to achieve interoperability through cross-certification. As mentioned above, the EV must use the "trusted_ca_keys" extension in the TLS ClientHello message (according to the ISO 15118-2 specification[‡]). The Charging Station in turn must check the "trusted_ca_keys" extension field and use this to create a valid certificate chain.

During the interoperability testing with different components, it seemed that not all components were prepared for this feature. This depended on the implementation on the Charging Station and EV, offering / validating the certificates in the right order (see 14.3).

[‡] The ISO 15118-20 is expected to require the "certificate_authorities" extension as defined in IETF RFC 8446.

2. Plug and Charge. For Plug and Charge authentication the Charging Station must be able to process a contract certificate chain in the PaymentDetailsReq message that may have one additional layer. This does not necessarily include the cross certificate, as long as the Charging Station has the correct V2G Root CA (or MO) certificate or cross certificates to verify the chain of the contract certificate of the EV.

It is worth noting that only the ISO 15118-2 requirements limit the path length of the PKI certificate tree to 3 (V2G RootCA certificate / Sub CA1 certificate / Sub CA2 certificate), thus, not allowing the inclusion of a cross certificate on the Root CA level since this increases the path length to 4. The ISO15118-2 XML schema document used for encoding and decoding V2G messages to EXI has defined the max occurrence of the certificate-Type within the SubCertificatesType to 4 (see [ISO 15118-2]). As a result, the EV and the Charging Station could append two additional certificates to the SaprovisioningCertificateChain and the ContractSignature-CertChain without facing any encoding or decoding errors.

Summary of the impact when applied on Root CA level

In summary, to make cross certification work on Root CA level, the following points should be addressed: see table.

		Supported by ISO15118-2 EV	Supported by ISO 15118-2 CS	Supported in ISO 15118 Specification	
				-2	-20***
1	Handling cross certificates in the TLS communication mechanism.				
	When using 1 PKI layer for cross certificates	✓/—*	✓/—*	✓/—*	✓
	When all PKI layers used: an additional layer in the PKI structure must be allowed	—	—	—	✓
2	Provisioning certificate validation, when assuming cross certification on Root CA level:				
	When using 1 PKI layer for cross certificates	✓	✓	✓	✓
	When all PKI layers used: an additional layer in the PKI structure must be allowed	—	—	—	✓
3	Contract certificate validation, when assuming cross certification on Root CA level:				
	When using 1 PKI layer for cross certificates	✓**	✓	✓	✓
	When all PKI layers used: an additional layer in the PKI structure must be allowed	—	—	—	✓

* Depending on correct implementation of the TLS handshake mechanism

** If contract certificate is not validated (as specified in ISO 15118-2)

*** As understood from the current draft version.

Applying cross certification with existing ISO15118-2 implementations

In the current ISO15118-2 specification, the PKI hierarchy has a predefined structure and number of layers. This structure includes two Sub CA layers, one of which is optional. As explained in this chapter, paragraph 14.1, when cross certification is applied on Root CA level, this would introduce an additional layer in the hierarchy for some certificates. One of the reasons that cross certification is sometimes regarded as “not possible”, is that it would conflict with existing implementations available, since when all layers are already in use for a specific certificate, an additional layer would exceed the maximum. Based on our research and based on the current implementations in the field, this is not an issue from a technical perspective. When looking in more detail, when cross certification is applied in the infrastructure, interoperability between PKIs can already be achieved:

- When applying cross certification on Root CA level for PKIs that do not have all Sub CA layers in use for Charging Station and CPS certificates.
- When applying cross certification on Sub CA level for PKIs that already have all Sub CA layers in use for Charging Station and CPS certificates.

Furthermore, both types of certificates could be replaced by certificates with a shorter chain in existing implementations without any impact, except of course for (re-)creating and updating existing certificates. This is illustrated in the figure below for the Charging Station certificates.

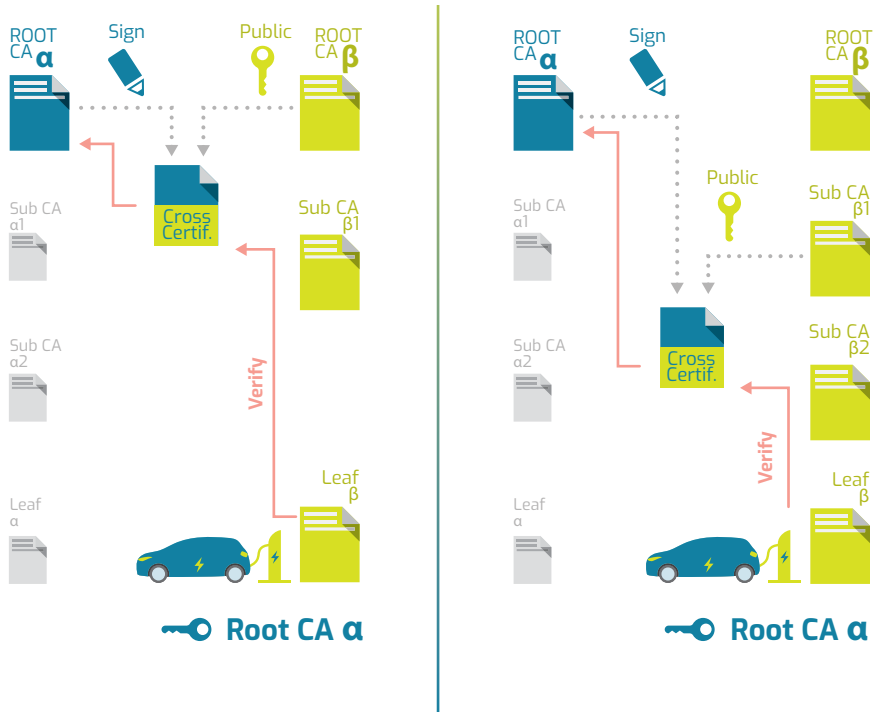


Figure 5: applying cross certification to existing implementations

Applying cross certification on Root CA level

In the example on the left side we have a PKI **a** that uses all layers. For setting up the connection between an EV and Charging Station, the EVSE certificate is verified by the EV during the TLS setup and the contract certificate is verified by the Charging Station. In case that an EV from PKI **a** would charge at a Charging Station from PKI **b**, as illustrated in the figure, this could be achieved by using cross certification, provided that the hierarchy from PKI **b** does not use all Sub CA layers for EVSE and CPS certificates. In this case, when connecting to a Charging Station, the EV would receive an EVSE certificate chain consisting of 4 certificates up to its own trust anchor, Root CA **a** (Leaf **b**, Sub CA **b1**, Cross Certificate, Root CA **a**).

When an EV from PKI **β** wants to charge at an EVSE from PKI **α**, this is not possible by using cross certification, because then the maximum amount of layers would be exceeded.

So a more concrete (hypothetical) example: an ElaadNL V2G Root CA / Driivz Sub CA1 / EVBox Charging Station could charge with an EV that has a Hubject V2G Root CA installed and even install a contract certificates with a Hubject V2G Root CA / Hubject CPS Sub CA1 / Hubject CPS signer, if ElaadNL and Hubject would cross certify. An EV with an ElaadNL V2G Root CA cannot charge at a Hubject V2G Root CA / Ionity Europe CSO Sub CA1 / Ionity Germany CSO Sub CA2 / Ionity leaf certificate charger.

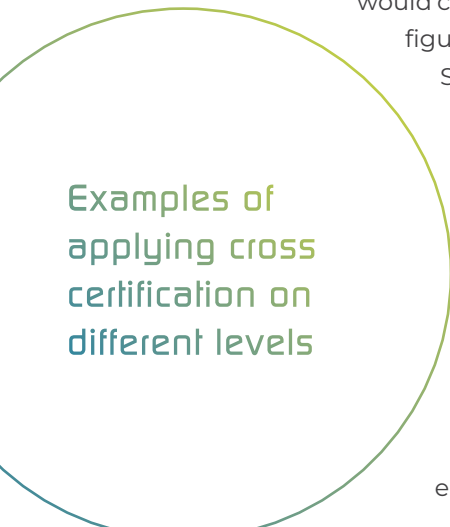
Applying cross certification on Sub CA level

In the example on the right side we have a PKI **α** that uses all layers. Here cross certification on the Sub CA 1 level is applied. Again, for setting up the connection between an EV and Charging Station, the EVSE certificate is verified by the EV during the TLS setup and the contract certificate is verified by the Charging Station. In case that an EV from PKI **α**

would charge at a Charging Station from PKI **β**, as illustrated in the figure, this could be achieved by using cross certification on Sub CA1 level. In this case, when connecting to a Charging Station, the EV would receive an EVSE certificate chain consisting of 4 certificates up to its own trust anchor, Root CA **α** (Leaf **β**, Sub CA **β2**, Cross Certificate, Root CA **α**).

This option would mean that for CSOs only one Sub CA level is available, so they will not have the option of having, for example, regional Sub CAs. However, we believe that this “sacrifice” by the CSOs in exchange for only joining one PKI and having interoperability with other PKIs is worth the sacrifice.

So a more concrete (hypothetical) example: the chain ElaadNL V2G Root CA / Allego Sub CA1 / Allego Europe Sub CA2 / EVBox Charging Station would not be possible anymore, instead the chain would be Elaad-



Examples of
applying cross
certification on
different levels

NL V2G Root CA / ElaadNL Sub CA1 / Allego Sub CA2 / EVBox Charging Station. If the ElaadNL Sub CA1 cross certificate would be cross signed by the Hsubject V2G Root CA, an EV that has the Hsubject V2G Root CA in its trust store, would be able to charge at the EVBox Charging Station from the example.

Consequences for current implementations

This means that if (the PKI operator of) a V2G Root CA decides to use one of the Sub CA1 layers for themselves and the Sub CA2 for CSOs, cross certification on Root CA level with the ISO 15118-2 will not be possible. A valid reason for using this Sub CA1 layer for the V2G Root CA operator is that the V2G Root CA is stored offline for security reasons.

Alternatively, cross certification on the Sub CA level will be possible, but could lead to more cross certificates to maintain in the ecosystem. This depends on the number of Sub CA certificates used on the Sub CA1 level. This should be kept as small as possible for maintenance reasons, but here PKIs are dependent on how each PKI fills in its layers.



Based on the above discussion, we propose, to enable Cross Certification in Europe, to dedicate one layer for the purpose of Cross Certification by applying cross certification on Sub CA1 level together with reducing the Sub CA1 layer for CPS and CSO certificates to one.

At this point in time there is to our knowledge no negative impact on existing implementations (except a one-time certificate chain replacement). We do not advise to use cross certification on a Sub CA2 level, since this could highly increase the number of cross certificates in the ecosystem.

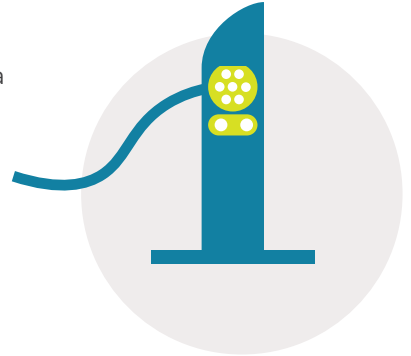
Cross certification in the upcoming ISO15118-20 specification

As we have understood from the current draft of the ISO 15118-20 version (October 2021), the new version introduces the concept of cross certification. This means it allows an additional layer in the PKI structure (if used for a cross certificate). It does not mandate where cross certification must be applied, this is left to the implementers. It only provides examples, such as cross certification between a V2G Root CA and OEM Sub CA, which can be used for verification of a newly introduced vehicle certificate for TLS with mutual authentication. No detailed example is provided of cross certification between V2G Root CAs.

14.2.2. Impact on OCPP 2.0.1 implementations

Impact on Charging Station implementations

Currently, it is possible to install a cross-certificate in a Charging Station but to specifically indicate that it involves a cross certificate, an extension mechanism of OCPP must be used. To be more specific: the enumeration of the certificateType in the InstallCertificateRequest message does not have a value for a “cross certificate”. For this reason, the following approach can be used:



- Cross-certificates are added via OCPP 2.0.1 use case M05, using the InstallCertificateRequest message
- In this message, the field certificateType has the value 'V2GRoot-Certificate'
- Furthermore, the message is extended with an additional customData object with the following fields:
 - VendorId = 'VendorXYZ'
 - CertificateSubType = 'CrossCertificate'

For demonstrating the approach to support cross-certification on the Charging Station side, the following has been done:

The cross-certificates were added to trust store and key store of the Charging Station. Theoretically a Charging Station could try to fetch the cross certificate from the CSMS if the one supported on EV side is not “cached” locally, but in practice this will add a lot of time impacting the user experience. Furthermore, this would imply a larger change in the standards used.

When an EV arrives at the Charging Station, the Charging Station chooses the V2G Root CA certificate it uses for setting up the TLS connection.

Impact on CSMS implementations

Similar to the Charging Station, the OCPP 2.0.1 implementation on the CSMS side can be extended to support the installation of cross certificates. This can be done using the approach described in the previous paragraph, via OCPP 2.0.1 use case M05, with a customData extension.

Summary of the impact on OCPP2.0.1 implementations

In summary, to make cross certification work, the only point that should be incorporated in OCPP 2.0.1 implementations in both Charging Stations as well as CSMS's is enabling the installation of cross certificates in a Charging Station. This is currently supported by the current customization mechanisms of OCPP. Please note that customizations that are applied, could also be added to a next version of the protocol specification.

14.2.3. Certificate pool functionality

Communication

In a demonstration setup, a central hub was used that fulfilled the role of OEM certificate pool and contract certificate pool. When an EV requests a certificate (installation) at the Charging Station, this request is forwarded via OCPP 2.0.1 to the CSMS. The CSMS in turn fetches the contract certificate at the central hub. This contract certificate was created by an EMSP (using the OEM provisioning certificate for encrypting the private key) and sent to the central hub. In our setup, the central hub was responsible to return the certificate and signing the message using the Certificate Provisioning Service (CPS) certificate.



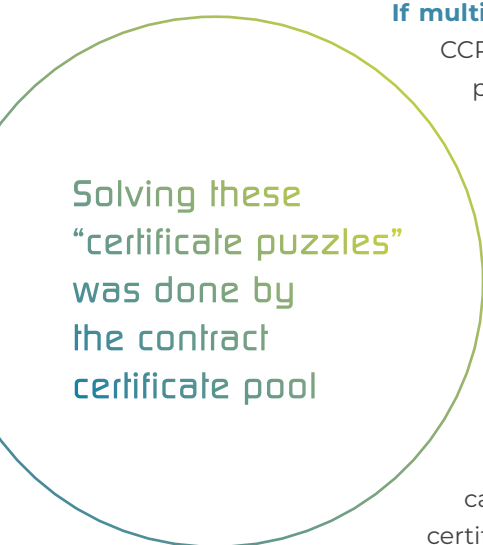
In case of cross certification, only one change was needed in the communication to the central hub: the list of root certificate IDs from the ISO 15118-2 CertificateInstallationReq message was added to the message to the central hub (along with the already existing fields, such as PCID). The impact on the functionality, however, was bigger, which is explained in the next paragraph.

Functionality

When the contract certificate pool (CCP) receives a request for a certificate (for installation) that originates from an EV, it can find the right contract certificate based on the PCID (or eMAID) from the request. The list of root certificate IDs from the ISO 15118-2 CertificateInstallationReq message that was added to the communication to the central hub, is necessary to build a complete certificate chain towards one of the root certificates from the list sent by the EV, since the EV only trusts certifi-

cates it can validate with one of its own pre-installed “trust anchors”. In case that the list of root certificate indicates that the EV is from a different PKI than the certificate of the CPS (in our setup: the central hub), a cross certificate is needed by the EV to be able to establish a complete chain to its V2G Root CA for verifying the CPS certificate.

Please note that the time restrictions for the installation of a contract certificate are quite strict (5s response time from EV to CCP and back). For this reason, current CCP implementations often prepare (signed) contract certificate bundles beforehand. Responses messages to contract certificate installation requests are prepared and signatures of the CPS are already added (sign operation often causes delays).



Solving these
“certificate puzzles”
was done by
the contract
certificate pool

If multiple V2G Root CAs apply cross certification, and the CCP wants to prepare a response, a response will have to be prepared for each possible V2G Root CA. Reason for this is that the CCP has to respond with a CPS certificate chain that can be validated by the EV, but the CCP does not know in advance which V2G Root CA the EV has (pre)installed. Depending on the V2G Root CA of the EV, the CCP should return a response, containing a CPS certificate chain that the EV will trust. This will add some additional burden (memory, preparation, clean-up and logic) in the CCP.

Similarly, in case that the list of root certificate indicates that the EV is from a different PKI than the contract certificate that was sent to the contract certificate pool by the EMSP, the contract certificate chain that is returned to the CSMS could contain a cross certificate to allow the EV to verify the complete chain of the contract certificate. However, since this is not required by the EV according to the ISO 15118-2 specification, including the cross certificate in the contract certificate chain is optional.

The functionality for solving these “certificate puzzles” was added to the contract certificate pool, allowing an EMSP to upload a certificate, even for EVs from another PKI.

For example: when the contract certificate pool receives a message from a PKI with a Root CA named OTHER-PKI, it should establish a provisioning certificate chain consisting of:

V2G Root CA from OTHER-PKI (does not have to be included in the message, since the EV has that one as "trust anchor")

Cross certificate with issuer referring to the V2G Root CA from the OTHER-PKI

Sub CA1 (in our setup: the central hub certificate)

CPS Sub CA2

CPS certificate

In case that (over the years) multiple cross certificates exist that can create a path to the V2G Root CA from the OTHER-PKI, the central hub / contract certificate pool should also validate the chain itself, implying that it should not only store the cross certificates, but also the V2G Root CAs that have signed the cross certificates. In this case, the central hub / contract certificate pool can verify the chain before responding back to the request from the EV.

The definition of this functionality is currently not part of any standard or supporting document. The functionality and the rules that should surround it, could be added to the documentation related to certificates such as the VDE Anwendungsregel [VDE-AR] or in its successor, the CharIN PKI Interoperability document (reference CharIN-IOP) that fills

in the open spots in the functionality for creating a working ISO 15118 ecosystem.

In the VDE Anwendungsregel [VDE-AR] the concept of a directory service was already introduced, to deal with having more than 1 contract (or OEM) certificate pool. When having multiple PKIs this should map PCID or EMAID to a reference to the correct certificate pool. This should be a certificate pool of any of the PKIs in the ecosystem.

14.2.4. VDE Anwendungsregel / CharIN PKI Interoperability document

Plug and Charge with EV from other PKI

The VDE Anwendungsregel [VDE-AR] introduces the concept of contract certificate pool for preparing and storing contract certificates, which in our setup is implemented in the central hub. The changes to be added to this documentation for the Plug and Charge functionality would consist of describing a repository where cross certificates can be found, similar to (or even in) the VDE-AR Root Certificate Pool.



Certificate installation from other PKI

In order to execute a certificate installation, functionality was added for composing a contract certificate message based on list of root certificate IDs. The reasoning behind this is that every EV could then be able to get a certificate at every Charging Station. The current approach described in the VDE Anwendungsregel introduces the concept of directory services, which could be used to determine where contract certificates are, as a "signpost" pointing to the right contract certificate pool to access

contracts of different EMSPs. In our setup, the choice was made to also include cross certificates in the certificate installation, since this would mean that contract certificates could be stored at different contract certificate pools and CSOs should only have access to one of these because of the use of cross certificates.

14.2.5. CharIN Certificate Policy

Currently, CharIN has defined a certificate policy guideline [CharIN-CP], which states the rules to be followed for PKIs that want to be a “CharIN approved” PKI for ISO 15118 (in the future). When cross certificates become integrated into the ISO 15118 ecosystem, this would also imply a number of requirements that must be added to this certificate policy:

- Quality / auditable requirements that a PKI must fulfil before it is “trusted” enough to allow for cross certification with other “CharIN approved” PKIs^Y.
- Requirements for PKIs to allow for cross certification once another PKI meets the requirements from the Certificate Policy

^Y This would also mean that existing PKIs in the market might have to update their Certificate Policy.

14.3. Technical issues encountered

During testing the test setup for testing cross certification, we encountered some issues / details that must be addressed to ensure interoperability.

- Technical issues were encountered during the TLS communication setup when using cross certificates. These were solved correctly by applying the `trusted_ca_keys` extension (as required by the ISO 15118-2 specification). Not all available TLS libraries have implemented the “`trusted_ca_keys`” extension from the ClientHello message. Both the EV (TLS client) and the Charging Station (TLS server) should configure or, if needed, customize its TLS library in order to enable the “selection process” of the correct CSO certificate chain. Alternatively the client could store cross certificates in its trust store. However, in case of cross certification on Root CA level this would be equivalent to storing additional Root CA certificates. Since the mechanism is part of the ISO 15118-2 specification and the ISO 15118-20 draft specification (“`certificate_authorities`”), we propose to add verifying the correct working of this mechanism to the ISO 15118 certification program and further explain the use of this mechanism in the CharIN Interoperability Guide including the identifier types to use.
- Some publicly available TLS stacks couldn't verify the chain when the ordering of the DN attributes is not identical. Validations of certificates and fetching of certificates at the central hub were adjusted to deal with this. Furthermore, when creating a cross certificate, the CSR must be created using the subject fields in the right order. We propose to standardise the order of the certificate subject attributes in the CharIN Interoperability Guide.

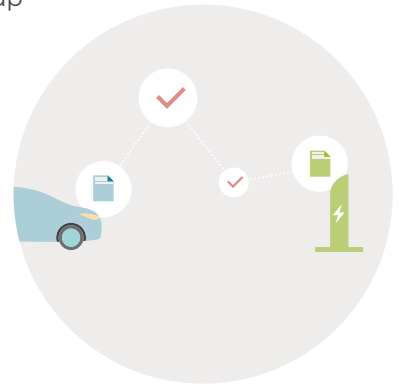
14.4. Impact of Cross Certification on hardware requirements

Cross Certification only adds hardware requirements to Charging Stations, not to the EVs^φ. The impact on the hardware used when bringing the cross certification in practice is limited. The amount of certificates in the Charging Station was larger, using up more memory. The amount of extra memory that is needed, is dependent on the amount of PKIs and the amount of cross certificates in use.

The certificate size in ISO 15118-2 is 800 bytes, so based on the calculation from 14.1.2, the memory impact on the Charging Station when applying cross certification on Root CA level for n PKIs would be:

So, for example, for 5 PKI's^θ this would be $5 \cdot 4 / 2 \cdot 2 \cdot 800 =$

$$\frac{n(n-1)}{2} * 2 * 800 \text{ bytes}$$



^φ To be precise: when applying cross certification, the EV actually does not have to store all V2G Root CAs, so it could actually reduce the required memory in the EV. It might require an additional revocation check for the cross certificate since the use of OCSP-stapling for this certificate is not foreseen in the ISO 15118 specification.

16.000 bytes \approx 15,6 kB.

Since the number of certificates for a V2G Root CAs must be between 1 and 10, based on the validity requirements (V2G2-878) from [ISO 15118-2], the maximum certificates for which cross certificates are needed, would be much higher.

However, one could wonder whether the amount of 10 would be needed in practice. One would expect these to be smaller, due to the 5 year period in between certificates. OEMs could for example only prepare for 2 V2G Root CAs at a time instead of 10, one “old” and one “new” certificate. This would change the amount of memory for cross certificates to:

For 5 PKIs this would result in $10 \cdot 9 / 2 \cdot 2 = 90$ cross certificates or

$$\frac{2n(2n-1)}{2} * 2 * 800 \text{ bytes}$$

$90 \cdot 800 = 72.000$ bytes \approx 70 kB. Managing a high number of cross certificates would require additional effort from each PKI operator and would also require CSOs to manage these cross certificates in their Charging Stations. This managing not only involves adding new certificates, but also handling updates of certificates and revocations of certificates.

Please note that with the introduction of newer versions of the ISO 15118 standard [ISO15118-20] it can also be expected that there will be technical reasons for introducing new certificate types or hierarchies, introducing a new V2G Root CA certificate.

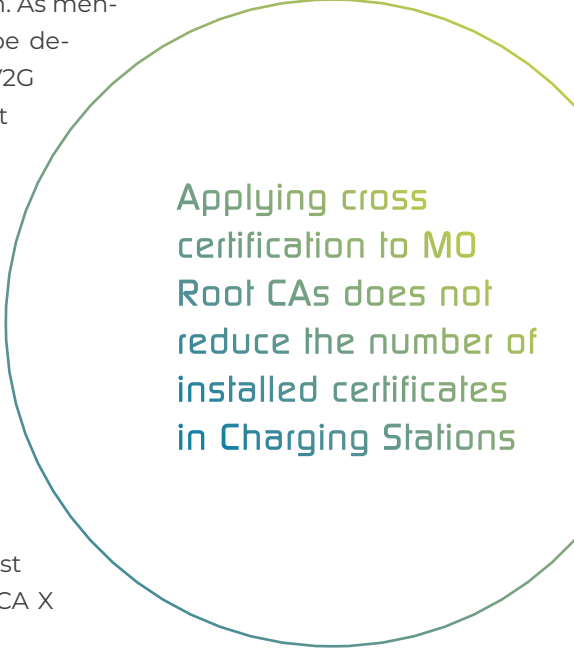
ⓘ Please note that this is per generation and this number can be higher (e.g. old / new or if other types of certificates are used in the future)

14.5. Contract certificate chain verification

In the ISO 15118 specification, contract certificates, which are created by EMSPs (or MOs), can be derived from the V2G Root CA or from an MO Root CA. It is up to the EMSP to choose whether it wants to operate its own MO Root CA for contract certificates, although the EMSP remains dependent on the Certificate Provisioning Service (that is derived from the V2G Root CA).

In the above chapter, the main focus was on the TLS connection and installation of contract certificates. The verification of contract certificates can be done at the Charging Station. As mentioned above, these contract certificates can be derived from an MO Root CA certificate or the V2G Root CA certificate. In order to verify contract certificates, the Charging Station needs to install in its trust store all applicable V2G Root CA certificates and MO Root CA certificates. One could use cross certificates for verifying contract certificates up to a V2G Root CA, but this does not impact the number of certificates that needs to be added to the Charging Station trust store. If a Charging Station trusts contract certificates derived V2G Root CA X and also wants to trust contract certificates from V2G Root CA Y, it can either add this V2G Root CA Y certificate to its trust store or a cross certificate between V2G Root CA X and Y.

For MO Root CA certificates, cross certificates could in theory also be used, but here the same logic applies: it does not reduce the number of installed certificates in Charging Stations and it would require cross certification (and thus bilateral agreements) between MO Root CAs.



Applying cross certification to MO Root CAs does not reduce the number of installed certificates in Charging Stations

14.6. Summary

In summary, using cross certification is an option for PKI interoperability that could be applied in an ISO 15118 EV ecosystem. When dedicating 1 certificate layer for cross certification, it could already be applied for ISO 15118-2, provided that the TLS setup is supported by EVs and Charging Stations. During testing we found that not all test-implementations supported this TLS setup, so this point would need attention in the ISO 15118 Certification Program and should be further explained in the CharIN Interoperability Guide. The impact on the implementations of other devices / systems in the EV ecosystem is limited (and doable), as described in this chapter.



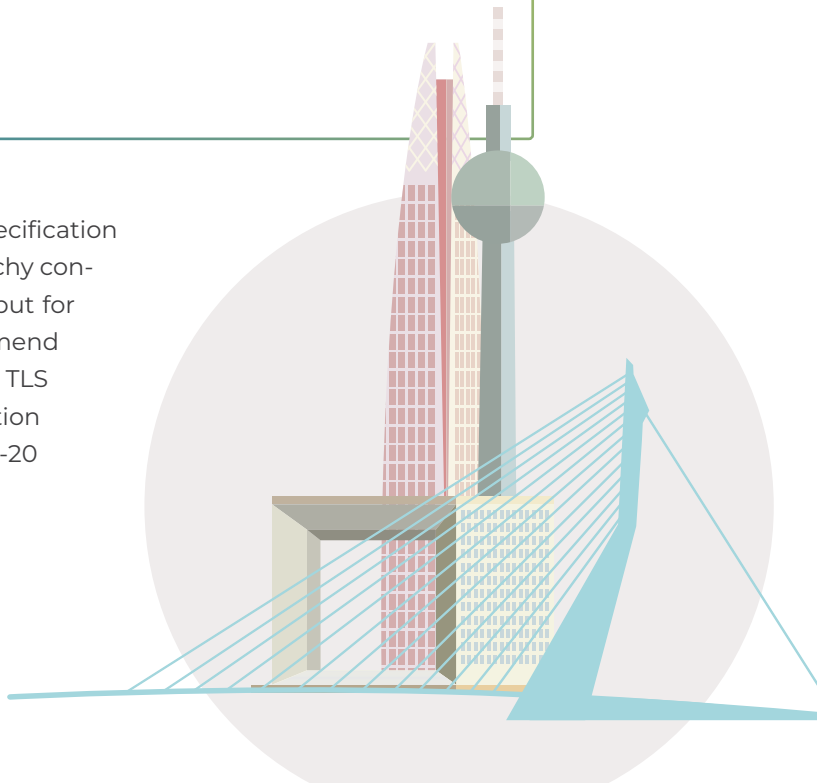
When cross certification is in place, the EV manufacturer can install one V2G Root CA certificate and this will then work everywhere (either direct or because of cross certificates being available).

14.7. Recommendations

Based on our work described in this chapter, we believe that if cross certification would be chosen as an interoperability mechanism for ISO 15118-2, the following would need to be done:

- Dedicate one certificate layer in the Charging Station and CPS certificate chains for cross certification on Sub CA1 level, meaning that the CSO can only become Sub CA2 in the PKI hierarchy
- Standardize TLS behaviour inside the CharIN Interoperability Task Group
- Verify this TLS behaviour during the ISO 15118 Certification Program.

The ISO 15118-20 (draft) specification is prepared for a PKI hierarchy containing a cross certificate, but for this version we also recommend to pay attention to the TLS handshake implementation as specified in the ISO 15118-20 specification.



15. CERTIFICATE TRUST LISTS IN PRACTICE

15.1. Certificate Trust Lists explained

15.1.1. General explanation

A Certificate Trust List (CTL) is a predefined list of items that has been signed by a trusted entity. Technically, a CTL can be anything, such as a list of hashes of certificates, or a list of file names. All the items in the list are authenticated (approved) by the signing entity, a trusted entity that puts its signature on the Trust List. For the purpose of ISO 15118 PKI interoperability, a CTL can be used to maintain and distribute a list of V2G Root CA certificates that are trusted in the market.

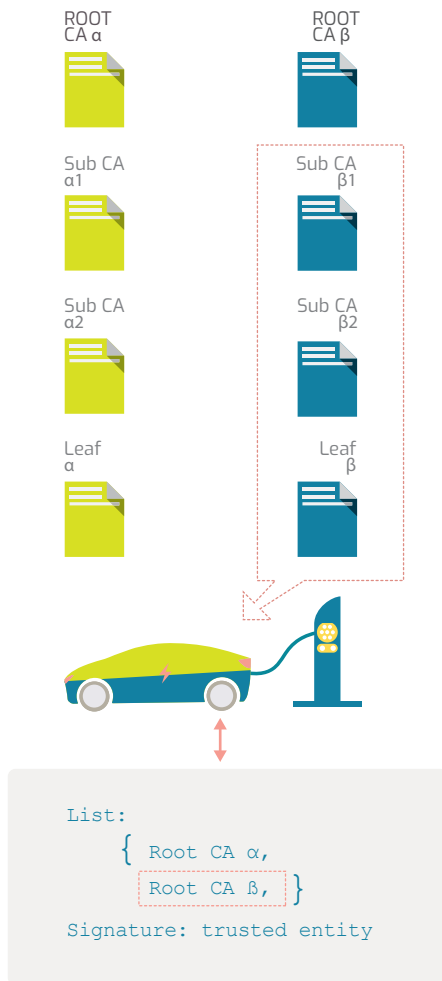
Applying a signature by a trusted entity means that once the signature of this signing entity has been verified, the items on the list are “trusted” by the receiver. In order to have interoperability between PKIs, i.e. to allow an EV that belongs to a PKI to charge at a Charging Station of another PKI, a Certificate Trust List with trusted V2G Root CAs can be sent to the EV. Once verified, all V2G Root CA certificates on the list, can be trusted and can be used for setting up the connection with an EVSE.

The figure on the right illustrates how a connection can be setup, when an EV with a chain derived from Root CA **α**, wants to establish a trust relation with a station with Root CA **β**:

When setting up the connection, the Charging Station must send the certificate chain, excluding the Root CA certificate, in this example Root CA **β**.

The EV receives this chain of certificates and can validate this using Root CA β that is on the certificate trust list and can thus build up the certificate chain to a “trust anchor”, knowing that Root CA β certificate is a trusted certificate based on the signature on the CTL. Using Root CA β certificate, the EV can thus verify the certificate chain derived from Root CA β and setup a connection.

In practice a system will not literally check a Root CA certificate on the CTL, the most likely usage of a CTL is as a secured and centralised way of managing trust stores of the different systems in the EV ecosystem. The actual certificate validations are done using these trust stores.



Trust List Manager

An important aspect of a Certificate Trust List is the trusted entity that adds / deletes certificates on the list and provides the signature that proves integrity of the list. This entity, called the Trust List Manager (TLM), is a role that must be trusted by all companies and systems in the market that is using the CTL. The TLM has strictly a governance role and does not have a business involvement in the PnC market. From a market perspective the TLM role is usually fulfilled by a neutral governmental organisa-

tion. Please refer to part 1 for more information on the requirements for guaranteeing the neutrality of this TLM.

The technical signature on the CTL must be verified by the receiver of the CTL using the public certificate of the Trust List Manager. It has to be taken into account that the receiver of the CTL must always be able to verify the signature, thus always needing the public certificate of the

TLM. This raises the question on how this TLM certificate must be distributed and managed. Besides installing this via a separate

mechanism, the approach could also be to make a new TLM certificate part of the CTL, where the CTL integrity is provided by the CTL. In addition, mechanisms can be used

such as signing the new TLM certificate with the old TLM certificate. When this is done, the receiver of the TLM can first verify the integrity of the entire CTL by verifying the signature using the current TLM certificate. As

a double verification the current TLM certificate can then be used to verify the new TLM certificate that is provided

in the CTL.



Applying a Certificate Trust List for ISO 15118

Using a Certificate Trust List in an ISO 15118 ecosystem involves, similarly to the Cross Certification, using a CTL for:

- Setting up the TLS communication between an EV and Charging Station from different PKIs
- Installing certificates for verification of the Certificate Provisioning Service (CPS) certificate (chain)
- Handling additional contract certificate chain verification by the Charging Station, which is done by verifying with V2G Root CA or MO Root CA certificates

When applying a CTL, the points a and b above are handled by providing a CTL with the right V2G Root CA certificates to the EV. If this is done, the TLS connection can be setup and the CPS certificate chain can be validated. Although point c is already handled in the existing OCPP standard and a CTL is not specifically needed here, this option will be considered as it could work together with one of the options for installing the CTL in the EV. This will be further explained in the next paragraphs.

15.1.2. Variants for distributing a CTL to an EV

If a CTL is used within a market, it has to be distributed for installation / updating in the systems. The primary focus will be on the EV, since applying a CTL in the EV can provide most of the needed interoperability between EVs and EVSEs from different PKIs. Using the CTL mechanism for other purposes is discussed later in this chapter.

Distributing a CTL to EVs can be done in multiple ways:

- 1** **Via the infrastructure:** sending it via the Charging Station to an EV using an ISO 15118 Value Added Service. The EV unpacks the CTL. **Variant-1**

- 2** **Via the telematics route:** the CTL is sent via the OEM to the EV. Two sub-options are possible: **Variant-2**
 - 2a** CTL in the vehicle: the CTL is sent to the OEM and forwarded to the EV. The EV unpacks the CTL and installs the individual certificates.

 - 2b** CTL extracted by OEM: the CTL is sent to the OEM, unpacked and the individual certificates are sent to the EV.

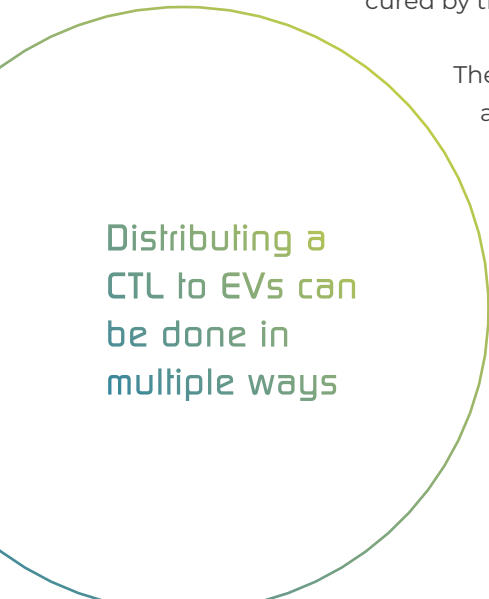
Please note that – **for variant 1** - when the CTL is signed by the TLM, the infrastructure variant can only be applied by providing the entire CTL to the EV, so that the EV can verify the signature.

Unpacking it at the CSO or in the Charging Station would mean that the EV cannot verify the signature on the CTL anymore and thus not verify the integrity of the CTL. Recreating the CTL in the Charging Station again and resigning it would not make sense, since the EV would then need to trust a random Charging Station instead of the TLM that created the CTL. In practice, this variant therefore does not seem realistic and therefore it is not further discussed.

For the telematics route **variant 2a**, (where the CTL is verified and unpacked by the EV), the OEM should implement this ‘unpacking’ feature in the EV similar to **variant 1**.

The most logical method seems to be that the CTL is verified and unpacked by the OEM, before it reaches the EV. The telematics route is secured by the OEM and the EV can of course trust its own OEM.

The table on the next page shows the advantages and disadvantages of these possible variants:



Distributing a
CTL to EVs can
be done in
multiple ways

No	Variant	Advantages	Disadvantages
1	Infrastructure route	<p>No effort from OEM via telematics communication needed.</p> <p>Signature on CTL provides certainty that the CTL has not been tampered with.</p> <p>Not depending on GSM module or 2/3/4/5G coverage</p> <p>Could be used together with variant 2a (compatible)</p>	<p>Using a Value Added Service does not guarantee interoperability.</p> <p>Value added service for installing a CTL requires TLS: distribution of new Root CAs must start before it is used by the charging infrastructure (e.g. 3 months ahead)[⊞].</p> <p>Impact on EV side:</p> <ul style="list-style-type: none"> ● Memory: storing + installing a new list ● Logic for verifying, unpacking and installing a new CTL (see also next paragraph on feasibility of variants) <p>Impact on Charging Station side: CTL forward logic</p> <p>Mechanism to trust initial CTL is needed (e.g. TLM Root CA)</p>
2a	CTL in the vehicle	<p>No impact on ISO 15118 specification ("addition / extension")</p> <p>Signature on CTL provides certainty that the CTL has not been tampered with.</p> <p>Could be used together with variant 1 (compatible)</p>	<p>Impact on EV side:</p> <ul style="list-style-type: none"> ● Memory (storing + installing a new list) ● Logic for verifying, unpacking and installing a new CTL (see also next paragraph on feasibility of variants) <p>Mechanism to trust initial CTL is needed (e.g. TLM Root CA)</p>
2b	CTL extracted by OEM	<p>No impact on ISO 15118 specification ("addition / extension")</p> <p>Since the signature is verified by the OEM and the individual certificates are sent to the EV, the security depends on the OEM</p>	<p>Impact on EV side: memory for all certificates</p> <p>Cannot be used together with 1 or 2a (incompatible)</p>

⊞: To clarify this: it must be distributed earlier to prevent a chicken & egg problem: If an EV cannot setup the required TLS connection to a Charging Station, because it does not have the correct V2G Root CA installed, it will be unable to use the value added service to install the CTL containing this V2G Root CA.

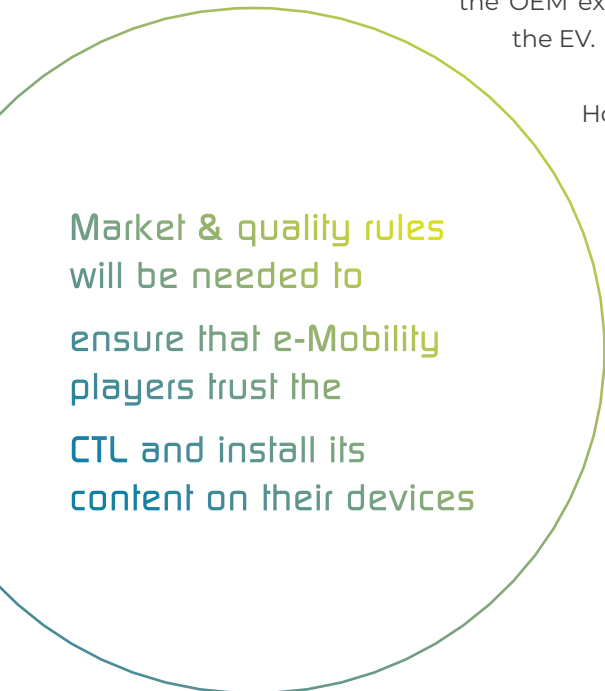
Feasibility of the variants

As already mentioned previously, assuming that the CTL is used with signature verification, for both the infrastructure route, as well as the variant 2a, where the CTL is sent to the EV in its entirety, the EV must support verifying and unpacking the CTL. This would need to be newly introduced in EVs and this might not be practically feasible, especially for current implementations. It is thus unsure if OEMs will support this CTL support feature in future and the **variants 1 and 2a** therefore seem less realistic.

Furthermore, currently all vehicles already have a telematics connection, it is not expected that OEMs will abandon this route, since OEMs also use this for other purposes. This makes the infrastructure route even less likely. Besides this it is expected that OEMs have already taken into account that V2G Root CAs need to be updated in the future based on the validity requirements (V2G2-878) from [ISO 15118-2], the functionality for variant 2b is expected to be already more or less available. Therefore, the most likely and feasible variant seems to be the variant 2b, where the OEM extracts the CTL and sends the certificates to the EV.

However, market rules will be needed to ensure that e-Mobility players do trust the CTL and install its content to their devices. Depending on the variant for distributing the CTL, it can be more or less complex to test and certify devices for following such rules.

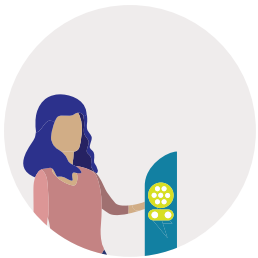
Please refer to part 1 for more information on this topic.



Market & quality rules
will be needed to
ensure that e-Mobility
players trust the
CTL and install its
content on their devices

15.1.3. Using a CTL for MO Root CA certificates in a Charging Station

Until this point, the CTL mechanism was primarily considered in the light of the interoperability by distributing the V2G Root CAs to EVs using a CTL, in order to provide interoperability similar to cross recognition. Besides the use of V2G Root CAs in the EV, the authorization of an EV at a Charging Station, requires the use of Contract Certificates. In the ISO 15118-2 and ISO 15118-20 (draft) standard, V2G Root CA certificates and MO Root CA certificates are used in Charging Stations for verifying these contract certificates from an EV. These are not necessarily derived from a V2G Root CA, these can also be derived from an MO Root CA certificate. If the Charging Station wants to verify the Contract Certificate of an EV at the Charging Station, the MO root CA certificates of EMSPs that do not choose to have their contract certificates derived from a V2G Root CA that can be expected in that region must be installed.



For distributing MO root CA certificates, the CTL mechanism could also be used. Currently, installing V2G Root CA certificates and MO Root CA certificates can already be done with the existing OCPP 2.0.1 version (or with OCPP 1.6 with the OCPP 1.6 – ISO 15118 Application Note implementation). However, if the CTL mechanism would also be applied here, similar to the installation of the CTL in the EV, the CTL can also be distributed for installation / updating in the Charging Station in multiple ways:

1. **CTL extracted by CSO:** CSO unpacks CTL and sends individual certificates to Charging Station
2. **CTL in the Charging Station:** CSO sends the CTL to the Charging Station. The station unpacks the CTL and installs the certificates.

The following table shows the advantages and disadvantages of these possible variants:

No	Variant	Advantages	Disadvantages
1	CTL for MO Root CAs extracted by CSO	Multiple smaller portions of data to Charging Station Already supported in OCPP.	The Charging Station cannot verify the signature on the CTL to be certain that the CTL has not been tampered with. Since the Charging Station and CSO have a trust relation, this signature verification seems irrelevant. A bit more overhead sending the certificates to the Charging Station
2	CTL for MO Root CAs sent to the Charging Station	Signature on CTL provides certainty that the CTL has not been tampered with to Charging Station.	Impact on Charging Station side: memory (storing + installing a new list) + logic In case of many V2G Root CAs: large CTL file (-> work with delta's) Only supported in OCPP when using customization option

Market rules will be needed to ensure that e-Mobility players do trust the CTL and install its content to their devices. Depending on the variant for distributing the CTL, it can be more or less complex to test and certify devices for following such rules.

Please refer to part 1 for more information on market rules.

15.2. Impact of the CTL on existing implementations

In this paragraph, the impact on existing implementations is explained. For each of the protocols / standards, the impact is discussed for the different variants of distributing the CTL. The main focus will be on using the CTL for distributing V2G Root CAs.

15.2.1. Certificate Trust List format

When speaking about a Certificate Trust List, as explained in 15.1.1, we only speak about a concept. As opposed to the cross certification mechanism that is technically clearly defined, a Certificate Trust List requires an additional step of determining the CTL format and how to exchange the CTL. Multiple variants for the CTL distribution mechanism will be discussed in this chapter, this section discusses the CTL format. As mentioned in the introduction of this part, the PKI interoperability mechanisms have been implemented as part of a field test. The format that was used for this test is included in ASN.1 format in Appendix A: CTL ASN.1 format. The most important aspects of this trust list are the following:

- It contains a signature of the Trust List Manager
- It contains a distinction between deltas (adding / deleting) and a full Trust List
- It contains the list of (V2G) Root CA certificates

In our demonstration we used a self-signed TLM certificate. The Trust List Manager must be a trusted party, of which the certificate can be validated (at least initially, the TLM can be update as part of the TLM mechanism by signing a new certificate with the private key belonging to its old certificate).

15.2.2. Impact of the CTL on ISO 15118 implementations

Impact on EV implementations when managing the CTL via the infrastructure

When distributing the CTL via the infrastructure by sending it via the Charging Station to an EV, this would impact the ISO 15118 specification (both the -2 and the -20). Currently the specification does not have messages for this. However, the specification does offer the functionality of “value added services”. For the field test, we used this mechanism. A value added service was defined, that worked as follows:

When the EV and Charging Station setup an ISO 15118 communication session, at the beginning of the session the Charging Station indicates which services it offers to the EV using the ServiceDiscoveryReq / -Res messages. In our case, we defined a service with the name “CTLInstallation”, that provides a URL to the EV where it can download the CTL from the Charging Station. The implementation of the service on the EV side was responsible for downloading the CTL from the Charging Station with that URL and installing the V2G Root CA certificates from the CTL in its trust store. The value added service as used during our field test, is included (as an example) in Appendix B: CTL Value Added Service.



An alternative could have been to send the entire CTL to the EV directly via ServiceDetailsRes instead of only sending a URL. However, we expected this not to be future proof and could end communication if the EV is not prepared for a large data block.

In summary, the impact on existing implementations would be that when distributing the CTL via the infrastructure, either additional messages are needed in the ISO 15118-2 or ISO 15118-20 or the existing messages for value added services

as defined in the specifications would need to be used. To provide interoperability between implementations using a value added service, this value added service would need to be clearly specified. This could be done by creating a separate “extension” to the specification clearly explaining how to use / fill the value added service messages.

Currently ISO 15118 does not have predefined messages for distributing a CTL

Whether additional messages are added to the ISO 15118 specification or a value added service is used, in both cases this would mean that it would require additional work for existing implementations on the EV and Charging Station side, either for adding new messages or implementing the value added service.

Impact on the EV implementation when managing the CTL via telematics directly to the vehicle

When not using the infrastructure route, the ISO 15118 communication between EV and Charging Station is not impacted. The CTL mechanism can be added as a separate mechanism to install V2G Root CA certificates in the EV. This does not impact the ISO 15118 implementation and will thus not require any changes to existing implementations.

Impact on the EV implementation when managing the CTL via telematics extracted by OEM

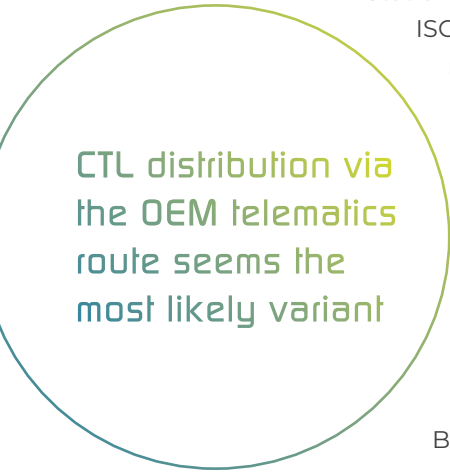
Similar to the variant where the CTL is sent directly to the EV, this variant does not impact the ISO 15118 specification and can be added as a separate mechanism.

15.2.3. Impact of the CTL on OCPP 2.0.1 implementations

Impact on the CSMS / CS when managing the CTL via the infrastructure

When distributing the CTL via the infrastructure by sending it from via the Charging Station to an EV, the CTL first has to be sent to the Charging Station by the CSMS. The OCPP 2.0.1 protocol is aligned with the ISO 15118-2 specification, but since a Certificate Trust List is not part of ISO 15118-2, this is not by default supported in the existing OCPP messages. The OCPP 2.0.1 extension mechanisms, such as DataTransfer and CustomData extensions, can be used to add this functionality.

In the field test, sending the CTL from the CSMS to the Charging Station was done by using the DataTransfer mechanism. The messageId used in the DataTransfer was "InstallTrustListCertificates", the vendorId "com.trialog.iso15118.ctl". The data field contained the entire CTL, Base64 encoded.



CTL distribution via the OEM telematics route seems the most likely variant

Impact on the CSMS / CS when managing the CTL via telematics directly to the vehicle

When not using the infrastructure route, the OCPP communication is not impacted.

Impact on the CSMS / CS when managing the CTL via telematics extracted by OEM

When not using the infrastructure route, the OCPP communication is not impacted.

15.2.4. Impact of the CTL on certificate pool functionality

The CTL mechanism does not add or change functionality that is done by a central hub or a certificate pool. In the VDE Anwendungsregel [VDE-AR] the concept of a directory service was introduced, to deal with having more than 1 contract (or OEM) certificate pool. When having multiple PKIs this should map PCID or EMAID to a reference to the correct certificate pool. This should be a certificate pool of any of the PKIs in the ecosystem.

In theory central platforms could play a role since they can already play a role in the distribution of Root CA certificates ("Root Certificate Pool" as described in reference [VDE-AR]). However, in other markets where a Certificate Trust List is used, the distribution of the list is often done by the Trust List Manager.

15.2.5. Impact of the CTL on the VDE Anwendungsregel

The current VDE Anwendungsregel is considered as a necessary extension for implementing the ISO 15118-2 standard. In the case that the Certificate Trust List mechanism would be introduced in addition to the ISO 15118 standard, the way this works, must be explained somewhere. This could be done as a part of the VDE Anwendungsregel, but because of the world / market wide impact of the CTL mechanism, this seems more appropriate for an ISO 15118 Interoperability Guide. Currently an Interoperability Guide for ISO 15118 (both ISO15118-2 as well as ISO15118-20) is under development within CharIN, so in case the CTL mechanism would be introduced, this seems a more logical place to describe this.

15.3. Impact of the CTL on hardware requirements

The impact on the hardware requirements when applying a Certificate Trust List differs depending on the variant that is chosen.

When distributing the CTL via the infrastructure, this impacts both the EV side as well as the Charging Station side. On the EV side memory is needed for storing a CTL and installing a new CTL, and additional logic (requiring a limited amount of additional computational power). On the Charging Station side memory and logic are needed for forwarding the CTL to an EV.

When distributing the CTL directly to the vehicle, this variant does not impact the Charging Station. When the OEM unpacks the CTL and forwards the individual certificates, the EV only needs enough memory for installing all V2G Root CA certificates.

In all cases, the amount of memory that is needed for storing the certificates from a CTL is depending on the number of PKIs: for n PKIs, the amount of storage needed is:

$$n * 800 \text{ bytes}$$

Since the number of certificates for a V2G Root CAs must be between 1 and 10 (based on the validity requirements (V2G2-878) from [ISO 15118-2]), the maximum would then need to be multiplied by 10. So, for example, for 5 PKI's this would be $5*800*10 = 40.000 \text{ bytes} \approx 39 \text{ kB}$.

This amount of memory would have to be available at the EV and Charging Station for storing, depending on the variant it could be more (e.g. an EV would need the double amount if installation is done by sending the entire CTL for updating / unpacking at the EV side).

15.4. Summary

In summary, using a Certificate Trust List is an option for PKI interoperability that could be applied in an ISO 15118 EV ecosystem. Several variants can be used for distributing a CTL. All of these options require the EV to install the CTL or certificates from this CTL. The distribution of the CTL could be arranged via the charging infrastructure or via the OEM's telematics. When sending the CTL via the OEM, it does not impact the ISO 15118 specification, when sending it via the infrastructure, it requires the specification of distributing the CTL. This can be done either as a new part of the ISO 15118 specification or as a standardized value added service (not requiring a change in the existing ISO 15118-2 specification).

The most likely implementation of a Certificate Trust List Mechanism is the OEM retrieving and unpacking the CTL and forwarding the individual V2G Root CAs to the EV using Telematics. For this solution to be scalable however, the available space in the EV Trust Store must be addressed as a serious point of attention.

15.5. Recommendations

Based on our work described in this chapter, we believe that if a Certificate Trust List would be chosen as an interoperability mechanism for ISO 15118-2, **further industry discussions** and market regulation regarding the space in the EV Trust Store are needed to be engaged in. Until this is enlarged, applying a Certificate Trust List for V2G Root CA certificates for PKI interoperability is not feasible.

In a similar way an industry discussion could be started about the use of a CTL for distributing MO Root CA certificates to Charging Stations for verification of contract certificates. In case that the outcome of this discussion would be that memory limitation of Charging Stations would be an issue, EMSPs could consider deriving their contract certificates from a V2G Root CA.



Further industry
discussions and market
regulation regarding
the space in the EV
Trust Store are needed

16. INTEROPERABILITY DISCUSSION

16.1. PKI Interoperability using cross certificates

Achieving PKI interoperability by using cross certification is a common method for PKI interoperability. When using this approach, interoperability can, in addition to the adding multiple V2G Root CAs in the EV, also be handled “outside of the EV”, by using cross certificates at the Charging Station.

The approach is rather scalable, the main limitations are in the memory of Charging Station, when in case of many PKI’s, a lot of cross certificates are used. The scalability can be increased by applying a “bridge CA” mechanism. However, this would require 2 additional layers in the PKI hierarchy. Furthermore, this would require one neutral, regulated party that has to fulfil the role of bridge CA, which leads to similar issues for the options where there is only one V2G Root CA.

Cross certification can already be used with the ISO 15118-2 specification, when one existing certificate layer is used for cross certificates. The only issue that could occur is during establishing a TLS connection by the EV, which resulted in not all implementations on the EV



side supporting cross certification out of the box. Furthermore, a larger amount of PKIs, and thus a larger number of cross certificates, causes a larger complexity / maintenance effort.

With the ISO 15118-20 version, based on the current draft, it is expected that cross certification is made possible as part of the standard. As with the ISO 15118-2 specification, this new version is also expected to support the TLS handshake for cross certification (using a slightly different technical mechanism). However, due to the issues we encountered, this still makes the TLS handshake a point of attention for ISO 15118 certification. Using cross certification also has a minor impact on OCPP and the VDE Anwendungsregel.


Therefore we think this is a possible useful solution for ISO 15118 PKI interoperability in addition to cross recognition.

16.2. PKI Interoperability using a Certificate Trust List

Achieving PKI interoperability by using a Certificate Trust List is another method for PKI interoperability that is also used in other markets, such as Intelligent Transport Systems.

The approach is scalable, the main limitations are in the memory of the EV, when in case of many PKI's, many V2G Root CAs are used. The mechanism is very similar to cross recognition: the V2G Root CAs from the CTL are to be installed in the EV and the Charging Station.

A CTL can be used with the ISO 15118-2 and ISO 15118-20 specification. Depending on the variant that is used for distributing the CTL, an addition to the ISO 15118 specification or standardized value added service could be necessary.



PKI interoperability
by using a
Certificate Trust
List is also used
in other markets

Alternatively a separate CTL distribution mechanism via the OEM could be introduced. When the CTL is distributed via the infrastructure route, using a CTL also has a minor impact on OCPP, as described in 15.2. Furthermore, for the infrastructure route an interoperability guide would be needed to describe the standardized value added service.

Based on our findings we think a Certificate Trust List is also a possible useful solution for ISO 15118 PKI interoperability as a governed and maintainable form of cross recognition, provided that the OEMs will accommodate sufficient support for multiple V2G Root CAs in the EVs Trust Store.

16.3. Other PKI interoperability findings / further research

One of the topics that was encountered during the demonstration project is that the API interface to the various involved Contact Certificate Pools (CCPs) was different. One noticeable difference was that the one implementation required an `exiRequest` (containing the raw `CertificateInstallationReq` message from the EV) to be sent to the CCP in order to receive the `exiResponse`. Another implementation required only the `PCID / EMAID` (and some additional required fields such as `SessionID`, `schema version` and `list of Root Certificate IDs`). The first implementation does not require a CSO to decode the message from the EV, although this could be necessary if a directory service is used to find the right CCP based on `PCID / EMAID` as suggested in the VDE application guide [VDE-AR]. To improve interoperability between PKIs (or even within PKIs if multiple CCPs are available within one PKI), we suggest that the CharIN PKI Interoperability Taskforce standardizes the information that is included in the interface to a CCP (and perhaps even the actual interfaces to the certificate pools and directory services).



Another recent suggestion that will be explored in the future is to apply cross certification between an “external” EMSP (“MO Root CA”) with a V2G Root CA PKI and add that cross certificate to the contract certificate chain. This could make it possible to omit the CPS service/signature.

In this document we have not explored replacing Root CA certificates or revocation of certificates. The mechanisms described, cross certification and a Certificate Trust List, are interoperability mechanisms not specific to ISO 15118 and are also applied in other industries / ecosystems. The general revocation mechanisms OCSP and CRL can be applied, but the impact on an ISO 15118 ecosystem of a revoked (or replaced) certificate requires further exploration.

In this report we have touched upon using MO Root CA certificates (suggesting that a CTL could be used for this). Currently there are already hundreds of EMSPs in the European e-mobility market. If all these EMSPs decide to use their own MO Root CA certificate, this could have quite some impact on the Charging Station memory, since Charging Stations have to store MO Root CA certificates for contract certificate validation. This particular aspect requires further exploration.

Finally, all different PKI interoperability options will have to be able to deal with the situation that a CA certificate or a cross certificate is compromised. The latter can be handled by the right use of CRLs or OSCP responders. When a Root CA itself is compromised, there is no other choice then rebuilding the entire PKI. This topic is not further explored in this document.

16.4. PKI Pool Interoperability

For the installation of contract certificates in an EV, the CSO of the Charging Station that the EV is connected to, must fetch the contract certificate from the right Contract Certificate Pool (CCP). Instead of connecting either all EMSPs or all CSOs to all Contract Certificate pools, we are currently exploring options to simplify this by introducing interoperability on the level of PKI Pools. One of the options that is explored, is connecting PKI Pools to each other. This can support CSOs to fetch any (signed) contract certificate bundle from any pool by connecting to just one Contract Certificate Pool and let the various Contract Certificate Pools connect to each other to find the one that is actually storing the bundle.

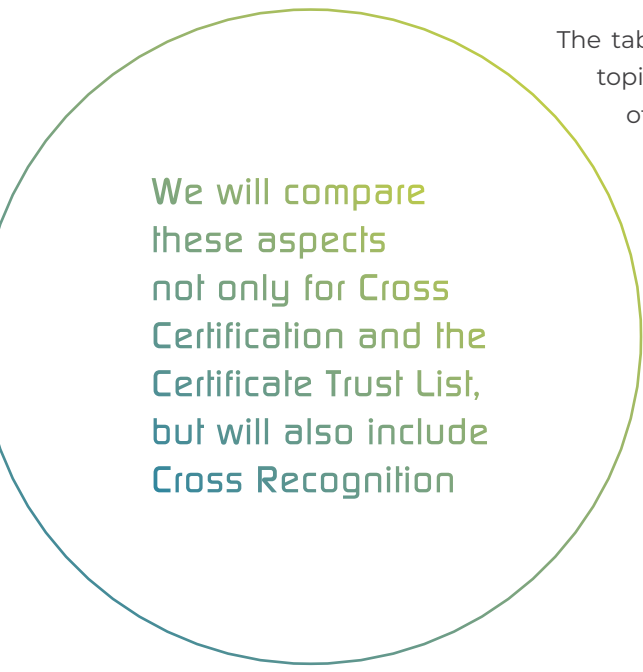
Besides exploring options for fetching contract certificate pools, we are also exploring the preparation of contract certificates at a Contract Certificate pool in an interoperable way. The CPS certificate that is used to sign a Contract Certificate bundle must be verified by an EV. To reach interoperability for installing a signed contract certificate bundle from any Contract Certificate Pool, several different options are available on PKI Pool level. One of the ways that is explored to reach interoperability for this, is that every CCP where a contract can be requested, would be able to sign contract data (either directly or indirectly) using the CPS certificate from any available V2G Root CAs.

Options for interoperability for Contract Certificate Pools (and for OEM Provisioning Certificate Pools), as described in this paragraph, are currently being explored and will be demonstrated in the near future.

16.5. Topics besides providing interoperability

Now that the technical interoperability of Cross Certification and a Certificate Trust List are described in chapter 14 and 15, we will shortly look at a number of other aspects to consider. We will compare these aspects not only for Cross Certification and the Certificate Trust List, but will also include Cross Recognition. The aspects considered are:

- Maintainability
- Technical feasibility of the solution
- Scalability
- Where is interoperability handled



We will compare these aspects not only for Cross Certification and the Certificate Trust List, but will also include Cross Recognition

The table provides an overview of a number of topics that is addressed by the different ways of providing interoperability.

All options require similar amounts of quality rules and market rules as described in Part 1.

Issues addressed	Maintainability	Technical feasibility	Scalability	Where is interoperability handled?
Cross recognition	<p>"Root Certificate Pool" useful in case of many PKIs.</p> <p>Revocation = removing a V2G Root certificate directly from trust store (CRL cannot be used)</p>	<p>Confirmed</p> <p>Possible with ISO 15118-2 / -20</p>	<p>If n PKIs -> n V2G Root CAs installed in EV and Charging Station</p> <p>On boarding effort is once per additional root CA</p>	<p>Interoperability handled "inside" the EV (for installing CC and setting up TLS to Charging Station) and EVSE (for authorizing the CC)</p>
Cross Certification	<p>Perhaps a "Cross Certificate Pool" needed in case of many PKIs?</p> <p>Revocation: add cross certified V2G Root CA to the CRL of the cross certifying V2G Root CA. This is standard way of handling CRLs.</p>	<p>Yes, as shown in webinar / demo July 2020</p> <p>Possible with ISO 15118-2 with PKI hierarchy layer limitation.</p> <p>Possible with ISO 15118-20 (based on current draft)</p>	<p>If n PKIs -> max $n(n-1)/2$ cross certificates in Charging Station and CCP, only 1 in EV during certificate installation and setting up TLS connection</p> <p>On boarding effort per additional cross certification relation</p>	<p>Interoperability is handled "outside the EV" (at the EVSE / PnC ecosystem)</p> <p>Cross certification entails a bilateral trust relation between independent PKIs and therefore requires the governance rules to take this "per actor"/bilateral character into account</p>
Certificate Trust List	<p>CTL manager maintains list, maintenance is part of CTL mechanism.</p> <p>Revocation = removing a V2G Root certificate from CTL (CRL cannot be used)</p>	<p>Yes, as shown in webinar / demo June 2021</p> <p>For infrastructure route: possible with use of a Value Added Service (VAS) or other extension to ISO 15118.</p> <p>For telematics route: no impact on ISO 15118</p>	<p>If n PKIs -> n V2G Root CAs from CTL installed in EV and Charging Station</p> <p>Identical to cross recognition</p> <p>On boarding effort is only once per additional root CA</p>	<p>Trust List Manager</p> <p>This has an association with "central governance", due to the role of the central Trust List Manager that has to trust a PKI in order to add it to the CTL.</p>

16.6. Co-existing interoperability options

Currently the EV market is rapidly growing and it is not known yet how many PKI's will coexist and which interoperability option (or options) will be chosen. Therefore it is interesting to see whether and how it would be possible to use multiple options at the same time. The overview below shows that all combinations are possible. The way how this can be handled / the points of attention are given in the following table:

** Multiple verification paths are no problem with most TLS libraries (implementers should verify).*

*** Whenever cross recognition and a CTL are combined as mechanisms, it is useful to keep track of which certificates were added/removed because of the CTL updates and which were separately installed. It is up to the implementer how to handle the case when a certificate is removed from the CTL but was previously added because of cross recognition.*

No	Variant combination	Handling combination on EV side	Handling combination on Charging Station side
1	Cross-Recognition + Cross-Certification 	Cross certificates can be used in combination with cross recognition. This could lead to multiple paths for verifying certificates of the Charging Station*	When cross recognition and cross certification are used in combination, Charging Stations will have a trust store consisting of V2G Root CAs and cross-certificates (and MO Root CAs) This combination could lead to multiple paths for verifying Contract Certificates*
2	Cross-Recognition + Certificate Trust List 	When using this combination, the EV must have a trust store for the V2G Root CAs that is partially managed by the CTL mechanism**	When using this combination, the Charging Station must have a trust store for the V2G Root CAs and MO Root CAs that is partially managed (adding / removing) by the CTL mechanism (for V2G Root CAs only)**
3	Cross-Certification + Certificate Trust List 	When using this combination, the EV has a trust store for the V2G Root CAs that is managed by the CTL mechanism Additionally, cross certificates can be used, which can lead to multiple paths for verifying certificates of Charging Station / installation messages*	When using this combination, Charging Stations will have a trust store consisting of V2G Root CAs and cross-certificates (and MO Root CAs). The V2G Root CAs in this trust store are managed by the CTL mechanism. MO Root CA's can be managed by the CSO separately (either completely by the CSO or using a CTL for MO Root CAs as described in 15.1.3)
4	Cross-Recognition + Cross-Certification + Certificate Trust List 	When using this combination, the EV has a trust store for the V2G Root CAs that is (partially) managed by the CTL mechanism** Additionally, cross certificates can be used, which can lead to multiple paths for verifying certificates of Charging Station / installation messages*	When using all mechanisms, Charging Stations will have a trust store consisting of V2G Root CAs and cross-certificates (and MO Root CAs). The V2G Root CAs are managed by the CTL mechanism** MO Root CA's can be managed by the CSO separately (either completely by the CSO or using a CTL for MO Root CAs as described in 15.1.3)

16.7. Conclusion

For the technical interoperability between PKIs when using ISO 15118, we have discussed different variants. All these variants can provide interoperability and can all be used in parallel, if that would be necessary based on market developments. The variants do have some advantages and disadvantages when it comes to maintenance or technical feasibility, some variants have more impact than others.

Cross Certification is a feasible interoperability mechanism, in a market where:

- The number of operational PKIs is small, e.g. three (currently only one, with several more in the making)
- The available space in the EV's trust store is limited
- CSOs can guarantee interoperability using cross certificates whilst selecting the PKI of their choice.

A Certificate Trust List is a good and scalable interoperability solution in a market where:

- More PKIs (e.g. more than three) are operational
- The EV's trust store can hold the larger numbers of V2G Root CAs that are on the CTL
- OEMs can guarantee interoperability and an open market by facilitating all V2G Root CAs on the Certificate Trust List, enabling CSOs and EMPS freedom to select the PKI of their choice.



16.8. Recommendations

The following points require further investigation:

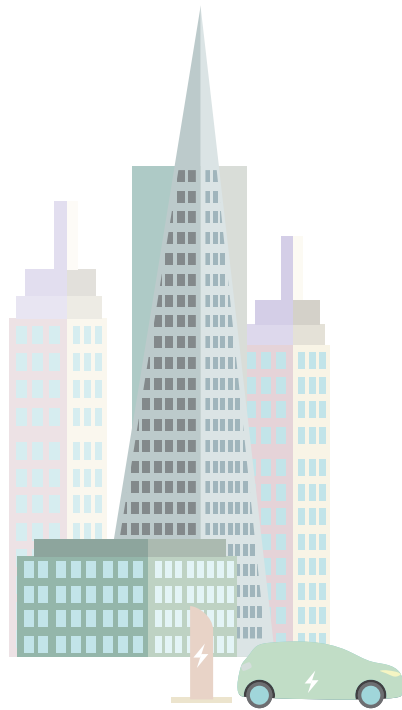
In general it will take more time to review the impact of the ISO 15118-20 draft version that recently has become available. Subsequently we will explore the possible interoperability demonstrations using the new opportunities that the ISO 15118-20 specification offers.

For Cross Certification

- The requirement to dedicate one layer for a cross certificate shall be further explored.
- As mentioned in the chapter about cross certification, not all implementations were able to setup a TLS connection, although this should be possible based on the ISO 15118-2 requirements. This should be further investigated how this currently works with EVs on the market. This could mean that, of cross certification would be chosen as an interoperability mechanism, this would require minor modifications to EVs on the market to support this if this ISO 15118-2 requirement is currently not implemented (correctly). The CharIN PKI Interoperability Task Group (for explaining) and the ISO 15118 Certification Program (for verification) would be a logical choice.

For Trust List

- Statements from OEMs about the number of available “slots” in the EV trust store for installing V2G Root CAs are mixed / not always consistent. This topic should be further investigated to get a more accurate view on the limitations / possibilities. Without increasing the capacity in the EV Trust Store, the CTL is not a realistic interoperability mechanism, so OEMs need to take into consideration the storage capacity needed in the EVs trust store in order to manage the installation of multiple V2G Root CA certificates.
- Work needs to be done to identify who can fulfil the role of the Trust List Manager.
- The CTL approach would need to be specified as an addition to the ISO 15118, perhaps in the CharIN PKI Taskforce Interoperability Document.







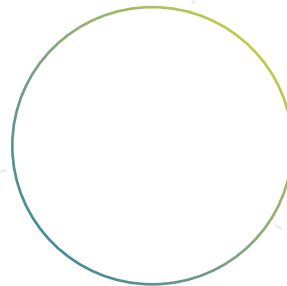
PART 3

Quality Rules

For independent PKIs
to trust each other



For parties to trust
a PKI, quality
rules need to
be agreed on





17. INTRODUCTION

The most important aspect of a Public Key Infrastructure is “trust”. When using digital certificates for securing communication, certificates that are used by different roles and components in the EV ecosystem must be trusted by other market participants. Besides a technical trust aspect, this must also be a trust relation on a business level.

For market parties to trust a PKI and for independent PKIs to trust each other (and therefor cross certify or apply a Trust List mechanism) there needs to be agreement on the individual PKI’s Quality rules.

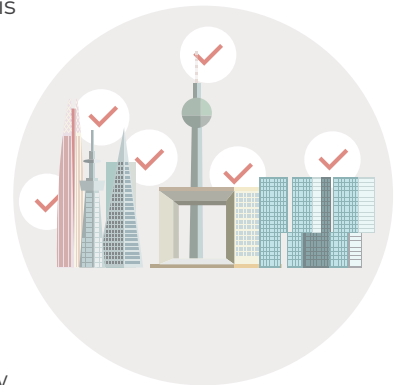
These Quality rules are written down in detail in a PKI’s Certificate Policy, Certificate Practice Statement, audit requirements and other additional documentation.

18. PKI QUALITY RULES

18.1. Quality aspects of a PKI

The operator of a PKI must ensure the quality of the PKI. In order to do this, it has to provide insight in its own internal procedures and professionalism, but it must also ensure that each participant in the PKI can be trusted. In order to do this, the following aspects are important:

- A Certificate Policy (CP) which states what are the different entities / participants of the PKI, the details on the data formats and how the PKI is operated (processes). This describes, among others, what rules apply for participants such as Sub CAs in the PKI (entities that distribute certificates). Examples of these rules are how to fill the technical fields in certificates and who is allowed to revoke certificates. By providing this information in a transparent way, the contents of a Certificate Policy give insight in the quality of a PKI.
- A Certificate Practice Statement that explains how the operator of the PKI executes its internal processes (such as issuance, publication, archiving, revocation, renewal). The details of these processes are sometimes not given, to prevent providing external attackers with too much information.



- Underlying audit requirements. As part of the CP, a PKI operator will state the prerequisites for the different types of participants of the PKI. An audit is usually performed to determine whether the requirements in the CP are met. In addition, these audit requirements often include providing insight in the technical solution, but also in security related procedures of a participant. Depending on the role of the participant in the PKI, example requirements could be ISO 27001 certification, insight in the participant IT architecture, applying software and hardware security, insight in the roles and responsibilities in the participant organization.
- In case of the interoperability option of a Certificate Trust List (CTL), the Trust List Manager (TLM) will have to comply to quality rules that guarantee the trustworthiness of the CTL and the Root CA addition process .



- For the interoperability option of cross certification, when 2 PKIs are cross certified, it basically means that one PKI is responsible for the quality and trustworthiness of a certificate that it has never issued itself, but that was issued by the other PKI. Consequentially, it can be expected that Root CAs have high demands / requirements before cross certifying with other PKIs.

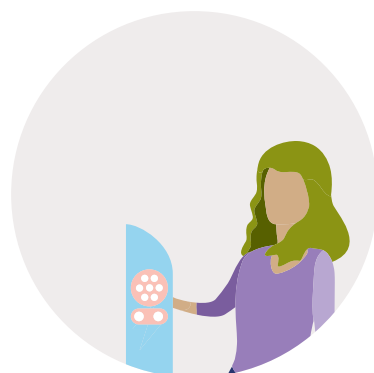
18.2. Requirements for applying quality rules

In order to achieve the goal of having open market access, the following requirements for applying quality rules are applicable:

- The quality criteria that are applied must be transparent to all market participants. It must be clear in advance what is expected of a new PKI. This allows new PKIs to prepare and prevent unexpected requirements that might take a lot of work to solve when applying

for participating in a PKI ecosystem (using cross recognition, cross certification or a Certificate Trust List).

- The quality criteria that are applied must be verified by neutral auditors. Neutral in this case means that it must not be the PKI operator itself, nor a market participant nor a company that has a market participant as a shareholder. The costs for such an audit should be reasonable and transparent. Furthermore, reasonable response times should be guaranteed to participants and monitored independently.
- The (level of detail of the) information that is to be provided by participants to the neutral auditor must be relevant only for verifying quality and must not include any other, possibly (competition) sensitive information which could be seen as a barrier for participating in such an audit. These audits should be subject to a strict confidentiality agreement.
- When multiple PKIs are used within the market, these have to agree on a minimum quality level for all PKIs. Verifying whether this minimum level is achieved must be either by agreeing on a minimal CP and adherence to this CP by a PKI operator must be independently verified by a neutral entity.
- In case of a dispute, a neutral entity must be available for arbitration. In case of a conflict, that entity can resolve the conflict in a neutral way, to prevent quality rules being used a barrier for specific parties / competitors. An example of a dispute could be when fundamental system choices are imposed to a participant, leading to high costs and delays in participating in the market.



18.3. Work in progress at CharIN

CharIN has developed a template for a Certificate Policy (CP) [ref: CharIN-CP] which contains requirements with a sufficient level of security in the context of ISO 15118. PKI service providers must meet or exceed these requirements so that the PKI can be regarded as “approved by CharIN”. However, this CP is not specific enough to address and describe the points mentioned in 18.1 or 18.2.

The quality criteria that are applied must be verified by neutral auditors

CharIN has also launched a project called “Plug and Charge Europe”, that aims to set up a PKI with CharIN as operator and provider of required services. Within this project, CharIN will draft among others a detailed CP, CPS and audit requirements. Whilst it is still early days, this CharIN documentation could serve as a template for PKI Quality rules.

18.4. Recommendations

We recommend that the topic of concrete and detailed PKI Quality Rules is addressed at a central European Level (e.g. a European Security Regulatory body, the AFID, the STF). We expect that additionally, in some European countries, this topic will also be addressed at a National Legislative level.

PKI Quality Rules addressed at a central European Level



REFERENCES

TERMINOLOGY

This section contains the terminology that is used throughout this document.

Terminology	Description
CC	Contract Certificate
(C)CCP	(Central) Contract Certificate Pool
Certificate	A digital certificate authenticates a public key or entity. See also Public-Key Infrastructure.
Charging Station	The Charging Station is the physical system where an EV can be charged. A Charging Station has one or more EVSEs.
CharIN	Industry association dedicated to promote interoperability based on the Combined Charging System (CCS) as the global standard for charging vehicles of all kinds, supporting ISO 15118 as the standard between EV and Charging Station.
CP	Certificate Policy
COPCP	Central OEM EV Provisioning Certificate Pool
CPS	Certificate Provisioning Service
CSMS	Charging Station Management System. The system that manages Charging Stations and has the information for authorizing Users for using its Charging Stations.
CSO	Charging Station Operator. Synonym for Charge Point Operator (CPO)
CTL	Certificate Trust List
EMAID	E-Mobility Account Identifier
EMSP	E-Mobility Service Provider. Synonym for Mobility Operator (MO).
EV	Electric Vehicle
EVSE	An EVSE is considered as an independently operated and managed part of the Charging Station that can deliver energy to one EV at a time.

High level communication	bi-directional digital communication using protocol and messages and physical and data link layers specified in ISO 15118 series [ISO15118-1]
Intermediate certificate	Certificate between the root certificate at the top of the certificate hierarchy and the leaf certificates.
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.
OCSP	Online Certificate Status Protocol
PCID	Provisioning Certificate ID. Unique identifier of the certificate that is installed in an EV during manufacturing.
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.
Trust store	Similar to a key store, but for certificates that identify other parties.
Use case	A use case is a structured way of describing the (inter) actions necessary to achieve a certain objective. In this document, a use case consists of an actor list, a scenario description, postconditions and a sequence diagram and is always followed by a list of numbered requirements.

REFERENCES

Reference	Description
[ISO15118-1]	ISO 15118-1 specifies terms and definitions, general requirements and use cases as the basis for the other parts of ISO 15118. It provides a general overview and a common understanding of aspects influencing the charge process, payment and load leveling. https://webstore.iec.ch/publication/9272
[ISO15118-2]	Road vehicles "Vehicle to grid communication interface" Part 2: Technical protocol description and Open Systems Interconnection (OSI) layer requirements, Document Identifier: 69/216/CDV. https://webstore.iec.ch/publication/9273
[ISO15118-20]	Draft Road vehicles — Vehicle to grid communication interface — Part 2: Network and application protocol requirements, ISO/PreFDIS1a 15118-20, 2021-10-08 This document can be accessed when you are a member of the ISO 15118 group
[OCPP2.0-PART1]	"OCPP 2.0.1: Part 1 - Architecture & Topology". http://www.openchargealliance.org/downloads/
[OCPP2.0-PART2]	"OCPP 2.0.1: Part 2 - Specification". http://www.openchargealliance.org/downloads/
[ElaadNL-PKI]	Exploring the PKI for ISO 15118 in the EV charging Ecosystem, ElaadNL, 2018 https://www.elaad.nl/uploads/files/Exploring_the_PKI_for_ISO_15118_in_the_EV_charging_ecoystem_V1.0s2.pdf
[VDE-AR]	VDE-AR-E 2802-100-1: 2019-12, VDE Anwendungsregel / application rule: Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118 This document can be purchased at the VDE: https://www.vde-verlag.de/standards/0800642/vde-ar-e-2802-100-1-anwendungsregel-2019-12.html

[CharIN-CP]	<p>Certificate Policy - CP for CharIN Taskforce PKI, 2020, CharIN</p> <p>https://www.charin.global/media/pages/news/charin-e-v-publishes-certificate-policy-guideline-for-an-iso-15118-v2g-pki/ce7e617a39-1615552641/charin_cp_for_iso_15118_v2g_pki.pdf</p>
[OCA-OCPP-ISO]	<p>Using ISO 15118 Plug & Charge with OCPP 1.6. https://www.openchargealliance.org/uploads/files/ocpp_1.6_ISO_15118_v10.pdf</p>
[CharIN-IOP]	<p>Charin PKI Interoperability document, Charin PKI TaskForce</p> <p>This document is under development within the Charin PKI Taskforce</p>
[STF-RECOMM]	<p>Sustainable Transport Forum, Recommendations for public authorities on: procuring, awarding concessions, licences and/or granting support for electric recharging infrastructure for passenger cars and vans</p>

OTHER PUBLICATIONS IN THIS SERIES

PUBLICATION

"Exploring the Public Key Infrastructure
for ISO 15118
in the EV charging Ecosystem"

ElaadNL, Arnhem,
The Netherlands,
November 2018

Download: https://www.elaad.nl/uploads/files/Exploring_the_PKI_for_ISO_15118_in_the_EV_charging_ecosystem_V1.0s2.pdf



This first exploration of the ISO 15118 standard explains Public Key Infrastructures (PKIs) in general, how a PKI design is used to secure the ISO 15118 standard and a first open design of a PKI for ISO 15118. It presents a multiple options for PKI designs that are possible, 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.





APPENDICES

APPENDIX A: CTL ASN.1 FORMAT

As described in 15.2.1 a Certificate Trust List is a concept, a technical specification / format of a trust list does not exist and has to be created for each CTL implementation. Below the technical ASN.1 format for the CTL that was used in our demonstration project is shown.

V2GCTL

```
-- Derived from EtsiTsl102941TrustLists { itu-t(0)
identified-organization(4) etsi(0) itsDomain(5)
wg5(5) ts(102941) trustLists(6) version2(2) }
--- Author : pierre.girard@thalesgoup.com
-- Version 0.3
--
-- Change log
-- 0.1: Initial version
-- 0.2: Correction of ToBeSignedTlmCtl, change
Certificate as Opaque
--      add signature data structure
-- 0.3: Moved generation time to the signed data
part
```

```
DEFINITIONS AUTOMATIC TAGS ::=
```

BEGIN

```
-- Certificate and Signature are defined as Opaque
to avoid to drag
-- too much dependencies
Certificate ::= Opaque
Signature   ::= Opaque
```

```

-- Time32, Opaque, HashAlgorithm and HashedId8
are defined in IEEE1609 (redefined here to avoid
IMPORTS)

-- This type gives the number of (TAI) seconds
since 00:00:00 UTC, 1 January, 2004
Uint32 ::= INTEGER (0..4294967295)
Time32 ::= Uint32

HashAlgorithm ::= ENUMERATED {
    sha256,
    ...,
    sha384
}

Opaque ::= OCTET STRING

--This data structure contains the truncated hash
of another data structure. The HashedId8 for a
given data
--structure is calculated by calculating the SHA-
256 hash of the encoded data structure and taking
the low-
--order eight bytes of the hash output. The
low-order eight bytes are the last eight bytes of
the 32-byte hash
HashedId8 ::= OCTET STRING (SIZE(8))

Version ::= INTEGER {v1(1)}

Url ::= IA5String

CtlCommand ::= CHOICE {
    add      CtlEntry,
    delete  CtlDelete,
    ...
}

```

```

CtlCommand ::= CHOICE {
  add      CtlEntry,
  delete  CtlDelete,
  ...
}

CtlEntry ::= CHOICE {
  rca      RootCaEntry,
  dc       DcEntry,
  tlm      TlmEntry,
  ...
}

CtlDelete ::= CHOICE {
  cert     HashedId8,
  dc       DcDelete,
  ...
}

DcDelete ::= Url

TlmEntry ::= SEQUENCE {
  selfSignedTLMCertificate Certificate,
  linkTLMCertificate      Certificate OPTIONAL,
  accessPoint
  Url
}

RootCaEntry ::= SEQUENCE {
  selfsignedRootCa Certificate,
  linkRootCaCertificate Certificate OPTIONAL
}

```

```

DcEntry ::= SEQUENCE {
    url      Url,
    cert     SEQUENCE OF HashedId8 -- the
RCA(s) certificate digests that publish via the
Distribution Centre
}

CtlFormat ::= SEQUENCE {
    version      Version,
    nextUpdate   Time32,
    isFullCtl    BOOLEAN,
    ctlSequence  INTEGER (0..255),

--used to check that no delta CTL has been missed
    ctlCommands SEQUENCE OF CtlCommand,
    ...
}

FullCtl ::= CtlFormat ( WITH COMPONENTS {
    ...,
    isFullCtl ( TRUE ),
    ctlCommands ( WITH COMPONENT((
        WITH COMPONENTS {
            ...,
            delete ABSENT
        })
    ))
})

DeltaCtl ::= CtlFormat (WITH COMPONENTS {..., is-
FullCtl(FALSE)})

ToBeSignedTlmCtl ::= CtlFormat (FullCtl | Del-
taCtl)

```

```
-- Simplified signed Tlm Ctl message below to avoid
imports

ToBeSignedData ::= SEQUENCE {
    generationTime Time32,
    payload          ToBeSignedTlmCtl
}

TlmCertificateTrustListMessage ::= SEQUENCE {
    hashId          HashAlgorithm,
    data            ToBeSignedData,
    signer          Certificate,
    signature       Signature
}

END
```

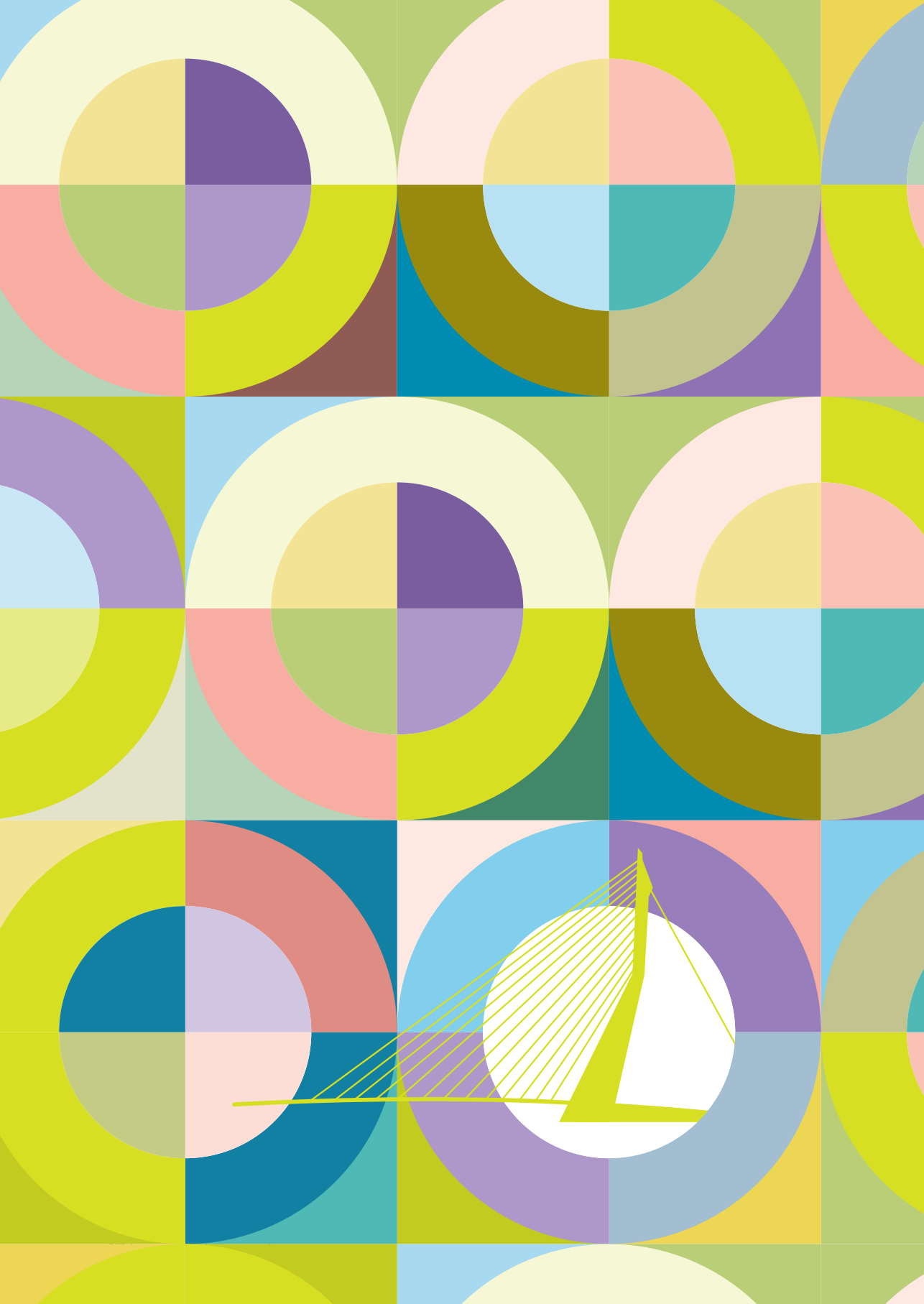
The above format is a standard. For many programming languages libraries are available to encode / decode data based on the **ASN.1 format**.

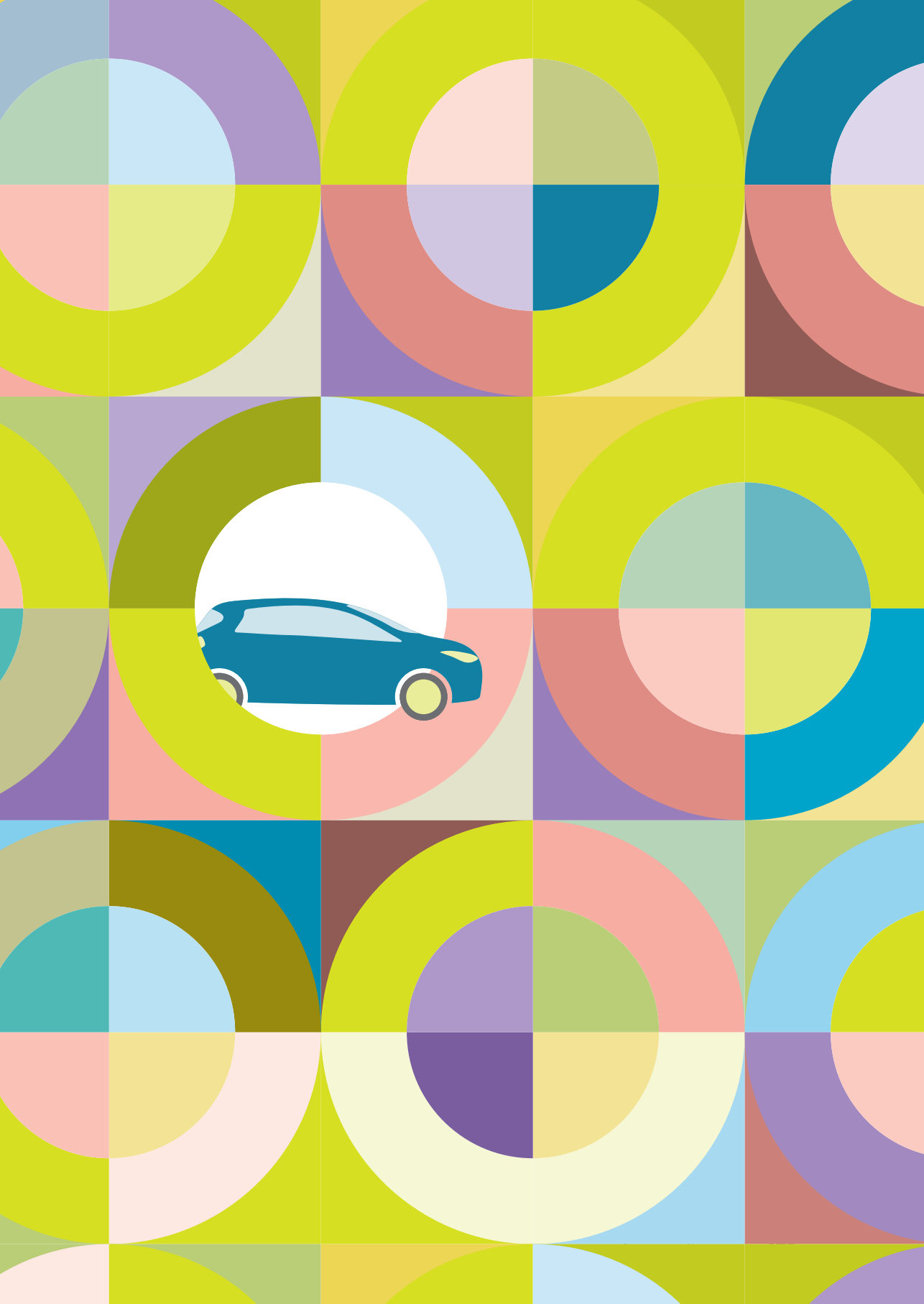
APPENDIX B: CTL VALUE ADDED SERVICE

When implementing a value added service in ISO 15118-2, a number of fields in the messages related to value added services have to be specified. Value added services that are offered by a Charging Station can be discovered by an EV using the ServiceDiscovery messages. The response to the EV must provide a list of offered services, in the table below the response to the EV as used in our project is presented.

After discovering the value added service, the service can be used, using the ServiceDetails message. This message allows parameters to be defined and exchanged from the Charging Station to the EV. In the table below the parameters used in our demonstration project are listed. The message that the EV receives does not contain the CTL itself, but the location where the CTL can be downloaded from the Charging Station.

System/Message	Field	Value
EV: ServiceDiscoveryReq	ServiceScope	<empty>
	ServiceCategory	<empty>
CS: ServiceDiscoveryRes	ResponseCode =>	OK
	PaymentOptionList =>	{Contract, ExternalPayment}
	ChargeService	(AC_single_phase_core, AC_three_phase_core)
	ServiceList => Service => ServiceID	60018
	ServiceList => Service => ServiceName	"CTLInstallation"
	ServiceList => Service => ServiceCategory	"OtherCustom"
	ServiceList => Service => ServiceScope	"Security"
	ServiceList => Service => FreeService	True
EV: ServiceDetailsReq	ServiceID	60018
CS: ServiceDetailsRes	ResponseCode = OK	
	ServiceID	60018
	ServiceParameterList => ParameterSetID	42
	ServiceParameterList => Parameter (string)	Name: "IP_address", value (e.g.): "fe80::4e1b:86ff:fe89:a0db"
	ServiceParameterList => Parameter (string)	Name: "Port", value (e.g.): "8080"
	ServiceParameterList => Parameter (string)	Name: "URL", value (e.g.): "/public/v2gctl/v2gctl.der"







CONTACT

ElaadNL


Westervoortsedijk 73

Gebouw KB, Industriepark Kleefse Waard (IPKW)

6827 AV Arnhem

+31(0)26 31 20 223

 info@elaad.nl

 [@ElaadNL](https://twitter.com/ElaadNL)

 www.elaad.nl