Secure and manipulation-proof TLS communication with Plug and Charge

Ahmet Kilic (✉ ahmet.kilic@nisantasi.edu.tr)
Nisantasi University

Research Article

Keywords: Plug and Charge, ISO 15118, TLS, PKI, secure communication, charging, interoperability, validation, verification

Posted Date: April 28th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2853445/v1

Abstract

PnC according to ISO 15118 enables most secure charging session and highest comfort for user and secure and manipulation-proof communication between electric vehicle and charging station. This secure communication is ensured by encrypted communication channel and asymmetric cryptographic algorithms using PKI. The encrypted communication channel between EV and EVSE must be ensured by using Transport Layer Security (TLS) according to ISO 15118. To realize V2G communication between EV and EVSE, first line certificates between EV and EVSE must be validated and verified. Due to new standard for TLS and due to new PKIs the requirements for TLS are significantly changed. With this work all requirements for TLS are collected, evaluated and solution concepts for secure realization of TLS function are derived. Here new concepts and solutions for secure TLS are developed, which are based on Cross Certificate Sign and on use of the network solutions within the PnC Ecosystem. These solutions are validated and verified in a testbench, and it is ensured that secure TLS function is also possible without Interoperable PKIs. So, a user can establish a secure TLS function at the charging station.

1. Introduction

Charging systems is decisive for the future of electromobility. The use of hybrid or electric vehicles is increasing sharply [1]. The high-voltage battery in the electric vehicle must be charged [2] and an invoice must be generated at the end of the charging process. For this, each charging process must be authenticated and authorized to start a charging process. In the state of the art, there are different manual method for activating the charging processes e.g. using app, scanning a QR code or RFID card. User needs to download app from each provider and manually type in step by step to start a charging session. This manual method bind with high effort for user. User needs to have multiple RFIDs from each individual provider and find matching RFID card for corresponding charging station. RFID card is not convenient and not secure for user because RFID can be easily copied. Thus RFID card is little or light security against manipulation and misuse.

On the opposite manual methods, there is automatic activation of the charging session with Autocharge or Plug and Charge. Both Autocharge and Plug and Charge (PnC) are used for the Combined Charging System (CCS). Overall, both methods allow for a seamless and customer-friendly charging process.

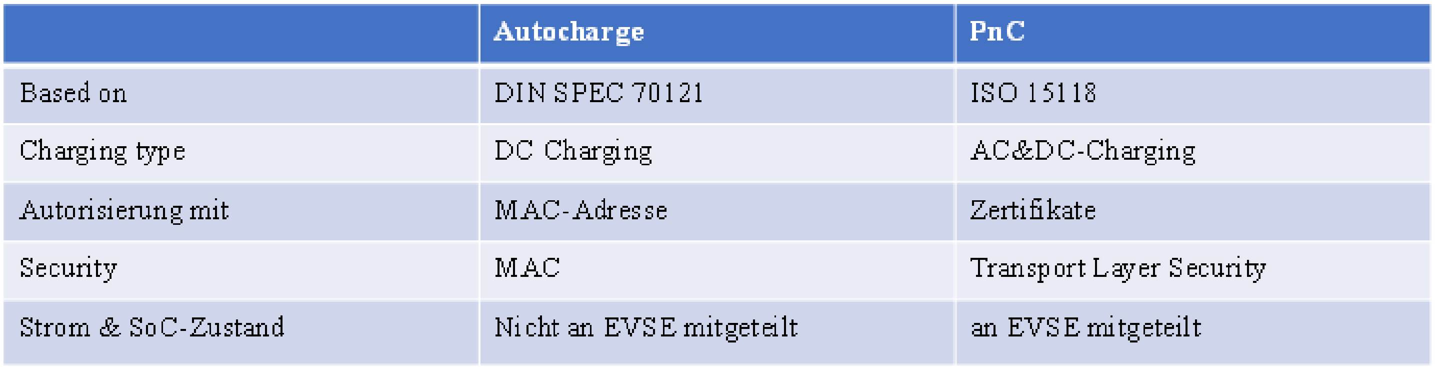
With Autocharge, user needs to plug in the charging cables to the vehicle. The vehicle sends its MAC address to the charging station. The charging station gets this authorization request from vehicle with this MAC address and forwards to CPO [3–4]. The CPO then reads the MAC address from the received authorization request and checks whether the MAC address matches a whitelist of EV MAC addresses. If the MAC address matches, then the CPO sends back a confirmation or release for authorization to the charging station. Thus, the charging session for that vehicle can be started. In order for the MO to generate an invoice for the charging process, MAC address must be associated with the MO user account.

The differences between RFID and Autocharge is based on security and convenience for end users. Autocharge brings higher convenience and relatively easy implementation compared to RFID cards. Autocharge has higher security level compared to RFID technology because MAC addresses are not as easy to duplicate as RFID cards.

The differences between Autocharge and PnC are security and complexity. The security in Autocharge is based on MAC address. MAC address can be changed or manipulated from someone. Manipulation of MAC address is easy and security levels need to be optimized several man-in-the-middle attacks. If MAC address is changed or manipulated by someone, there is no way to automatically detect this data manipulation. Thus, a user's account can be accessed. That is why MAC address has no effective security in data communication and MAC address is however used as an identifier for charging and invoicing process.

PnC, on the contrary Autocharge, enables secure communication and data exchange by establishing an encrypted communication channel between EV and EVSE and by creating and verifying digital signatures. Thus, PnC enables not only convenient charging session but highest security for user and vehicle. In PnC, the security is based on TLS, Table 1.

Table 1: Comparison between Autocharge and (PnC) Plug and Charge



	Autocharge	PnC
Based on	DIN SPEC 70121	ISO 15118
Charging type	DC Charging	AC&DC-Charging
Autorisierung mit	MAC-Adresse	Zertifikate
Security	MAC	Transport Layer Security
Strom & SoC-Zustand	Nicht an EVSE mitgeteilt	an EVSE mitgeteilt

With PnC, the absolutely secure and manipulation-proof communication and authorization between the electric vehicle and the charging station and that at the highest user comfort is realized by a combination of symmetric and asymmetric cryptographic algorithms, by Digital Certificates of a Public Key Infrastructure (PKI) and by encrypted and signed V2G messages. Therefore, PnC enables secure and scalable IT systems to seamlessly authenticate users, automatically authorize them for the charging process, and bill them after the charging process.

This setup of encrypted communication channel between EV and EVSE can be ensured by using Transport Layer Security (TLS). The possibility with TLS will prevent unauthorized access via spoofed MAC addresses. TLS is very important not only to realize encrypted communication channel between EV and EVSE, but also to start first phase V2G communication between EV and EVSE. Without successful TLS, no charging process can be started at the charging station. Thus TLS must be successfully implemented.

In the literature, TLS requirements were previously based on ISO 15118-2 with TLS 1.2 [5]. With the introduction of new norms (ISO 15118-20) [6] and standards, as well as PKIs, the requirements for TLS have changed significantly, which are not considered in the literature, Fig. 1. There is no validation for TLS functions. In literature so far TLS function is considered as conceptual or from existing security aspects, see Chap. 2.

ISO 15118 requires the encrypted communication channel for the secure communication between EV and EVSE according to TLS and the validation of the certificate files in EV and EVSE. With the introduction of multiple PKIs, the validation of the certificate files is even more difficult, which are not considered in the literature so far. What are the influences of interoperability on TLS and how can TLS work with or without interoperability. This are also so far not clear, or no literatures known.

Not only norm and standard have an influence on TLS communication, but also other players have a direct or indirect influence, see Fig. 1. Some OEMs want to have only one root CA from a PKI for storage space reasons. Or user does not want to have many certificates for license cost reasons. The goal of this work is to collect, analyze and evaluate these requirements from all players for TLS. From these evaluations issue, new concepts and solutions shall be created. These solutions are to be validated and verified with a test.

The rest of this paper is organized as follows. The rationale is presented in Section 1. The requirements are presented in Section 2. Section 3 deals with root cause identification and solution concepts. In Section 4, a validation environment for TLS function is built and described. With this validation environment, the validation of TLS function is performed in section to verify the developed solutions. Finally, in section 6 the conclusion is presented.

2. State of the art and requirements

2.1 State of the art for PnC with TLS functions

In literature so far quite, limited work is known for PnC with TLS functions [7–9], in these existing works TLS function (TLS 1.2) with PnC was considered only for ISO 15118-2 in particular only on encryption and validation of certificates for TLS handshake was not found. Previously used TLS 1.2 for PnC was standardized from in 2008 [10]. Since August 2018, a new TLS 1.3 has been developed and published by Internet Engineering Task Force (IETF) [11, 12], which encodes feedback and ideas about a document. This is called Request For Comments or RFC, which TLS 1.3 is defined by RFC 8446 [11]. TLS 1.3 allows lower latency (faster) and more secure than TLS 1.2 as well as optimized cryptographic algorithms compared TLS 1.2. TLS 1.3 is latest version and modern version of SSL as well as used by HTTPS and other network protocols for encryption. In [13–15] the general recommendations for encryption (TLS-ECDH or TLS-ECDHE) according to ISO 15118-2 and storage of keys in HSM were described. Risks assessment due to Cybersecure on the communication between the SECC and the secondary Actor [16]. The possibilities of server authentication towards the client are described in [17] with TLS.

2.2 Comparison of old and new TLS requirements

TLS 1.2 according to ISO 15118-2 was deployed and used for PnC in 2014. In recent years, the requirements for PnC with TLS function have changed significantly. Due to increasing cyber security attack in vehicle, secure communication plays more importance for user and OEM. As a result, TLS requirements were changed by both OEM and ISO 15118. With ISO 15118-20, the TLS requirements are significantly more stringent [17].

2.2.1 Authenticity of the sender by encrypting the certificates

Previously, the authenticity of the sender and the integrity of the received message were verified with signatures using SHA-256 as the cryptographic hash function according to the Elliptic Curve Digital Signature Algorithm (ECDSA) in ISO 15118-2.

In ISO 15118-2, Elliptic Curve secp256r1 (256 bits) key was used for certificate encryption.

In ISO 15118-20 SHA-512/SHAKE256 can be used as cryptographic hash function, secp521r1 / Ed448 keys can be used for certificate signing and encryption.

2.2.2 TLS-session key

The only task of session key is to establish a security layer. That is to encrypt the further communications in the session using the key.

For each charging process or TLS session a new TLS-session key is created. TLS-session key is a temporary symmetric cryptographic key because the same key is used for both encryption and decryption of the data between EV and EVSE. This symmetric key (same key derived by EVCC and SECc) and cannot be derived by any other entities (3rd party). The creation of the TLS session key is changed with ISO 15118-20 and a new cryptographic algorithm is used.

For ISO 15118-2, Elliptic Curve Diffie-Hellman (ECDH) was used by secp256r1 as the key agreement protocol to agree on a common (symmetric) TLS session key.

For ISO 15118-20, secp521r1/ed448 is used.

2.2.3 Requirements for relevant certificates in EV and EVSE

PnC according to ISO 15118 enables the highest convenience and most secure charging process for users and an absolutely secure and manipulation-proof communication between the electric vehicle and charging station, this achieved by a combination of symmetric and asymmetric cryptographic algorithms using a PKI. In a PKI, a public key and a private key encrypt the data exchanged between two EVs and EVSE after they have authenticated themselves through a secure TLS handshake.

As part of the PKI, secure digital certificates ensure that the parties involved are before any data is exchanged. This is very important for mobility operators to ensure that all users of the energy infrastructure are valid. For this reason, relevant certificate in EV and EVSE has been defined quite fixed according to ISO 15118-2 &-20.

In EV (EVCC), according to ISO 15118-2, at least one V2G-Root CA, OEM-Provision Certificate (PCID), Contract Certificate (EMAID) and according to ISO 15118-20 additionally Vehicle Leaf Certificate must be installed, Fig. 2.

In the EVSE (SECC), at least EVSE-Leaf Certificate (EVSE-Leaf) must be installed, and it is recommended to store all Root CA or more than 10 Root CAs in EVSE, see Fig. 2.

2. 2. 3 Requirements verification of certificates in EV and EVSE

According to ISO 15118-2: TLS 1.2:

According to ISO 15118, an encrypted communication session is established with a so-called Transport Layer Security (TLS) handshake between EV and EVSE. During this TLS handshake, the charging station presents its digital certificates (EVSE Leaf certificate, CPO Sub CA 1 certificate, and optionally CPO Sub CA 2 certificate) to the EV to identify itself as a trusted charging station. The EV must then verify the digital signature of all certificates - from the EVSE certificate to the pre-installed V2G root CA certificates - and check if any of the certificates have expired. If everything was verified without any problems, a TLS session is then successfully established, Fig. 3.

- To start TLS communication between EV and EVSE, EVSE-Leaf must be validated in EV against the V2G root.
- EV sends a TLS-Req (incl. list of root CA)
- EVSE returns a response with [EVSE/SECC Leaf Cert + CPO SubCA1 + 2]. This response EVSE -Leaf CA has to be validated by V2G in the EV.
- If the verification was successful, TLS can be started, like Scenario 1.
- If both certificates are created from different root CA, verification is not successful, like Scenario 2, TLS cannot be started. It is a security issue because the encrypted communication cannot be established.

According to ISO 15118-20: TLS 1.3:

With mTLS 1.3 TLS handshakes is still a roundtrip (or mutual communication) instead of TLS 1.2 requested or with ISO 15118-20 mutual validation must take place according to TLS 1.3. EVSE Leaf Certificate must be verified by V2G root CA in EV. The EVCCID -Leaf must be verified by V2G root or OEM root CA in EVSE. After both times of successful certificate validation, TLS communication may be established.

According to ISO 15118, TLS handshake must be used, and certificates must be successfully verified between EV and EVSE. Here it was identified that due to different PKIs (root CAs) a successful TLS handshake cannot be started (scenario 2). As a result, no charging process can be started, which is disadvantageous for users at the charging station. It is a root cause. This root cause needs to be fixed. To fix this root cause and to realize a secure and successful TLS handshake, new concepts and solutions are created and developed here, see Chap. 3.

3. Solution concept

In scenario 2, no TLS handshake can be performed due to different PKIs. Here, some possible solutions have been developed and used from ISO 15118 to realize a secure and successful TLS handshake for scenario 2. Here are the solution concepts:

- Interoperable solutions
- Non-interoperable solutions

3.1 Interoperable Concepts

According to ISO 15118, two options for interoperable root CA have been proposed, Cross Certificate Recognition according to ISO 15118-2 and Cross Certificate Sign according to ISO 15118-20. With Cross Certificate Recognition, multiple V2G root CA can be installed into the EV. With Cross Certificate Sign, one V2G root CA is sufficient since the agreement for the use of the root CA between the PKIs is in place.

TLS handshake can be successfully performed with interoperable root CAs (PKIs), Fig. 6, although the root CAs in EV and EVSE are different. For this, there must be coordination for sharing the root CA between the PKIs.

3.2 Non-interoperable concepts

Non-interoperable solutions are based on the use of the PnC network. To realize a secure and successful TLS handshake, missing root CAs from PnC network should be provided in EV or EVSE and installed in EV and/or EVSE. Thus, a secure TLS handshake can be performed, Fig. 7. For non-interoperable solutions, there are two options, as shown in Fig. 7.

Solution B: Provide EVSE Leaf Certificate from PnC network.

Vehicle has V2G root CA from PKI-A and EVSE has Leaf Certificate from PKI-B. In this concept TLS handshake is not possible. Using this PnC network solution, the EVSE sends a CSR to CPO for EVSE Leaf Certificate from PKI-A. CPO accepts this request and communicates with RCP from PKI-A. From RCP gets the EVSE -Leaf Certificate from PKI-A and forwards to EVSE. This PKI-A is installed in EVSE. Thus EV and EVSE have the same root CA. This allows TLS handshake to be performed successfully, Fig. 8.

Solution C: Provide V2G root CA from PnC Network.

Vehicle has V2G root CA from PKI-A and EVSE has Leaf Certificate from PKI-B. In this concept, TLS is not possible. With this PnC Network solution, a request is issued from EV to RCP for V2G root CA from PKI-B via OEM backend. This request shall be done via OTA. OEM backend accepts this request and communicates with RCP from PKI-B. From RCP fetches V2G root CA from PKI-B and forwards to EV. This PKI-B is installed in EV. Thus EV and EVSE have the same root CA. This enables TLS handshake to be performed successfully, Fig. 9.

Here, three different possible solutions for a successful and secure TLS handshake are developed and brought to enable a charging process for a user at the charging station. Solution A is based on interoperability and solutions B&C are independent of interoperability. Now these concepts need to be validated and verified, see Chap. 5.

4. Validation environment

To validate and verify these developed concepts from Chap. 3, a test environment was developed and built here, Fig. 10.

Electric Vehicle (Electric Vehicle Communication Controller) is simulated here with a toolbox from Verisco. This toolbox is covering all relevant communication for ISO 15118. OEM relevant certificates are V2G root CA, PCID and EMAID already installed. There can be new or multiple certificates installed in toolbox.

This toolbox from Versico, connected with DC charging stations via charging cable has also enabled WLAN communication with cloud.

Here is a real DC charger used as EVSE from Alpitronic Hypercharger model HYC 150DC wall box. This EVSE enables access control via Plug and Charge (ISO 15118) and communication via LAN, WLAN or mobile data connection. It is compatible with various backend systems via OCPP 1.6. EVSE is a Seitz connected to EVCC (toolbox) via charging cable according to conductive charging system for electric vehicles according to DIN EN61851-1) and other Seitz connected to mains.

5. Validation results

Scenario 2 was first tested with this testbench. EV and EVSE have different root CAs. As a result, no TLS handshake can be established between EV and EVSE, see Fig. 11. The system issues an error indicating that the charging process cannot be started, Fig. 11.

With different root CA between EV and EVSE no TLS handshake could be established. This causes the system to return an error that the charging process cannot be started. For this root cause a solution concept C is developed in Chap. 3. The solution concept C was tested with this established test bench. This fetched an additional V2G root CA from PKI-B and installed it in EV. Thus, a successful TLS handshake was established, see Fig. 12. Now, further charging process can be started because TLS - handshake is successfully completed.

As verified in this concept C, TLS handshake without interoperability PKIs is also possible. From this work it is derived and stated that secure TLS handshake is possible in scenario 2 without interoperability PKIs, see Fig. 12.

6. Conclusion

Plug & Charge according to ISO 15118 enables the highest comfort and safest charging process for users and an absolutely secure and manipulation-proof V2G communication between the electric vehicle and charging station, which is created by cryptographic algorithms, digital certificates and encrypted and signed V2G messages within the Plug & Charge ecosystem. Through this higher data security and protection against fraud and misuse with PnC trusts user and OEM for the use of PnC. According to ISO 15118, vehicle and charging station must create an encrypted V2G communication session with a so-called Transport Layer Security (TLS) handshake between vehicle and charging station.

In literatures so far only security aspects of TLS function according to ISO 15118-2 were considered conceptually and validation for TLS function was not known.

With the introduction of ISO 15118-20 since April 2022 and the entry of new PKIs since November 2022, the requirements and validation and verification of TLS functions must be redefined. With this work, all these new requirements from literatures, standards and standard are collected and summarized. The causes are not possible TLS function identified, evaluated, and validated. Here the influences of the new requirements (e.g., different PKIs between EV and EVSE) on TLS handshake were investigated. The different PKIs does not lead to successful TLS handshake. As a result, the charging session cannot be started. To fix this cause, realize a secure and successful TLS function, three new concepts and solutions were brought here. This allows user to charge his electric vehicle safely at the charging station. These solutions are independent of each other. The realization of TLS function is ensured with these solutions. Here are the Details:

First solution is based on interoperability with cross certificate sign between PKIs. If PKIs are aligned with each other for certificate merging, then validation at the charging station can work.

Second and third solution is based on using the network solutions within the PnC ecosystem. Certificates missing through the network can be provided in EV (solution 2) or in EVSE (solution 3). Thus, TLS function between vehicle and charging station can be realized without interoperability.

To realize this concept and solutions a testbench was developed and built. With validation in testbench investigations, successful TLS function was performed and proved that secure TLS function without interoperable PKIs is also possible.

Abbreviations

CCS	Combined Charging System

CCP	Contract Certificate Pool
CPO	Charge Point Operator
DHP	Dittmann Hall Public key
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic curve Diffie-Hellman
EMAID	E-Mobility Account Identifier
EV	Electric Vehicle
EVCC	Communication Controller
EVSE	Electric Vehicle Supply Equipment
HTTPS	Hypertext Transfer Protocol Secure
MO	Mobility Operator
MAC	Machine Aided Cognition
mTLS	Mutual Transport Layer Security
OTA	Over -The-Air
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OCPP	Open Charge Point Protocol
OCPI	Open Charge Point Interface
OICP	Open Inter Charge Protocol
OPCP	Open Plug Charge Protocol
PnC	Plug and Charge
PuS	Pool&Service
RFC	Request For Comments

PCID	Provisioning Certificate ID
PKI	Public Key Infrastructure
RCP	Root Certificate Pool
SECC	Supply Equipment Communication Controller
SECP	Refers to the parameters of the elliptic curve
SHA	Secure Hash Algorithm
SHAKE	Online Hash function
SSL	Secure Sockets Layer
Sub-CA	Subordinate Certificate Authority
TCP	Transmission Control Protocol
TLS	Transport Layer Security
V2G	Vehicle to Grid
WLAN	Wireless Local Area Network

Declarations

Research data policy and data availability statements The results/ data/figure in this manuscript have not been published elsewhere, nor are they under consideration by another publisher. The data sharing not applicable to this article as no datasets were generated or analyzed during the study.

Conflict of interest The authors declare that they have no competing interests as defined by Springer, or other interests that might be perceived to influence the results and/or discussion reported in this paper.

Ethical approval The authors have read the Springer journal policies on author responsibilities and submit this manuscript in accordance with those policies. Further, the authors did not receive support from any agency/organization for the submitted work and this research work does not involve any human participants and/or animals.

References

1. Kilic A., New fail operational powernet methods and topologies for automated driving with electric vehicle," Turkish Journal of Electrical Engineering and Computer Sciences: Vol. 29: No. 2, Article 39. https://doi.org/10.3906/elk-2005-14

2. Kilic A., Patent Apparatus and method for electrically connecting a charging station to a charging socket of a vehicle, US patent US20170349055A1, in 2017
3. How Autocharge works with OCPP https://github.com/openfastchargingalliance/openfastchargingalliance/blob/master/autocharge-final.pdf
4. DIN SPEC 70121 Elektromobilität - Digitale Kommunikation zwischen einer Gleichstrom-Ladestation und einem Elektrofahrzeug zur Regelung der Gleichstromladung im Verbund-Ladesystem, Ausgabe 2014-12
5. ISO 15118-2:2018-06: Road vehicles – Vehicle-to-Grid Communication Interface – Part 2: Network and application protocol requirements. Second Edition. May 2018.
6. ISO 15118-20:2022 Road vehicles - Vehicle-to-Grid Communication Interface - Part 20: 2nd generation network layer and application layer requirements. April 2022.
7. Brighente, A., Conti, M., Donadel, D., Poovendran, R., Turrin, F., & Zhou, J. (2023). Electric Vehicles Security and Privacy: Challenges, Solutions, and Future Needs. *arXiv preprint arXiv:2301.04587*
8. R. Baker and I. Martinovic, “Losing the car keys: Wireless PHY-Layer insecurity in EV charging,” in 28th USENIX Security Symposium (USENIX Security 19). Santa Clara, CA: USENIX Association, Aug. 2019, pp. 407–424. [Online]. Available: https: //www.usenix.org/conference/usenixsecurity19/presentation/baker
9. M. Mültin, "ISO 15118 as the Enabler of Vehicle-to-Grid Applications," 2018 International Conference of Electrical and Electronic Technologies for Automotive, 2018, pp. 1-6, doi: 10.23919/EETA.2018.8493213.
10. T. Dierks and E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.2*, April 2008, [online] Available: https://tools.ietf.org/pdf/rfc5246.pdf.
11. E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, August 2018, [online] Available: https://tools.ietf.org/pdf/rfc8446.pdf.
12. NIST Special Publication 800-52 Revision 2, “Guidelines for the Selection, Configuration, and Use of Transport, Layer Security (TLS) Implementations,” 2019.
13. BSI: Cryptographic Mechanisms: Recommendations and Key Lengths: Part 2 – Use of Transport Layer Security (TLS). Technical Guideline TR-02102-2, Federal Office for Information Security, February 2019. 16, 24, 25
14. D. Kern, Privacy-Preserving Architecture for EV Charging and Billing, Darmstadt 2021Jan10
15. D. Kern, C. Krauß, M. Zhdanova, System Security Mechanisms for Electric Vehicles and Charge Points Supporting ISO 15118, 2019 https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/SIT-TR-2019-04-FINAL.pdf?_=1579176671
16. F. Haidar, Vehicle to Grid, towards a cybersecure electric system including vehicle, charging points and batteries, conference in 2022.

17. Aubel V., Poll E., "Security of EV-charging protocols." *arXiv preprint arXiv:2202.04631* (2022).

18. Kilic A., Plug and Charge solutions with vehicle-to-grid communication, Electric Power Components and Systems (manuscript is accepted), in 19April 2023.

Figures

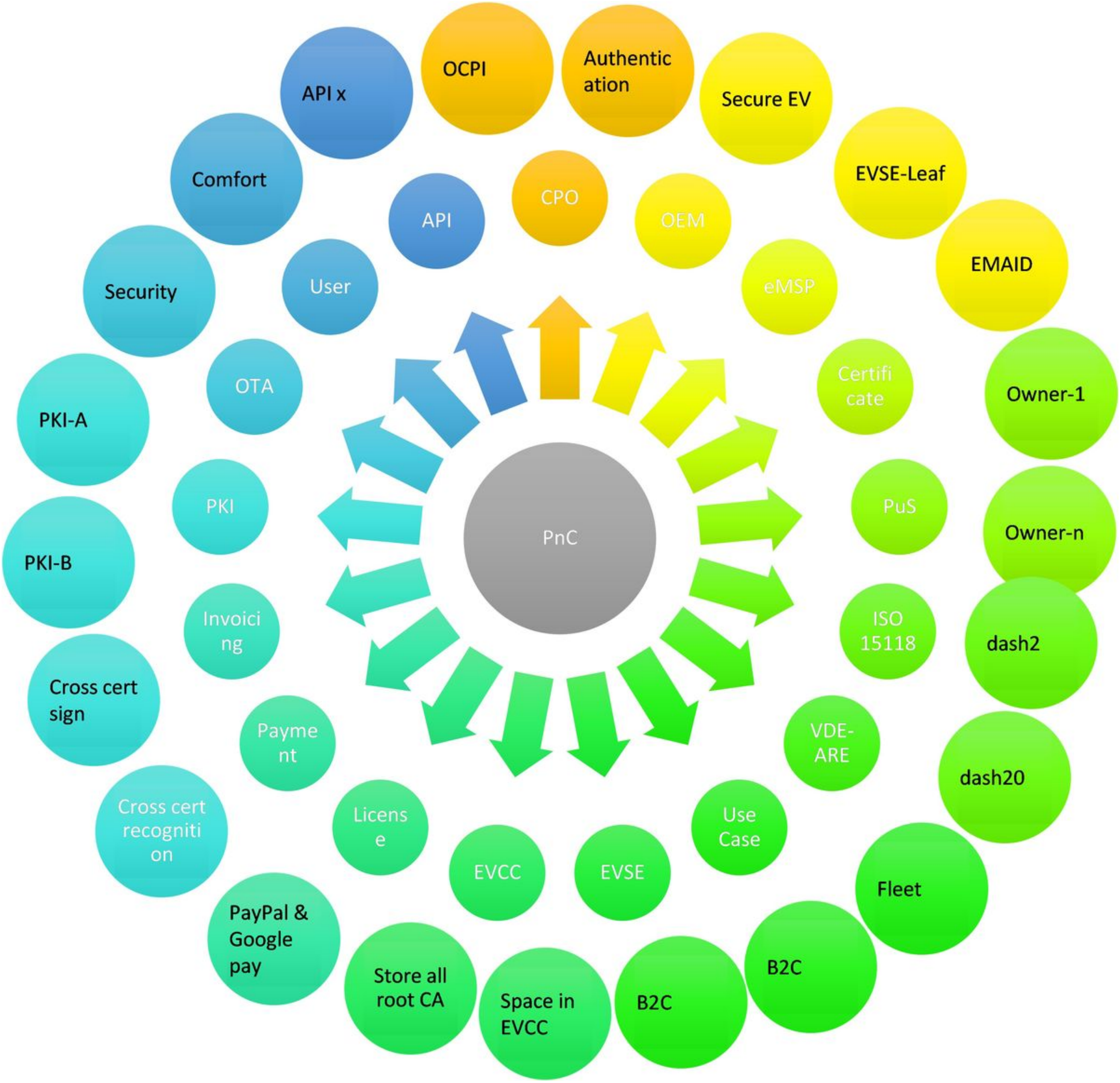
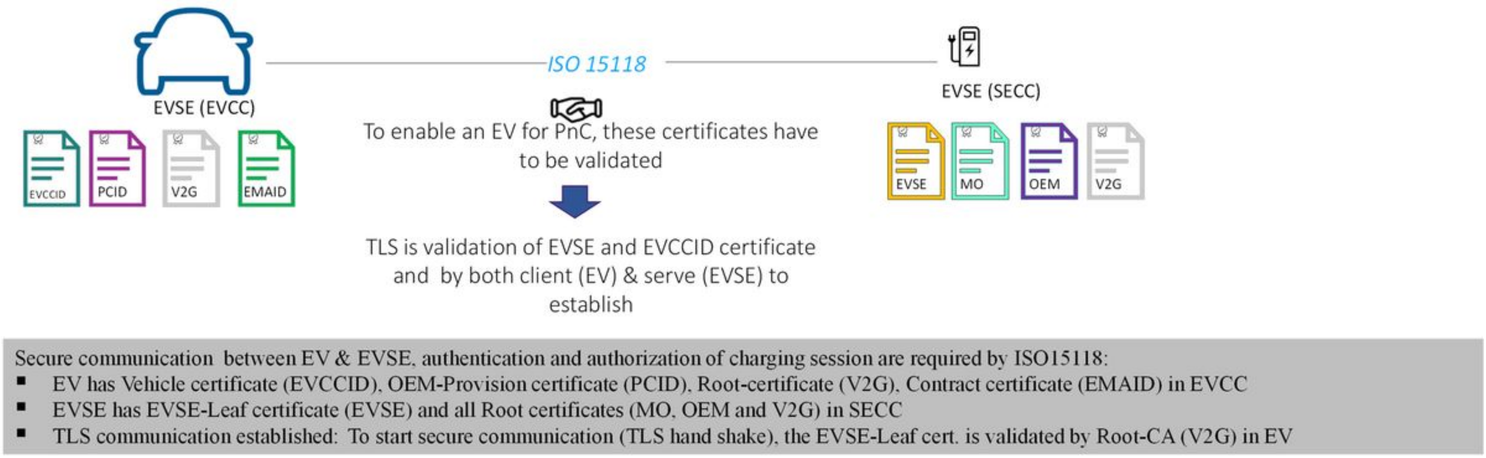


Figure 1

Requirements and players for PnC functions



To enable an EV for PnC, these certificates have to be validated

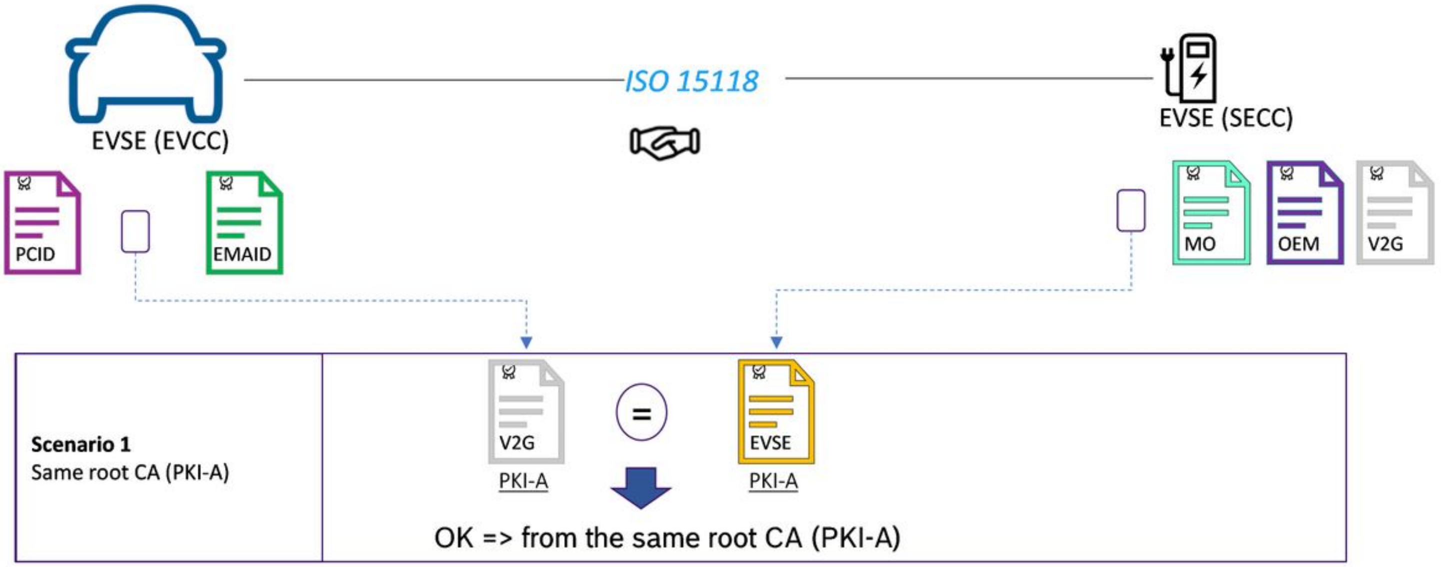
TLS is validation of EVSE and EVCCID certificate and by both client (EV) & serve (EVSE) to establish

Secure communication between EV & EVSE, authentication and authorization of charging session are required by ISO15118:

- EV has Vehicle certificate (EVCCID), OEM-Provision certificate (PCID), Root-certificate (V2G), Contract certificate (EMAID) in EVCC
- EVSE has EVSE-Leaf certificate (EVSE) and all Root certificates (MO, OEM and V2G) in SECC
- TLS communication established: To start secure communication (TLS hand shake), the EVSE-Leaf cert. is validated by Root-CA (V2G) in EV

Figure 2

Technical requirements for the certificates in EV and EVSE for PnC



Scenario 1
Same root CA (PKI-A)

OK => from the same root CA (PKI-A)

Figure 3

Verification of EVSE Leaf Certificate by V2G-root CA in EV on TLS function

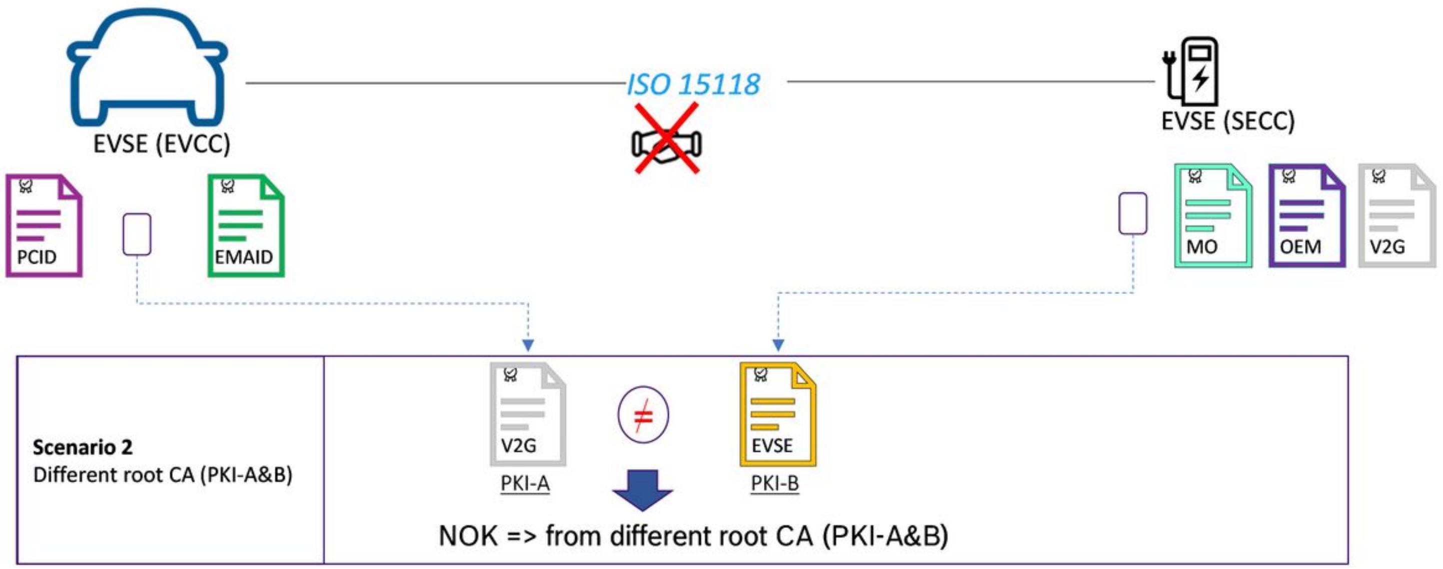
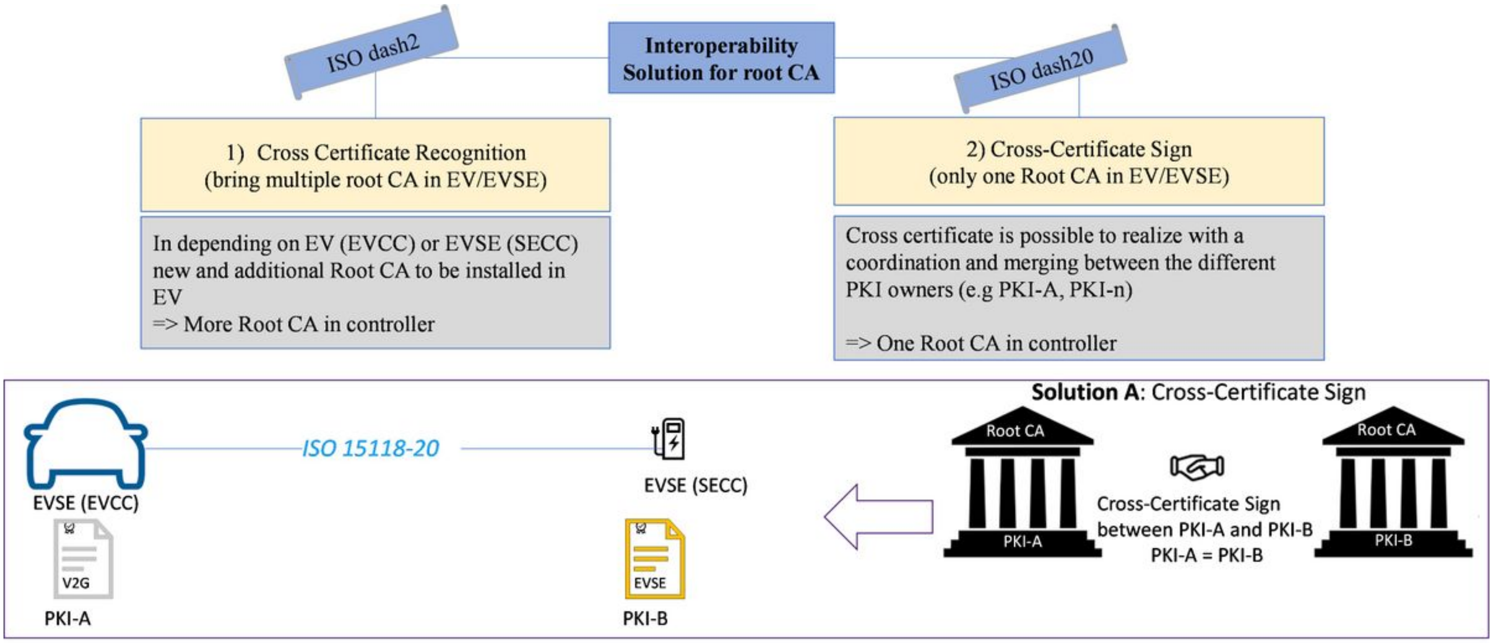


Figure 4

Influences of the different root CA on TLS function


ISO dash2
Interoperability Solution for root CA
ISO dash20
1) Cross Certificate Recognition (bring multiple root CA in EV/EVSE)
2) Cross-Certificate Sign (only one Root CA in EV/EVSE)

In depending on EV (EVCC) or EVSE (SECC) new and additional Root CA to be installed in EV
=> More Root CA in controller

Cross certificate is possible to realize with a coordination and merging between the different PKI owners (e.g PKI-A, PKI-n)

=> One Root CA in controller

Solution A: Cross-Certificate Sign
EVSE (EVCC)
ISO 15118-20
EVSE (SECC)
V2G
PKI-A
EVSE
PKI-B
Root CA
PKI-A
Cross-Certificate Sign between PKI-A and PKI-B
PKI-A = PKI-B
Root CA
PKI-B

Figure 5

Interoperability for root CA according to ISO 15118

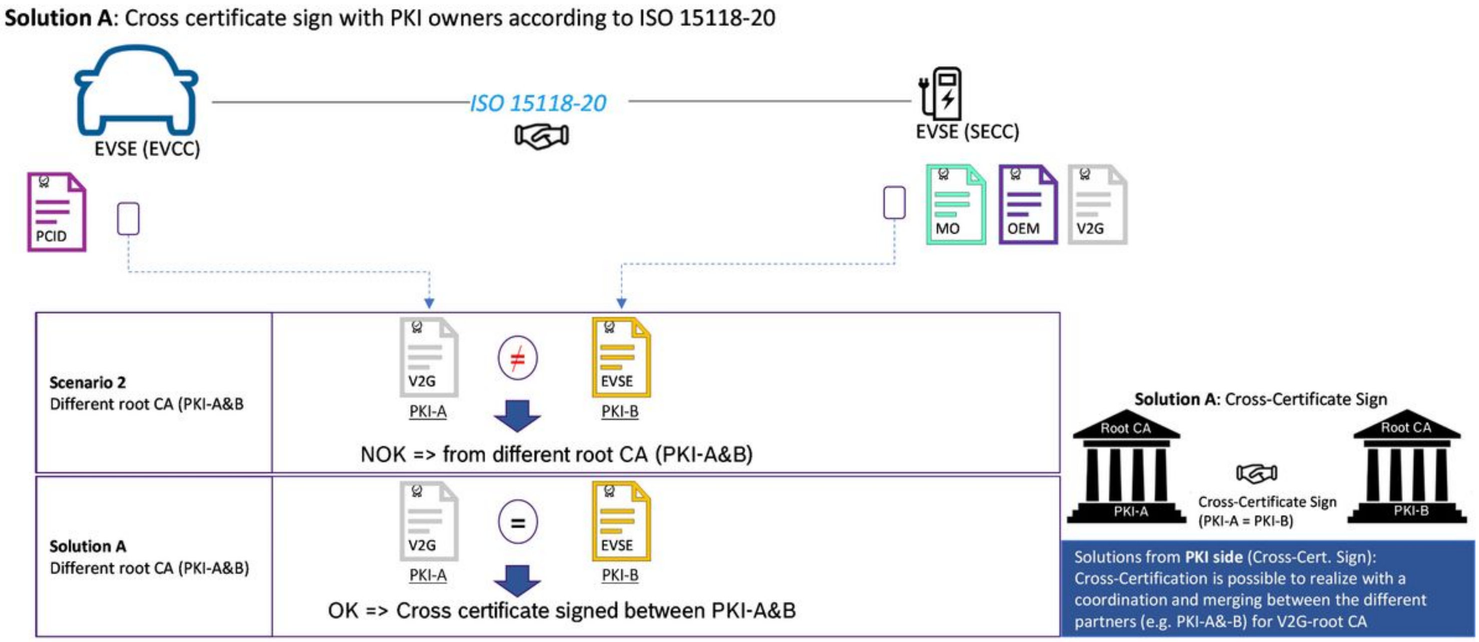

Solution A: Cross certificate sign with PKI owners according to ISO 15118-20
EVSE (EVCC)
ISO 15118-20
EVSE (SECC)
PCID
MO
OEM
V2G
Scenario 2
Different root CA (PKI-A&B
V2G
PKI-A
≠
EVSE
PKI-B
NOK => from different root CA (PKI-A&B)
Solution A
Different root CA (PKI-A&B)
V2G
PKI-A
=
EVSE
PKI-B
OK => Cross certificate signed between PKI-A&B
Solution A: Cross-Certificate Sign
Root CA
PKI-A
Cross-Certificate Sign
(PKI-A = PKI-B)
Root CA
PKI-B
Solutions from PKI side (Cross-Cert. Sign):
Cross-Certification is possible to realize with a coordination and merging between the different partners (e.g. PKI-A&-B) for V2G-root CA

Figure 6

Interoperable solution with Cross Certificate Sign

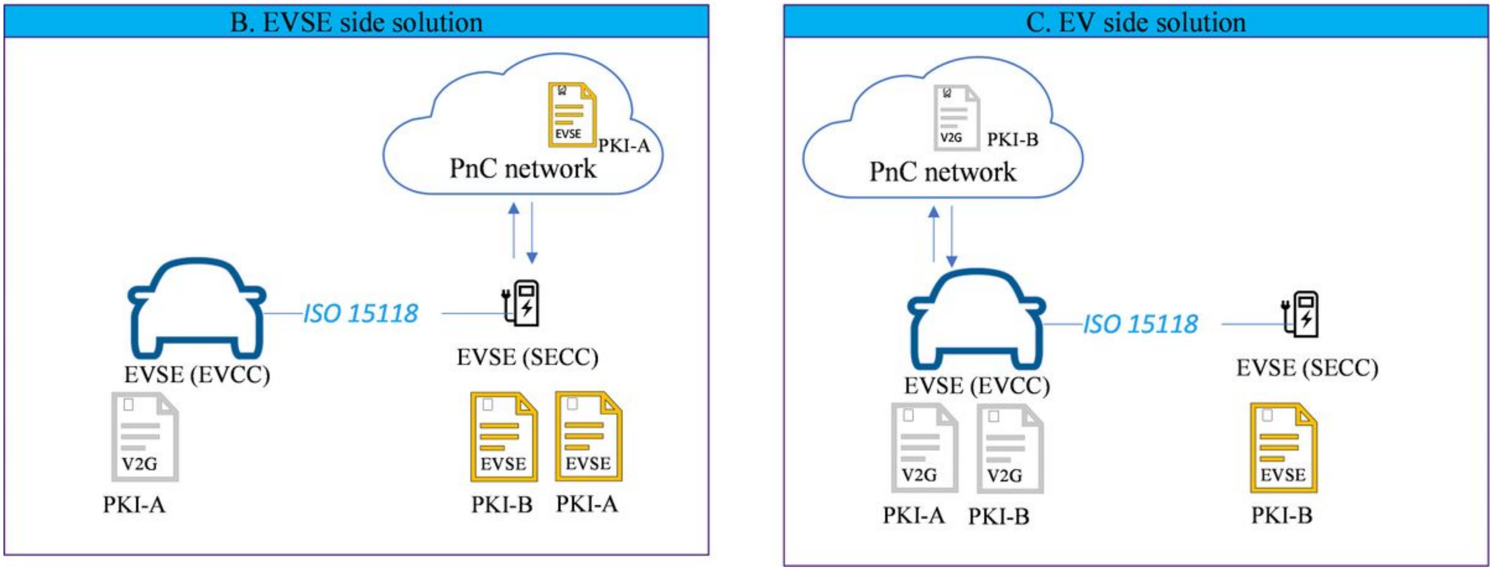


Figure 7

Non-interoperable PnC network solutions

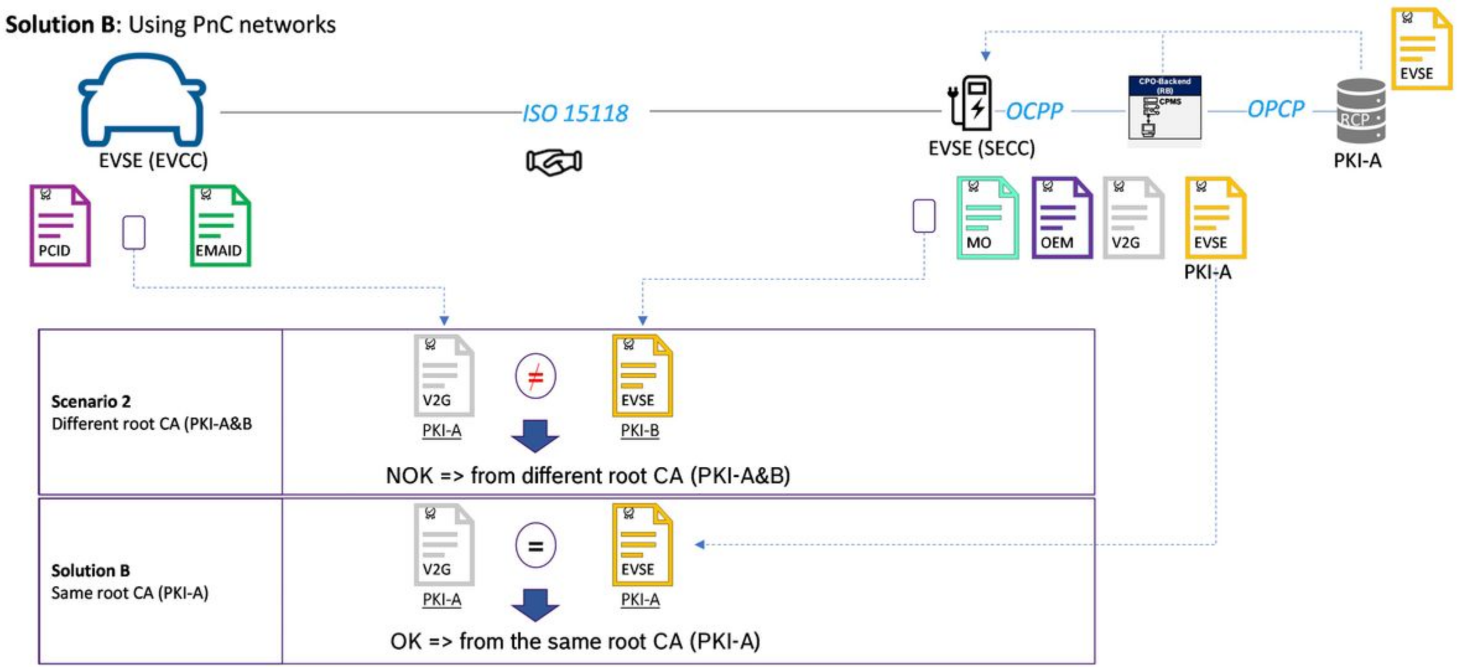


Figure 8

Non-interoperable PnC network solutions for EVSE

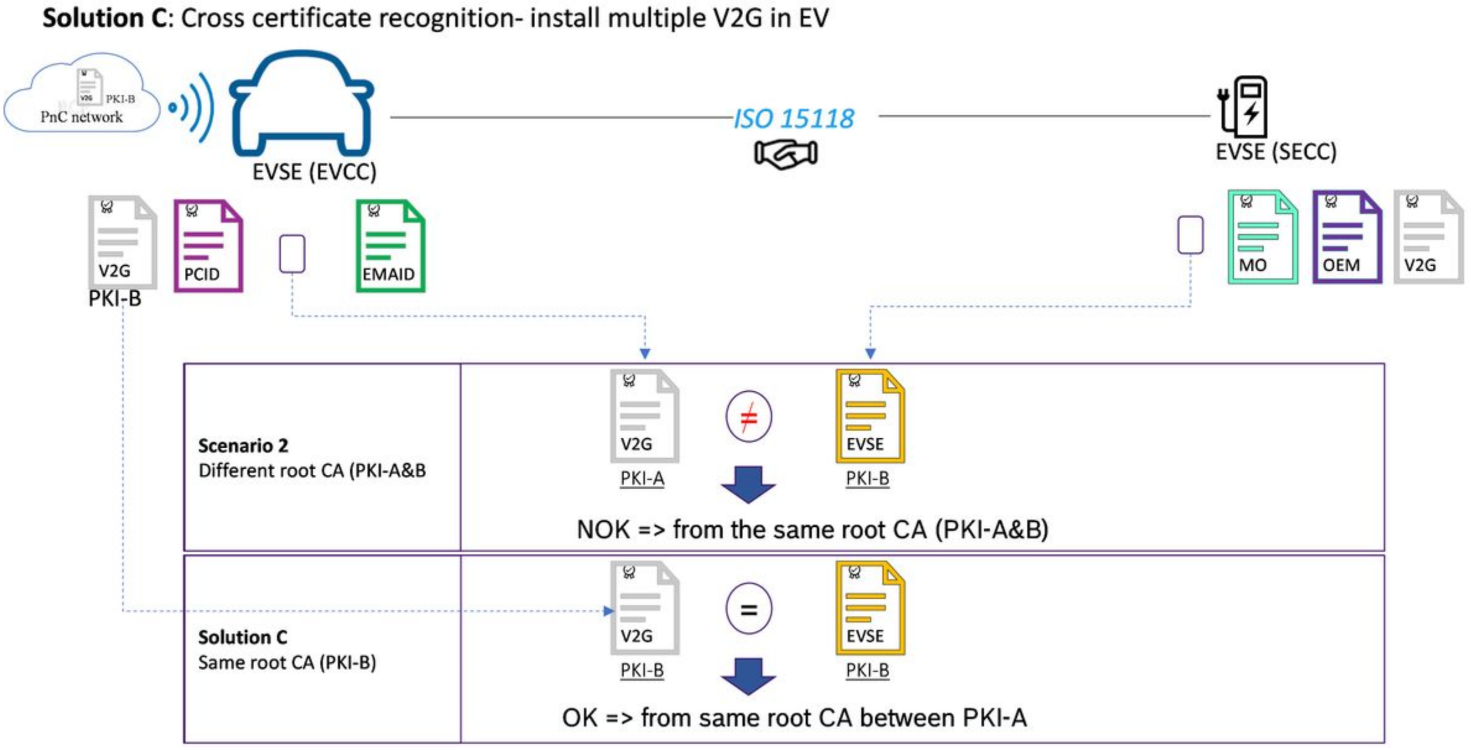

Solution C: Cross certificate recognition- install multiple V2G in EV
V2G
PKI-B
PnC network
EVSE (EVCC)
ISO 15118
EVSE (SECC)
V2G
PKI-B
PCID
EMAID
MO
OEM
V2G
Scenario 2
Different root CA (PKI-A&B
V2G
PKI-A
≠
EVSE
PKI-B
NOK => from the same root CA (PKI-A&B)
Solution C
Same root CA (PKI-B)
V2G
PKI-B
=
EVSE
PKI-B
OK => from same root CA between PKI-A

Figure 9

Non-Interoperable PnC Network Solutions for EV

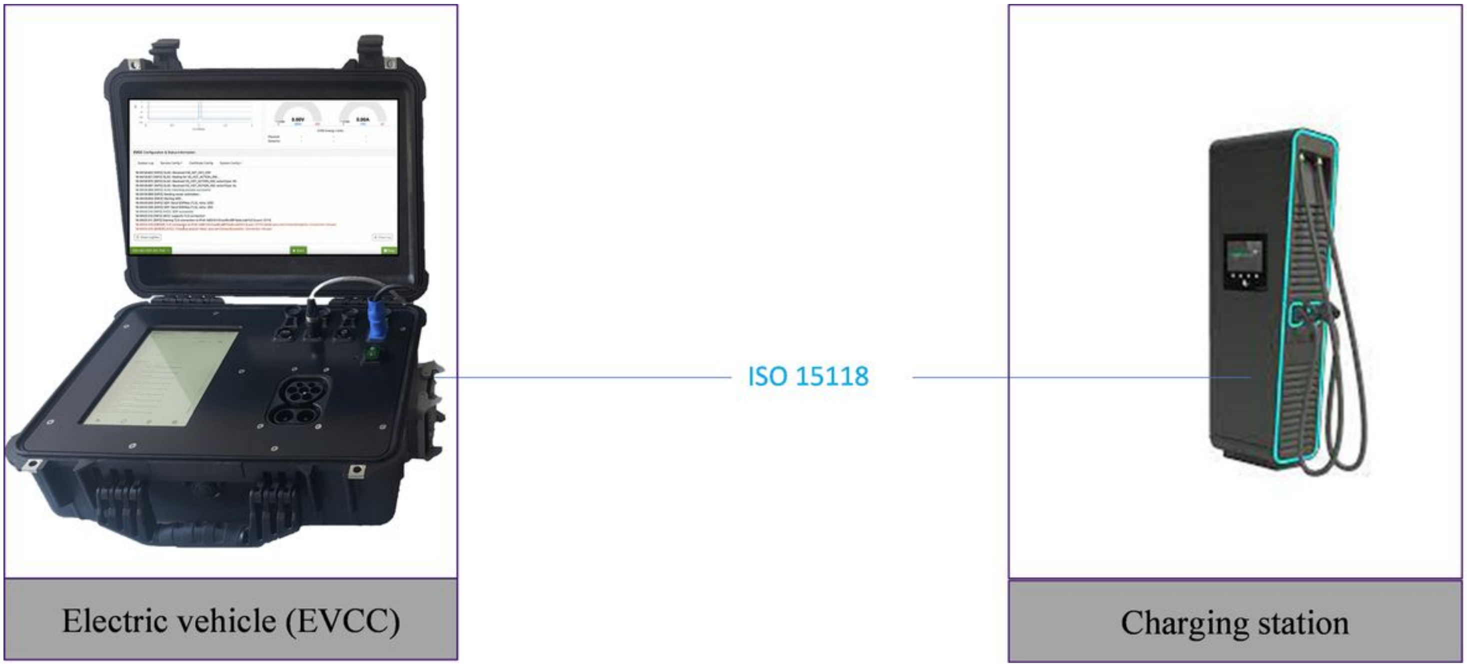
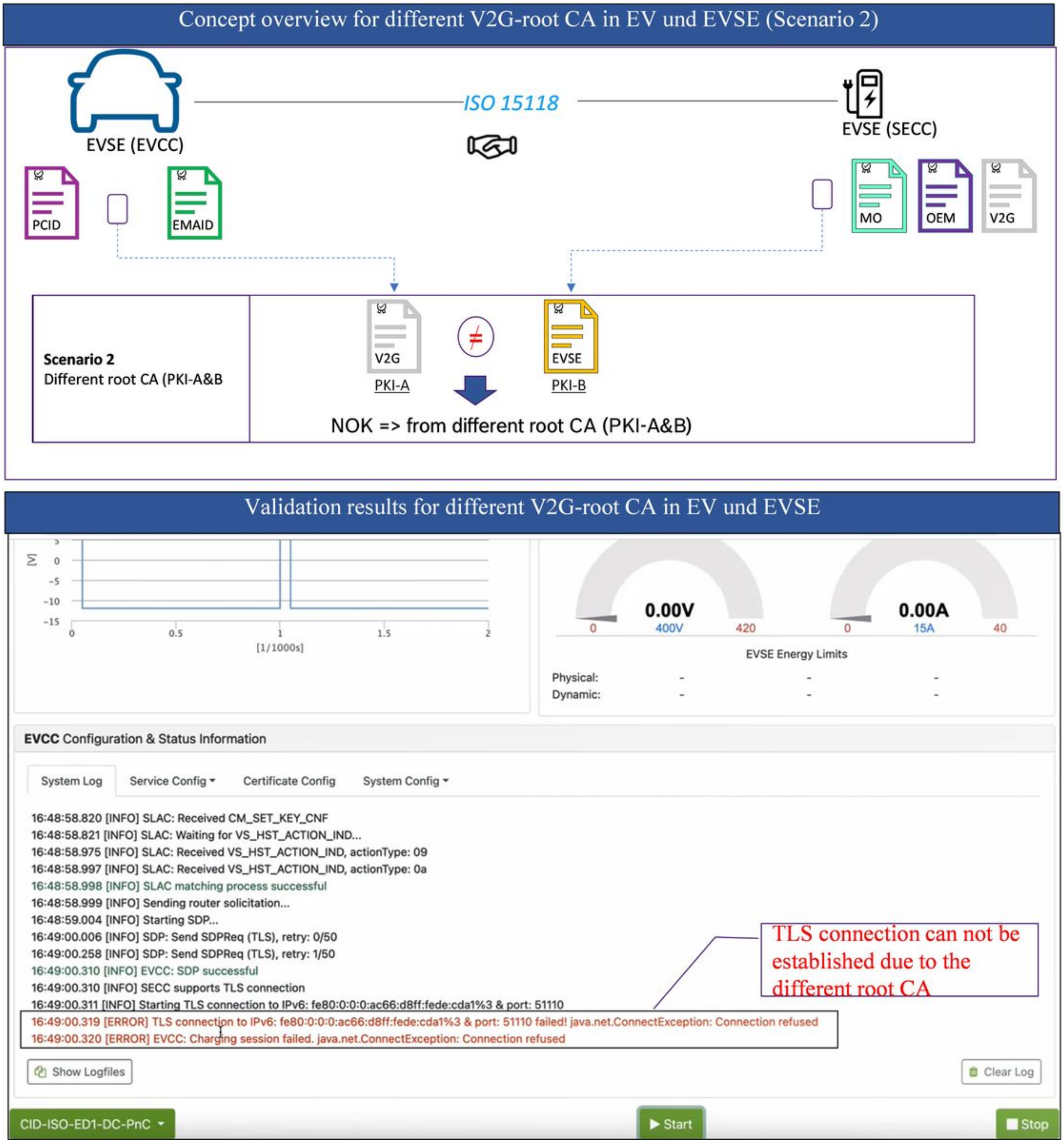


Figure 10

Validation environment for TLS function



Concept overview for different V2G-root CA in EV und EVSE (Scenario 2)

Scenario 2
Different root CA (PKI-A&B

NOK => from different root CA (PKI-A&B)

Validation results for different V2G-root CA in EV und EVSE

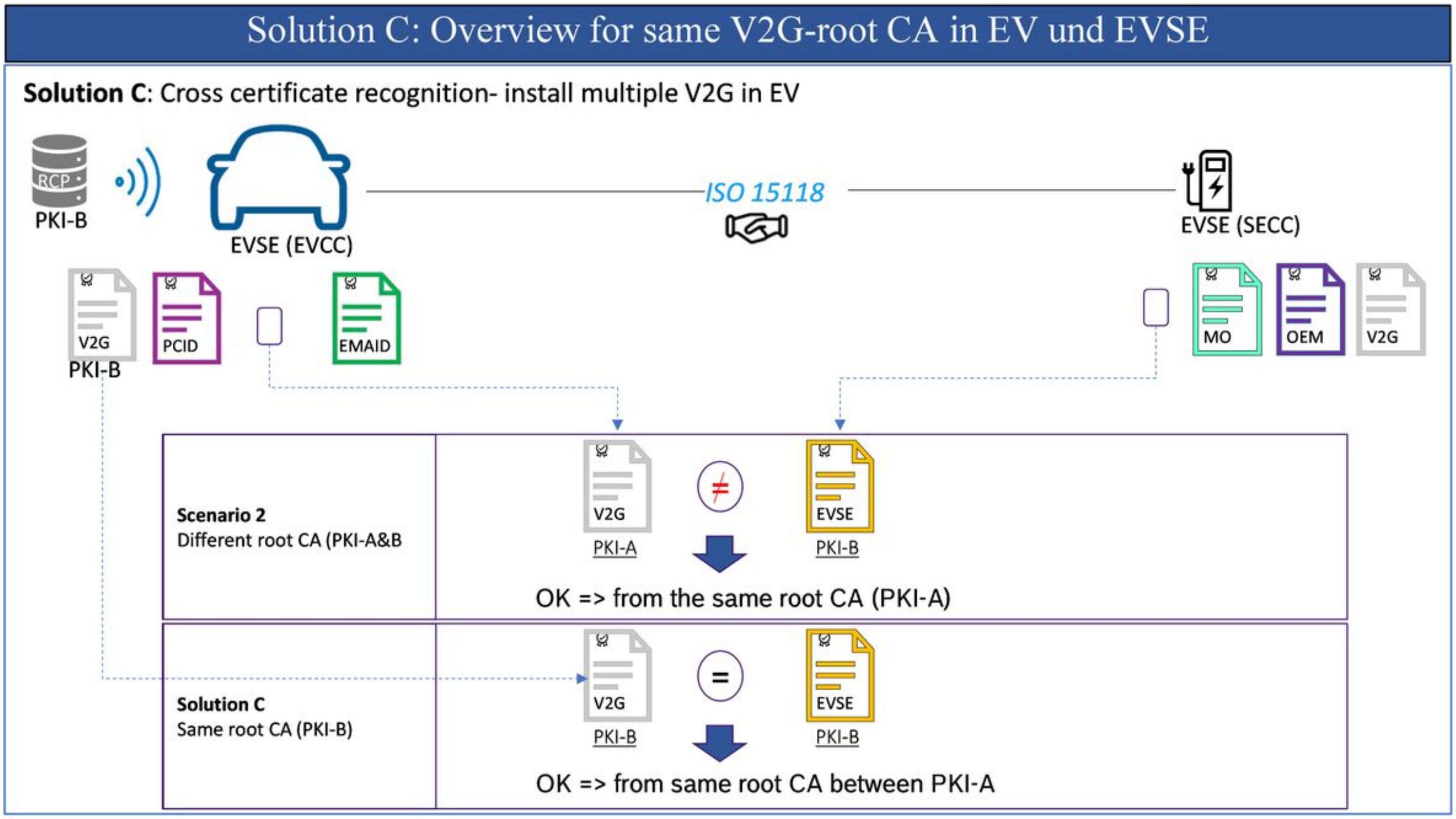
EVCC Configuration & Status Information

```
16:48:58.820 [INFO] SLAC: Received CM_SET_KEY_CNF
16:48:58.821 [INFO] SLAC: Waiting for VS_HST_ACTION_IND...
16:48:58.975 [INFO] SLAC: Received VS_HST_ACTION_IND, actionType: 09
16:48:58.997 [INFO] SLAC: Received VS_HST_ACTION_IND, actionType: 0a
16:48:58.998 [INFO] SLAC matching process successful
16:48:58.999 [INFO] Sending router solicitation...
16:48:59.004 [INFO] Starting SDP...
16:49:00.006 [INFO] SDP: Send SDPReq (TLS), retry: 0/50
16:49:00.258 [INFO] SDP: Send SDPReq (TLS), retry: 1/50
16:49:00.310 [INFO] EVCC: SDP successful
16:49:00.310 [INFO] SECC supports TLS connection
16:49:00.311 [INFO] Starting TLS connection to IPv6: fe80:0:0:0:ac66:d8ff:fede:cda1%3 & port: 51110
16:49:00.319 [ERROR] TLS connection to IPv6: fe80:0:0:0:ac66:d8ff:fede:cda1%3 & port: 51110 failed! java.net.ConnectException: Connection refused
16:49:00.320 [ERROR] EVCC: Charging session failed. java.net.ConnectException: Connection refused
```

TLS connection can not be established due to the different root CA

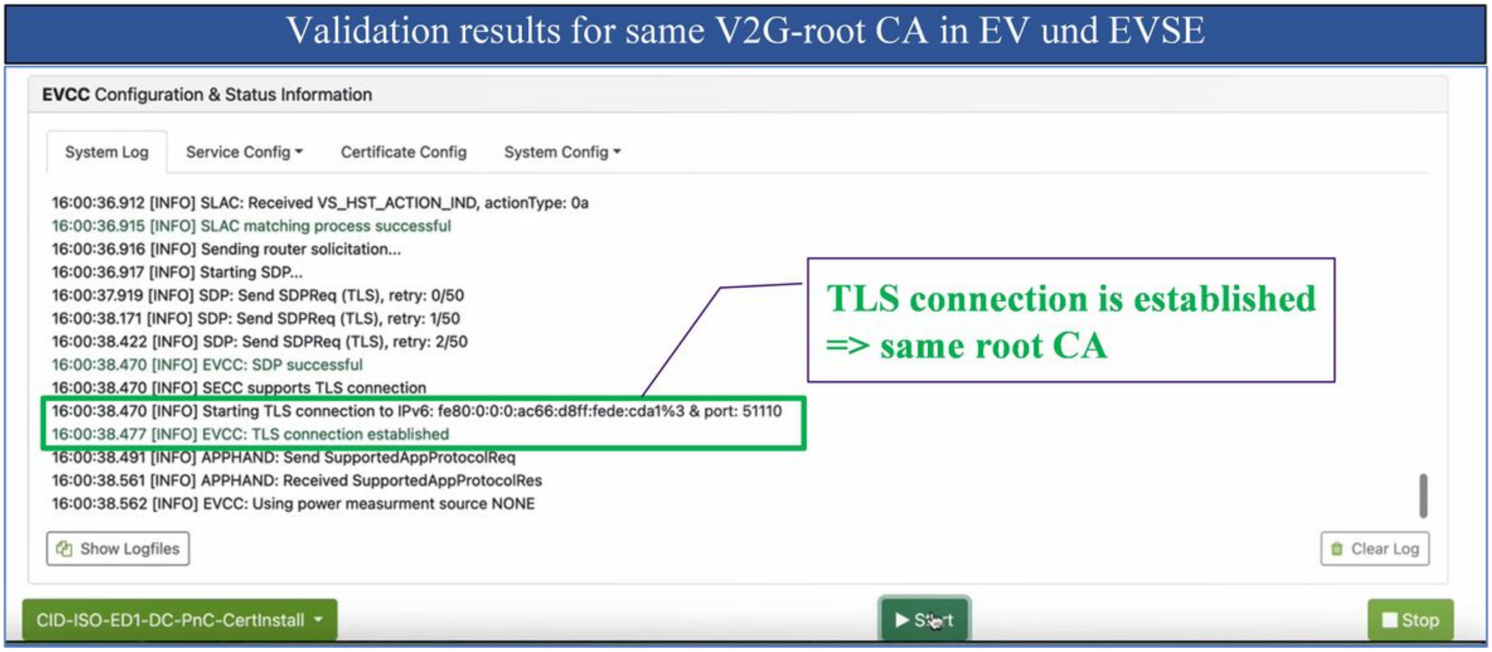
Figure 11

Validation of different PKIs between EV and EVSE influences on TLS function (scenario 2)



Solution C: Overview for same V2G-root CA in EV und EVSE

Solution C: Cross certificate recognition- install multiple V2G in EV



Validation results for same V2G-root CA in EV und EVSE

EVCC Configuration & Status Information

```
16:00:36.912 [INFO] SLAC: Received VS_HST_ACTION_IND, actionType: 0a
16:00:36.915 [INFO] SLAC matching process successful
16:00:36.916 [INFO] Sending router solicitation...
16:00:36.917 [INFO] Starting SDP...
16:00:37.919 [INFO] SDP: Send SDPReq (TLS), retry: 0/50
16:00:38.171 [INFO] SDP: Send SDPReq (TLS), retry: 1/50
16:00:38.422 [INFO] SDP: Send SDPReq (TLS), retry: 2/50
16:00:38.470 [INFO] EVCC: SDP successful
16:00:38.470 [INFO] SECC supports TLS connection
16:00:38.470 [INFO] Starting TLS connection to IPv6: fe80:0:0:0:ac66:d8ff:fede:cda1%3 & port: 51110
16:00:38.477 [INFO] EVCC: TLS connection established
16:00:38.491 [INFO] APPHAND: Send SupportedAppProtocolReq
16:00:38.561 [INFO] APPHAND: Received SupportedAppProtocolRes
16:00:38.562 [INFO] EVCC: Using power measurment source NONE
```

TLS connection is established
=> same root CA

Figure 12

Successful validation of certificates for TLS function (without interoperable PKI)