Position Paper of Charging Interface Initiative e.V.

CP for ISO 15118 V2G PKI

2020-08-06

Coordination Office

CharIN e. V.

c/o innos GmbH
Kurfürstendamm 11
10719 Berlin

Contact

André Kaufung

Phone: +49.30.288 8388-0
Fax: +49.30.288 8388-19
Mail: coordination@charinev.org
Web: www.charinev.org

Contents

Preface

The document shall serve as a basis for a guideline for the secure operation of an ISO 15118 V2G Public Key Infrastructure. The content contained in the present version V1.2 is based on existing best practice examples.

Structure

This document is structured following the RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework[1]

Intended Audience

Members of an ISO 15118 V2G PKI

History

Version	Author	Comment	Date
0.1	A. Ziska / secunet AG	Initial version	03.01.2020
0.2	A. Ziska / secunet AG E. Lafargue (Tesla)	Changes after the Task Force Telco from 15.01.2020 Comments and changes in chapter 7	15.01.2020
0.3	A. Ziska / secunet AG	Several changes after F2F meeting at the 12.02.2020 and the telephone confenrence at the 26.02.2020	02.03.2020
0.4	A. Ziska / secunet AG	Changes according to commenting sheet of 2020-03-09	09.03.2020
0.5	A. Ziska / secunet AG	Changes according to commenting sheet of 2020-03-23	30.03.2020
0.6	A. Ziska / secunet AG	Changes according to commenting sheet of 2020-04-01	08.04.2020
0.7	A. Ziska / secunet AG	Changes according to commenting sheet of 2020-05-06	15.05.2020
0.8	A. Ziska / secunet AG	Changes according to commenting sheet of 2020-06-03	10.06.2020
1.0	A. Ziska / secunet AG	Changes according to commenting sheet of 2020-06-24	30.06.2020
1.1	A. Ziska / secunet AG	Changes according to comment-	30.07.2020

[1] https://tools.ietf.org/html/rfc3647

		ing sheet of 2020-06-28	
1.2	A. Ziska / secunet AG	Changes according to Comment-ing_Sheet_CPv1.1.xlsx Several minor editorial changes	06.08.2020

1 Introduction

This document is the Certificate Policy (CP) for an ISO 15118 V2G PKI provided by the CharIN Taskforce PKI. It describes the PKI participants, the data formats and processes for the operation of the PKI.

Information about interoperability and governance and market rules will be described in future documents.

1.1 Overview

This document, “Certificate Policy (CP) ISO 15118 V2G PKI is the CharIN policy guideline for certificate services used within a PKI applied to ISO 15118-2 use cases. It will be revised for new editions of the ISO15118.

The CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital certificates within the PKI and providing associated trust services for all participants within the PKI. These requirements protect the security and integrity of the PKI and comprise a single set of rules that apply consistently PKI - wide, thereby providing assurances of uniform trust throughout the PKI.

The CP is not a legal agreement between participants of the PKI.

This document is targeted at:

- PKI Operators inside the Plug&Charge system landscape to enable ISO 15118-2 use cases.

The CP does not govern any services outside an ISO 15118 V2G PKI.

This CP conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. To retain the outline structure specified by RFC 3647, some sections will have the statement "Not applicable" or "No stipulation."

Within this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119.

1.2 Document name and identification

This document is the Certificate Policy (CP) for an ISO 15118 V2G PKI. This CP becomes effective the day when it is published. It remains valid until it is replaced by a new version.

This CP is identified by the following information:

- Name: Certificate Policy (CP) for an ISO 15118 V2G PKI
- OID: No OID needed

1.3 PKI participants

1.3.1 Certification authorities

A Certification Authority (CA) is system for issuing public key certificates within a PKI. The ISO 15118 V2G PKI describes various top-level Root CAs and subordinate Sub-CA1- and Sub-CA2 in accordance with [ISO 15118-2], as depicted in Figure 1 - Overview certificate structure, according to Annex E of ISO 15118 -2 below.

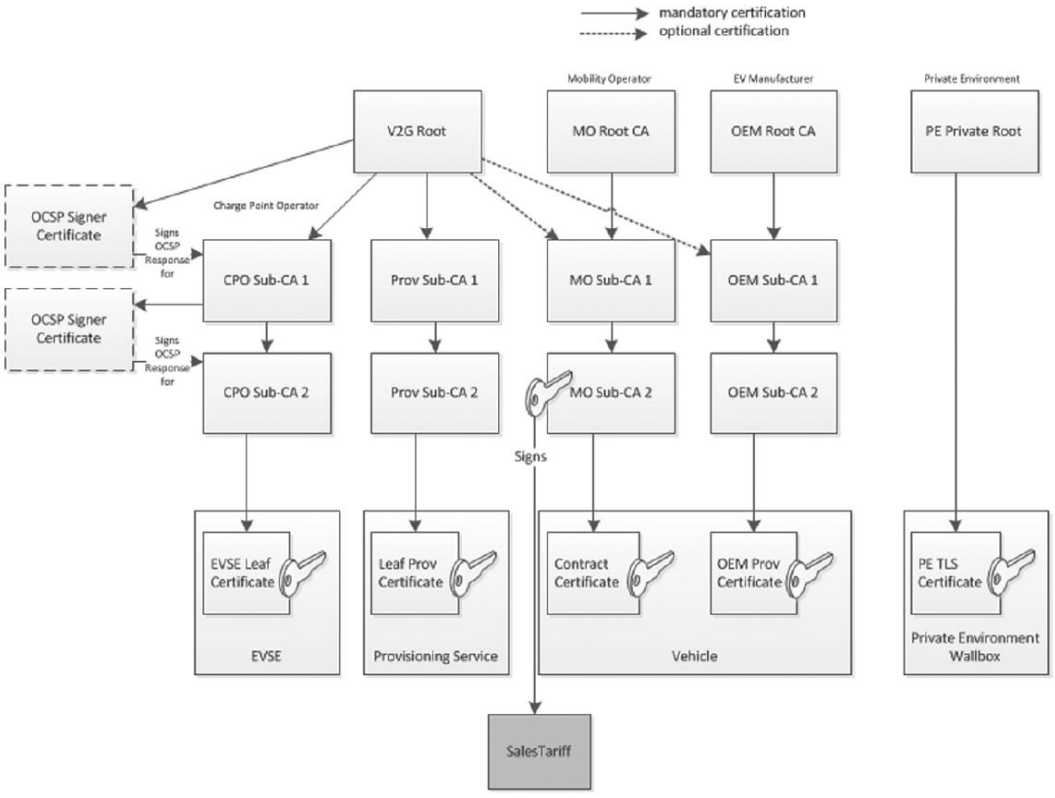

Figure 1 – Overview certificate structure, according to Annex E of ISO 15118 -2

The following types of CAs are entitled in the PKI to issue different kinds of certificates:

- V2G Root CA: This is the top-most CA of the public ISO 15118 V2G PKI
- V2G Root OCSP Signer Authority: The V2G Root CA may optionally delegate the task of signing OCSP responses on its behalf to an OCSP signer authority, if technically necessary (e.g. if the V2G Root CA is operated offline.)
- MO Root CA: The MO Root CA issues Contract Certificates. A MO Root CA may be operated by a Mobility Operator or another service provider and might not be part of the public ISO 15118 V2G PKI.
- MO Sub-CA1 and Sub-CA2: These CAs are certified by the MO Root CA. The MO Sub-CA2, unlike other CAs within the ISO 15118 V2G PKI, signs not only certificates but also the sales tariffs.
- OEM Root CA: The OEM Root CA issues OEM provisioning certificates. An OEM Root CA may be operated by an OEM or another service provider and might not be part of the public ISO 15118 V2G PKI.
- CPO Sub-CA1 and Sub-CA2: These Sub-CAs are certified by the V2G Root CA and are part of the ISO 15118 V2G PKI. This type of Sub-CA issues Sub-CA2 - EVSE certificates.
- CPO OCSP Signer Authority: The CPO OCSP signer authority may optionally sign OCSP responses on behalf the CPO Sub-CA1.
- Provisioning Sub-CA1- and Sub-CA2: These Sub-CAs are certified by the V2G Root CA and are part of the ISO 15118 V2G PKI. The V2G Root CA issues leaf provisioning certificates.
- [MO/OEM] Root OCSP Signer Authority: The [MO/OEM] Root OCSP signer authority may optionally sign OCSP responses on behalf the [MO/OEM] Root CA."

Multiple V2G Root CAs, MO Root CAs, OEM Root CAs, OCSP signer authorities operated by various PKI Operators can exist.

Issuing of certificates is done by independent CAs resp. PKI Operators

CAs will be operated by PKI operators. These are also referred as PKI service providers.

1.3.2 Registration Authorities

The RA responsibilities include, but are not limited to:

- Providing infrastructure and processes for receiving certificate requests from applicants.
- Identifying and authenticating certificate applicants.
- Accepting or rejecting certificate applications.
- Forward certificate requests to the corresponding CA
- Receive certificate from issuing CA
- Sending issued certificate to requester, directory service or another certificate pool.

Each CA inside the ISO 15118 V2G PKI must operate its own RA. The registration process for issuing certificates is in the sole responsibility of the issuing CA. The registration process must assure that only authenticated requests will result in issued certificates

1.3.3 Subscribers

Three different terms are used in this CP.

1.3.3.1 Subscriber

The **subscriber** is the entity which contracts with the ISO 15118 V2G PKI for the issuance certificates. The subscriber holds the organizational and technical responsibilities.

1.3.3.2 Subject

On the contrary to the subscriber is the **subject** the entity to whom the issued certificate is bound and which is authenticated when the certificate is presented.

1.3.3.3 Authorized Intermediary

An authenticated and authorized intermediary could request re-key for a subscriber

1.3.4 Relying parties

Relying parties are all individuals, devices or organizations that use certificates issued by the ISO 15118 V2G PKI for

- authenticating subjects of the ISO 15118 V2G PKI,
- confirming that a message is signed by a legitimate participant of the ISO 15118 V2G PKI,

- encrypting and decrypting messages.

and reasonably rely on such certificates in accordance with the requirements of this CP.

1.3.5 Other participants

None

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

Certificates issued within the ISO 15118 V2G PKI are intended to be used in conjunction with ISO 15118-2 context only.

1.4.2 Prohibited certificate uses

Certificates issued by a member of the ISO 15118 V2G PKI must be used for services inside the ISO 15118-2 use cases.

Certificates issued by a participant of the ISO 15118 V2G PKI are not intended and authorized for use in

- circumstances that offend, breach, or contravene any applicable law, regulation, decree or governmental order,
- circumstances that breach, contravene, or infringe the rights of others,
- breach of this CP or the relevant subscriber agreement.

1.5 Policy administration

1.5.1 Organization administering the document

This document is administered by CharIN. The organization can be contacted as stated in section 1.5.2

1.5.2 Contact person

Questions regarding this CP should be addressed to the following address:

André Kaufung, coordination@charinev.org, Phone: +49302888388-0, Fax: +49.30.288 8388-19, website: www.charinev.org

1.5.3 Person determining CPS suitability for the policy

CharIN is responsible for determining the suitability of this CP and other documents that supplement or are subordinate to this CP.

1.5.4 CPS approval procedures

See 3.2.6.

1.6 Definitions and acronyms

See the glossary at the end of the document.

2 Publications and repository responsibilities

2.1 Repositories

All Root CAs in the ISO 15118 V2G PKI provide Relying Parties with information on how to find the appropriate repository to check Certificate status and how to find the right OCSP responder.

The OEM must update the Directory Service(s) to indicate where its OEM EV Provisioning Certificates can be found.

The MO must update the Directory Service(s) to indicate where contract certificates can be found.

All MO contract certificates must be accessible to CPOs

Terms for accessing the repositories must be fair, reasonable and non-discriminatory.

2.2 Publication of certification information

CAs inside the ISO 15118 V2G PKI must publish the following information:

- Issued CA certificates in the repositories named in section 2.1,
- Certificate Revocation List for all revoked certificates,
- Online Certificate Status Information via OCSP,
- Information how and where to revoke a certificate,
- All revocation information must be publicly available without restrictions,
- A link to the appropriate CP. This CP must be publicly available without restrictions,
- The publication of the CPS is left to each Root CAs judgment,
- The Root CA certificate and its fingerprint,
- The Sub-CA certificate and its fingerprint.

The OEMs shall contribute their OEM EV Provisioning Certificates to one or more OEM Provisioning certificate pools

2.3 Time or frequency of publication

CAs inside the ISO 15118 V2G PKI must offer CRLs showing all revoked certificates through the repositories and must offer status checking services.

The CRL validity must not exceed 14 days

A new CRL must be issued at least weekly or immediately after revocation of a certificate.

2.4 Access control on repositories

The information published in the repositories by the PKI Operator must be publicly accessible for all participants of the ISO 15118-2 use cases.

Read only access to such information must be unrestricted for all participants of the ISO 15118-2 use cases

It must be ensured that only the Root CAs and subordinate CAs are the only authorized entities that have write access to repositories. Access controls, logical and physical security measures, must be implemented to prevent unauthorized persons from adding, deleting, or modifying the published information.

The MO contract certificates must be accessible to all CPOs and OEMs.

To improve response time and extend coverage, the MO can contribute their Contract Certificate to one or more “Central Pools”.

The CCCP must be accessible to all CPOs. Terms of access for CPOs must be fair, reasonable and non–discriminatory.

The OEM Provisioning Certificates must be accessible to all MOs.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

Inside the ISO 15118 V2G PKI, a consistent hierarchy for naming must be used. All issued certificates comprise distinguish names (DN) according to [RFC 5280]. Each participant in the ISO 15118 V2G PKI must be uniquely identified through the DN.

- C= <Country/Country Code, i.e. DE>,
- O=<Organization>,
- [OU=<Organizational Unit>,]
- CN=<Common Name>.

Attributes in angle brackets must be replaced by the respective values. Attributes in square brackets are optional. The attribute order is fixed and must not be changed.

Only the attribute “OU” can be added more than once.

The attribute “O” contains the name of the organization that the certificate holder is related.

Each issuing subordinate CA must declare a unique subject namespace towards the superordinate V2G Root CA. The issuing subordinate CAs must not use subject DNs outside the stipulated namespace.

The uniqueness of subject DNs is in the sole responsibility of the issuing CA. The subject DNs has a limit of 64 characters.

3.1.2 Need for names to be meaningful

End-entity subscriber (leaf) certificates shall include meaningful names in the following sense: end-entity subscriber certificates shall contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the subject of the certificate.

Contract Certificates and SECC certificates shall include Subject names which meet the requirements for the name forms specified in Annex F of [ISO 15118-2].

Wildcard and SAN certificates (e.g. *.cpoprovider.de) must not be used.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

No stipulation

3.1.5 Uniqueness of names

According to the obligation of 3.1.1 Sub-CAs must use a unique subject DN namespace and to assign unique subject DNs, the subject DN are unique within the ISO 15118 V2G PKI.

3.1.6 Recognition, authentication and role of trademarks

No stipulation

3.2 Initial identity validation

Identification processes

3.2.1 Method to prove possession of private key

The certificate applicant for a Sub-CA or end-entity certificate must demonstrate that he rightfully holds the private key corresponding to the public key to be listed in the certificate.

The method to prove possession of a private key should be a PKCS#10 Certificate Request. The PKCS#10 Certificate Request must be submitted by the applicant in a secure manner. The issuing CA must verify that the applicant's digital signature on the PKCS#10 was created by the private key corresponding to the public key in the PKCS#10 Certificate Request. If any doubt exists, the CA must reject the certification of the key.

3.2.2 Authentication of organization identity

Whenever a CA certificate contains an organization name, the identity of the organization and other enrolment information provided by the certificate applicant must be validated.

At least it must be verified that the application organization exists by using a third-party identity proofing service or trade mark registration organization. A second way of verifying this, e.g. over the phone, must be carried out.

If available, any kind of a corresponding official registry that is provided at national or international level must be consulted

3.2.3 Authentication of individual identity

No stipulation

3.2.4 Non-verified subscriber information

No stipulation

3.2.5 Validation of authority

No stipulation

3.2.6 Criteria for interoperation

3.2.6.1 Approval of subordinate CA's

If a new subordinate CA is to be introduced as part of the ISO 15118 V2G PKI, it must be verified by the Root CA. This applies to subordinate CAs of the same PKI operator, as well as subordinate CAs of another company or PKI operator.

The Root CA must check if the Certification Practice Statement of the new subordinate CA complies with the CP of the ISO 15118 V2G PKI. A responsible operator of the new subordinate CA must be identified and registered at the Root CA.

The approval procedure includes an audit for any subordinated CA before joining the PKI. The audit includes a Sub CAs Certification Practice Statement review and an on-site inspection.

Audit documentation, forms and approval document must be archived by the Root CA.

No need for additional approval if the PKI Operator in question is still operating an approved Sub CA inside the ISO 15118 V2G PKI which operates under the same Certification Practice Statement as the new Sub CA

3.2.6.2 Approval of PKI operators

PKI operators for an ISO 15118 V2G PKI that meet the requirements described in this CP can claim the status "Approved by CharIN" after an appropriate audit. The CP of the relevant ISO 15118 V2G PKI and all Certificate Practice Statement documents must be checked against the requirements of this CP.

The approval procedure includes an audit for the Root and any involved subordinated CA. The audit includes an on-site inspection.

Audit documentation, forms and approval document must be archived by the Root CA.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Prior to the expiration of an existing certificate, it is necessary for the subscriber to obtain a new certificate to maintain seamless operation. The subscriber must generate a new key pair to replace the expiring key pair (technically defined as “re-keying”).

Certificate renewal, without re-keying is not permitted in the ISO 15118 V2G PKI.[2]

3.3.2 Identification and authentication for re-key after revocation

Certificate re-keying for Sub-CAs and CA-related devices like OCSP and/or CRL signer are handled the same way as a new certificate request.

The identification and authentication for the re-key process must assure that only authenticated requests must result in issued certificates.

3.4 Identification and authentication for revocation request

A request to revoke a leaf certificate must be authenticated by the issuing CA to ensure that the revocation has in fact been requested by or in the name of the subject.

Acceptable procedures for authenticating the revocation requests are

- S/MIME signed email,

[2] Generally speaking, both “rekey” and “renewal” are commonly described as “Certificate Renewal”, focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated.

- written and signed corporate letter,
- API with mutual TLS authentication.

4 Certificate life-cycle operational requirements

4.1 Certificate application

The term certificate application refers to the following processes:

- Initial registration for a certificate,
- Application for a certificate,
- Re-key for a certificate.

4.1.1 Who can submit a certificate application

List of entities who may submit certificate applications:

- Any authorized representative of the appropriate Sub-CA,
- Any registered subscriber or any authenticated and authorized intermediary for end-entity certificates.

4.1.2 Enrolment process and responsibilities

See 3.2.6.1

The process for issuing end-entity certificates is in the sole responsibility of the issuing Sub-CA. The registration process must assure that only authenticated requests will result in issued certificates

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Application for certifications of Sub CAs must to be addressed to the responsible person at the superordinate CA. Subscribers of Sub CA certificates enter into a contractual relationship with the superordinate CA that will issue the Sub CA certificate.

Applicants must provide their credentials to demonstrate their identity and provide contact information during the contracting process. The superordinate CA must check the submitted identity information. The inspection results must be documented and archived.

The process for identification and authentication must assure that only authenticated requests will result in issued certificates.

4.2.2 Approval or rejection of certificate applications

The superordinate CA must approve an application for a Sub CA certificate if the requirements for identification and authentication of all required subscriber information are met. Furthermore the audit trail has been finished successfully as payment (if applicable) has been received.

The certificate application must be rejected by the superordinate CA if identification or authentication of all required subscriber information cannot be completed or the audit trail finished unsuccessfully or payment (if applicable) has not been received

The approval process must assure that only authenticated requests will result in issued certificates. (See 3.2)

4.2.3 Time to Process Certificate Applications

Issuing CAs must begin processing certificate applications within a reasonable time of receipt.

A certificate application should remain active until rejected or processed.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Following the approval of a certificate application the certificate must be created and issued by the CA. The certificate must be made available to the applicant. All CA actions must be logged and archived.

4.3.2 Notification to subscriber by the CA of issuance of certificates

CAs shall notify the respective subscribers about issued certificates and provide subscribers with access to the certificates by notifying them about the availability of and the means for obtaining the certificates.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Installing and using a certificate must constitute the subscriber's acceptance of the certificate.

4.4.2 Publication of the certificate by the CA

CAs inside the ISO 15118 V2G PKI must publish the certificates they issue in a repository. All CA certificates must be publicly available without restrictions and all leaf certificates must be available on request.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The regulations of section 1.4 apply.

4.5.2 Relying party public key and certificate usage

Before a relying party uses a certificate issued by the ISO 15118 V2G PKI covered by this CP the validity of certificate chain has to be checked.

Reference [5] describes how the contract certificate pool should check the revocation status of contract certificates

4.6 Certificate renewal

Certificate renewal is the issuance of a new certificate to the subject without changing the key pair.

Certificate renewal must not be applied in the ISO 15118 V2G PKI, neither for Sub CA certificates nor for end-entity certificates.

4.6.1 Circumstance for certificate renewal

Not applicable, see above.

4.6.2 Who may request renewal

Not applicable, see above.

4.6.3 Processing certificate renewal requests

Not applicable, see above.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable, see above.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable, see above.

4.6.6 Publication of the renewal certificate by the CA

Not applicable, see above.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable, see above.

4.7 Certificate re-key

Certificate re-key is the application for the issuance of a new certificate that certifies a new public key. CA certificate re-key is handled as a new certificate application.

Certificate re-key must only be carried out within the scope of the certificate life cycle or a security incident.

It must be assured, that only authenticated requests will result in issued certificates.

4.7.1 Circumstance for certificate re-key

Prior to the expiration of an existing subscriber's certificate, it is necessary for the subscriber to re-key the certificate to maintain continuity of certificate usage.

A certificate may also be re-keyed after expiration. In this case, special processes may be implemented to verify the identity, authentication and authorization of the re-key request.

4.7.2 Who may request certification of a new public key

Only the subscriber for a certificate or an authenticated and authorized intermediary may request certificate re-key.

4.7.3 Processing certificate re-keying requests

The certificate re-key process for Sub-CAs must be handled as a new certificate request.

It has to be assured, that only authenticated and authorized requests will result in issued certificates.

4.7.4 Notification of new certificate issuance to subscriber

See 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Using a certificate constitutes the subscriber's acceptance of the certificate.

4.7.6 Publication of the re-keyed certificate by the CA

See 4.4.2

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation

4.8 Certificate modification

Certificate modification must not be used in the ISO 15118 V2G PKI.

4.8.1 Circumstance for certificate modification

Not applicable, see above.

4.8.2 Who may request certificate modification

Not applicable, see above.

4.8.3 Processing certificate modification requests

Not applicable, see above.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable, see above.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable, see above.

4.8.6 Publication of the modified certificate by the CA

Not applicable, see above.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable, see above.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Only in the circumstances listed below, will a Sub-CA1- or Sub-CA2 certificate be revoked by the issuing CA.

- Compromise of the Sub-CA's private key.
- The Sub-CA certificate was issued in a manner not in accordance with the stipulations of this CP.

- The continued use of the Sub-CA certificate is harmful to the ISO 15118 V2G PKI e.g. if invalid or unauthorized certificates were issued.

Revoking a SubCA-certificate is recommended in one of the following cases:

- the organization name in the certificate changes,
- other information in the certificate are incorrect or
- other information in the certificate are changed

Revocation of end-entity subscriber certificates is in the sole responsibility of the issuing Sub-CA. It has to be assured, that only authenticated and authorized requests will result in revoked certificates. Revoked certificates must be listed in CRLs and/or OCSP directories.

Revocation of certificates must only take place within the scope of a security incident.

4.9.2 Who may request revocation

The below listed parties may revoke the specified certificate.

4.9.2.1 Revocation of ISO 15118 PKI V2G Root CA:

Only the ISO 15118 V2G PKI Operator is entitled to process the revocation of the V2G Root CA certificate, but every ISO 15118 V2G PKI participant may initiate a request for revocation.

4.9.2.2 Revocation of Sub-CA's

Sub-CAs are entitled, through their authorized representatives, to request the revocation of their own certificates at the superordinate CA, but only the ISO 15118 V2G PKI operator is entitled to process the authorization.

4.9.2.3 Revocation of contract certificates

As a special requirement for Contract Certificates, [VDE-AR v2017 or 2019 if English version is available], Section 10, §7 requires that MOs should provide a B2C interface for consumer to change or cancel their subscription, which will lead in revoking their own Contract Certificate. Accordingly, MO Sub-CA2 must provide a user interface or an API to other consumer-facing systems for revocation.

The MO operator may revoke a Contract Certificate, e.g. in case of cancellation of the consumer contract

4.9.2.4 Revocation of provisioning certificates

Only the ISO 15118 V2G PKI operator is entitled to process the revocation of a provisioning certificate, but every ISO 15118 V2G PKI participant may initiate a request for revocation of provisioning certificates.

4.9.2.5 Revocation of EVSE certificates

Only the CPO shall process the revocation of an end-entity certificate, but every ISO 15118 V2G PKI participant may initiate a request for revocation of the EVSE leaf certificate.

4.9.2.6 Revocation of OEM provisioning certificates

Only the OEM shall process the revocation of an end-entity certificate, but every ISO 15118 V2G PKI participant may initiate a request for revocation of the OEM provisioning certificate.

OEM Root CAs are out-of-scope.

4.9.2.7 Revocation of MO certificates

The MO must be able to revoke its own certificate, and every other party can request the revocation.

MO Root CAs are out-of-scope.

Revocation of end-entity subscriber certificates is in the sole responsibility of the issuing Sub-CA. It has to be assured, that only authenticated and authorized requests will result in revoked certificates.

4.9.3 Procedure for revocation request

Prior to the revocation of a certificate, the issuing CA must verify that the revocation has been requested by the certificate's subscriber according to Section 4.9.2.

CA certificates must only be revoked as a result of a security incident on the basis of the regulations of the Incident Management processes. Any revocation of a CA certificate must be confirmed by a Risk Commission.

4.9.4 Revocation request grace period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

The maximum time for processing must be defined in the CPS of the ISO 15118 V2G PKI Operator.

4.9.5 Time within which CA must process the revocation request

The revocation requests must be processed within a commercially reasonable time as possibly defined in the security risk analysis and IT supplier Policy or the Service Level Agreements of the CAs.

The maximum time for processing must be defined in the CPS of the ISO 15118 V2G PKI Operator.

4.9.6 Revocation checking requirement for relying parties

According to requirements [4] and [5], the EVCC should verify the certificate chain of the SECC, including certificate status check via OCSP service.

Certificate status validation is not required by [4] for other relying parties and respectively for other certificate types in the ISO 15118 V2G PKI.

According to [5], Chapter 11 §11.3.4, the contract certificate pool must verify the revocation status of all certificates that are involved in the provisioning of a new contract certificate. This includes the certificate chains of the MO, OEM, and CProvS.

Other relying parties should check the status of certificates which they rely on.

4.9.7 CRL issuance frequency

In accordance with [VDE-AR], Section 10, §3, if a certificate listed in a CRL expires, it must be removed from CRLs after the certificate's expiration.

- CRL of the V2G Root CA: max. 1 year and upon any revocation,
- CRL of CPO Sub-CA1: max. 4 weeks and upon any revocation,
- Every 7 days a new one must be published.

4.9.8 Maximum latency for CRLs

CRLs must be published immediately after their generation. The maximum time for processing must be defined in the CPS of the ISO 15118 V2G PKI Operator.

In accordance with [5], Section 10, §3, if a certificate listed in a CRL expires, it must be removed from CRLs after the certificate's expiration.

4.9.9 On-line revocation/status checking availability

In accordance with ISO 15118-2 the Root CA, CPO Sub-CA1-, and Sub-CA2 must provide an OCSP service. For other CAs of the ISO 15118 V2G PKI, providing an OCSP service is optional.

4.9.10 On-line revocation checking requirements

The EVCC must verify the certificate chain of the SECC if applicable.

According to requirement [V2G2-875] in [4], the EVCC must verify the certificate chain of the SECC (including OCSP Signer certificates) including certificate status check via OCSP service. The SECC must provide all necessary OCSP responses in the TLS initialization response by means of OCSP stapling according to [RFC6961].

According to [V2G2-649] of [4], the SECC should update (and cache) the OCSP response at least once a week. One solution for updating might be for example an online connection.

4.9.11 Other forms of revocation advertisements available

No stipulation

4.9.12 Special requirements regarding key compromise

ISO 15118 V2G PKI participants must be notified of an actual or suspected CA private key compromise. The responsible parties at the subsequent CAs must be notified within two working days starting from the day at which key compromise was detected.

4.9.13 Circumstances for suspension

ISO 15118 V2G PKI must not support suspension services for issued certificates. The revocation of a certificate is irreversible

4.9.14 Who can request suspension

Not applicable, see above.

4.9.15 Procedure for suspension request

Not applicable, see above.

4.9.16 Limits on suspension period

Not applicable, see above.

4.10 Certificate status service

To enable all parties to validate certificates from all ISO 15118 V2G PKI s, all parties providing certificates, should provide access to Certificate Revocation Lists and OCSP services accompanying these certificates, without any restrictions and free of charge.

4.10.1 Operational characteristics

The status of issued certificates must be publicly available via CRL, through a web-based repository and via an OCSP responder

4.10.2 Service availability

Certificate status services must be available 24x7 without scheduled interruption. A Service Level Agreement must be agreed between the business parties.

4.10.3 Optional features

No stipulation

4.11 End of subscription

A subscriber may end a subscription for a certificate by:

- Allowing the certificate to expire without re-keying that certificate,
- Revoking of certificate before certificate expiration without replacing the certificates.

4.12 Key escrow and recovery

Key escrow and recovery is not permitted for the ISO 15118 V2G PKI.

4.12.1 Key escrow and recovery policy and practices

Not applicable, see above.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable, see above.

5 Physical, procedural and personnel security controls

5.1 Physical controls

CAs of the ISO 15118 V2G PKI must implement physical security controls.

For requirements about procedural and personnel security see sections 5.2 and 5.3.

5.1.1 Site location and construction

All IT components for a CA of the ISO 15118 V2G PKI must be operated within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

5.1.2 Physical access

Access to CA premises of physical security must be auditable and controlled in a way that it can be accessed by authorized personnel only.

5.1.3 Power and air conditioning

The secure facilities of CAs of the ISO 15118 V2G PKI must be equipped with reliable access to electric power and internet connectivity. These secure facilities must be equipped with heating, ventilation and/or air conditioning systems to control temperature and relative humidity.

5.1.4 Water exposures

The secure facilities of CAs of the ISO 15118 V2G PKI must be protected against water exposure. For this reason, water and soil pipes are to be avoided.

5.1.5 Fire prevention and protection

The secure facilities of CAs of the ISO 15118 V2G PKI must be constructed and equipped, and procedures shall be implemented, to prevent damaging exposure to flame or smoke.

5.1.6 Media storage

CAs of the ISO 15118 V2G PKI must protect the storage media holding backups of critical system data or any other sensitive information from environmental hazards and unauthorized use of, access to, or disclosure of such media.

5.1.7 Waste disposal

CAs of the ISO 15118 V2G PKI must implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing confidential and private information.

5.1.8 Off-site backup

CAs of the ISO 15118 V2G PKI must perform regular backups of critical system data, audit log data, and other sensitive information. In case of complete loss of data, the data must be completely recovered from the backup data. Off-site backup locations must offer at least the same level of security as the main location. Only view-people can read the backup in case of an emergency situation.

5.2 Procedural controls

5.2.1 Trusted roles

Employees, contractors, and consultants that are designated to manage infrastructural trustworthiness shall be considered to be “Trusted Roles”. Persons seeking to become Trusted Role by obtaining a Trusted Position must meet the screening requirements of the CP.

Trusted Roles include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications,
- the acceptance, rejection, or other processing of certificate applications, revocation requests, re-key requests,
- the issuance or revocation of certificates, including personnel having access to restricted portions of its repository or the handling of subscriber information or requests.

Trusted Roles include, but are not limited to:

- Security Officer,

- Certificate Manager,
- Registration Authority Officer,
- Customer service personnel,
- Log Auditor,
- System administration personnel,
- designated engineering personnel, and
- Executives that are designated to manage infrastructural trustworthiness.

5.2.2 Number of persons required per task

The ISO 15118 V2G PKI operator must establish, maintain, and enforce rigorous control procedures to ensure the separation of duties based on job responsibility and to ensure that multiple persons of the required Trust Role are required to perform sensitive tasks.

Policy and control procedures must be in place to ensure separation of duties based on job responsibilities. The most sensitive tasks, like the access to and management of CA cryptographic Hardware Security Module (HSM) and associated key material require multiple persons of the required Trust Role.

These internal control procedures must be designed to ensure that at a minimum of two persons of the resp. Trusted Role are required to have either physical or logical access to the device, which also shall be protected against job rotation.

5.2.3 Identification and authentication for each role

CAs and RAs must confirm the identification and authorization of all personnel seeking to become Trusted Role before such personnel is on duty.

Roles requiring separation of duties include (but are not limited to)

- the acceptance, rejection, revocation requests or other processing of CA certificate applications,
- the generation or destruction of a private CA key,
- the activation of a private CA key,
- the generation, issuing or revocation of a CA certificate.

5.3 Personnel controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Proof of the requisite background (see 5.3.2), qualifications and experience

The gathered information must be documented and archived

5.3.2 Background Check Procedures

Background verification and competence checks on all candidates for employment must be carried out. These must be carried out in accordance with the relevant laws, regulations and ethics, and should be proportional to the business requirements, the classification of the information that will be accessed and the perceived risks associated. The screening should also take place for contractors.

5.3.3 Training Requirements

The persons assigned to trusted roles must receive training appropriate to the tasks assigned to them.

5.3.4 Retraining frequency and requirements

The persons assigned to trusted roles are required to continuously refresh their knowledge using a training environment provided by the CA operator.

5.3.5 Job rotation frequency and sequence

No stipulation

5.3.6 Sanctions for unauthorized actions

No stipulation

5.3.7 Independent Contractor Requirements

No stipulation

5.3.8 Documentation Supplied to Personnel

No stipulation

5.4 Audit logging procedures

The types of auditable events that must be recorded by CAs and RAs of the ISO 15118 V2G PKI, whether electronic or manual, shall contain the date and time of the event, and the identity of the entity that caused the event. Audit logs must be stored in a way that prevents unnoticed and undiscovered deletion and modification, up to the End-of-Life +5 years of the CA-Lifetime.

CAs of the ISO 15118 V2G PKI must state in their Certificate Practice Statement the logs and types of events they record.

5.4.1 Types of events recorded

Every CA of the ISO 15118 V2G PKI operator must keep several kinds of audit logs include, but are not limited to:

- All relevant information that is created during processing requests to the CA. This includes received requests as well as issued certificates and information about errors during processing of a request.
- Internal information about the CA operations. Data, checklists, forms, etc.
- Audit reports

5.4.2 Frequency of processing log

- Audit logs shall be reviewed automatically or manually in response to the varying degrees of alerts based on irregularities and incidents within their CA systems.
- Audit log processing must consist of a review of the audit logs and documenting the reason for all unexpected events in an audit log summary.
- Audit log reviews must include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the audit logs.
- Audit log must be archived at least weekly. An administrator / security officer must assure that the system have enough resources to operate in a reliable way.

5.4.3 Retention period for audit log

Log records related to certificate life cycles must be kept at least two years after the corresponding certificate expires.

Any local legal regulations where the CA is located may require a longer period of archival.

5.4.4 Protection of audit log

No stipulation

5.4.5 Audit log backup procedures

No stipulation

5.4.6 Audit collection system (internal or external)

No stipulation

5.4.7 Notification to event-causing subject

No stipulation

5.4.8 Vulnerability assessment

An vulnerability assessment of all IT equipment of the CAs of the ISO 15118 V2G PKI must be performed frequently (at least once a week) by technical means

From an organizational point of view, vulnerability assessment must be performed permanently by intellectual means. A deeper analysis must be conducted every 12 months. The result must be documented und archived.

5.5 Records archival

5.5.1 Types of records archived

CAs and RAs of the ISO 15118 V2G PKI must archive:

- All audit data collected in terms of section 5.4.1.
- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information e.g., creation, revocation, rekey and renewal application information

Audit log must be archived regularly as described in section 5.4.3.

5.5.2 Retention period for archive

No stipulation

5.5.3 Protection of archive

CAs of the ISO 15118 V2G PKI operator maintaining an archive of records must protect the archive in a way, that only the entity's authorized Trusted Roles are able to obtain access to the archive.

The archive must be protected against unauthorized viewing, modification, deletion, or other tampering.

5.5.4 Archive backup procedures

No stipulation

5.5.5 Requirements for time-stamping of records

No stipulation

5.5.6 Archive collection system (internal or external)

No stipulation

5.5.7 Procedures to obtain and verify archive information

No stipulation

5.6 Key changeover

When the certificate of a CA is about to expire, a new key pair must be created and a new CA certificate must generated. This process must be handled as a new certification application.

The validity periods of the old and the new certificate should overlap such that every certificate issued by the CA can be verified with a valid CA certificate during its complete validity period

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling

If an incident is detected or the CA system is compromised, the responsible authority and Trusted Roles within ISO 15118 V2G PKI operator's organisation have to be informed immediately. It must be decided whether the incident is severe enough to stop operations for the affected CA. Furthermore, a notification about the compromise must be published over the channels specified in section 2.1.

The affected CA may continue operation, only if the reasons for the incident or compromise have been thoroughly investigated, and it can be estimated that such a compromise will not be able to happen again.

5.7.2 Computing resources, software and/or data are corrupted

If a disaster is discovered that prevents the proper operation of a CA, the CA operation must be stopped and it must be investigated whether also the private key has been compromised.

If compromise cannot be ruled out, the procedures of section 5.7.3 must be applied.

Otherwise, defective hardware must be replaced as fast as possible and a backup of the last working state must be restored.

5.7.3 Entity private key compromise procedures

If a compromise of a private CA key is discovered, the involved CA must stop its operation immediately. Furthermore, the compromise must be published over the channels specified in section 2.2.

A new CA key pair must be created and a new CA certificate must be issued. The new CA certificate must be published over the channels specified in section 2.2.

5.7.4 Business continuity capabilities after a disaster

The CA operator must develop, test, maintain and implement a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster.

Relevant standards as ISO2700x and ISO 22301 Business Continuity Management should be used as source of information.

5.8 CA or RA termination

If a CA is about to terminate its operation, it must inform all subscribers about this as early as possible. When the date of termination is known, the CA must not issue certificates that are valid after the termination date. A CA should not terminate operation during the lifetime of its CA certificate. If an earlier termination is necessary for any reason, the CA private key must be de-activated on the day of termination.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key Generation Ceremonies must be conducted to generate CA key material. Key generation must take place in a hardware security module (HSM) following the standards specified in section 6.2.1. The key ceremony must be documented and the documentation must be archived.

End-entity or leaf-certificate keys should preferably be generated in the subject device (car control unit, charge point control unit, as described in Section 6.2.2), or in an HSM, which is located either in the production site of the control unit or the end product (car, charging equipment).

6.1.2 Private key delivery to subscriber

Key material must be generated by the subscriber. Private keys must not be generated by the CA operator and distributed to the subscriber.

6.1.3 Public key delivery to certificate issuer

PKCS#10 requests must be used to deliver public keys generated by subscribers to the certificate issuing system.

6.1.4 CA public key delivery to relying parties

Every relying party must verify the certificate of the Root CA before storing it safely. The validating of the Root CA Certificate fingerprint must include checking the certificate’s fingerprint using a second communication channel.

6.1.5 Key sizes

Key sizes and algorithms are defined in ISO15118-2.

6.1.6 Public key parameters generation and quality checking

Generation of CA keys must take place in appropriate HSM (6.2.1).

Before issuing a certificate the issuing CA or the resp. RA must check the public key parameters (algorithm and length), so that no non-compliant algorithm and key length can be used for requesting a certificate.

Requests with non-compliant algorithm and key length must be rejected.

6.1.7 Key usage purposes

ISO 15118 V2G PKI participants keys must be used according to the appropriate certificate usage specified in section 1.4.

Key usages are also specified in the key usage extension fields in the certificate profiles, see section 7

6.2 Private Key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

HSM's must be used for generating CA keys and CA-related devices like CRL- or OCSP signer. HSMs must be certified against FIPS 140-2 level 2 [FIPS 140-2] or a comparable protection profile. The HSMs shall be physically protected against theft and tampering. Appropriate logical control is specified in Section 6.2.2.

6.2.2 Private Key (n out of m) multi-person control

Private CA keys and the activation data for activating, de-activating, backup and restore of the private kay material must be protected using multi-person controls.

For the Root CA a six-eyes principle, for subordinated CAs a four-eyes principle must be implemented as a minimum.

Activation for end-entity private keys must not be used.

6.2.3 Private Key escrow

Key escrow for private keys must not be used.

6.2.4 Private Key backup

One copy of all active and non-active private CA keys must be stored on dedicated backup media or in dedicated HSM devices as a minimum. The backup process

must use the key export mechanism of the HSM for storing an encrypted copy of the key.

A private key must be recovered by importing the encrypted backup into the HSM.

The multi-person control as described in section 6.2.2 must be applied during the backup process as well as during key recovery

6.2.5 Private Key archival

End-entity private key of ISO 15118 V2G PKI must not be archived.

6.2.6 Private Key transfer into or from a cryptographic module

Transfer of private keys aside from 6.2.4 Private Key Backup must not be performed.

6.2.7 Private Key storage on cryptographic module

See section 6.2.1 Cryptographic module standards and controls.

6.2.8 Method of activating private key

CA key material must be activated before it should be used. See section 6.2.2 Private Key (n out of m) multi-person control.

6.2.9 Method of deactivating private key

Each CA key must be deactivated after usage. See section 6.2.2 Private Key (n out of m) multi-person control.

6.2.10 Method of destroying private key

At the end of the usage period of a private CA key, it must be destroyed by using the key removal function of the HSM. The multi-person control as described in section 6.2.2 Private Key (n out of m) multi-person control shall be applied for CA key removal.

CA key material must not be re-used.

If an end-user private key is generated in an HSM, it shall be destroyed after generation and read-out using the key removal function of the HSM

6.2.11 Cryptographic module rating

See 6.2.1

6.3 Other aspects of key pair management

6.3.1 Public Key Archival

CAs must archive their own public keys, as well as the public keys of all certified CAs, in accordance with section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity and the operation period (i.e. key usage or re-keying period) for certificates shall be set in accordance with Annex F of [ISO 15118-2] as given below.

- V2G Root CA and V2G Root OCSP Signer certificate
    - Validity: 40 years
    - Operational period: 10 years
- CPO Sub-CA1 and CPO Sub-CA1 OCSP Signer certificate
    - Validity: 4 years
    - Key usage period: max. 4 years
- CPO Sub-CA2 certificate
    - Validity: 1-2 years
    - Key usage period: max. 1-2 years
- Charge Point (SECC) certificate
    - Validity: 2-3 months
      Should not exceed the max. validity length defined by [4]. The ISO 15118 V2G PKI operator has to include use cases with recommended validity length as an annex to his CP
    - Key usage period: less or equal to the validity
- MO Sub-CA1 certificate
    - Validity: max. 20 years

- Key usage period: max. 15 years

- MO Sub-CA2 certificate
  - Validity: max. 10 years
  - Key usage period: max. 6 years

- Contract Certificate
  - Validity: 1 day – 2 years
    Should not exceed the max. validity length defined by [4]. The ISO 15118 V2G PKI Operator has to include use cases with recommended validity length in an annex to his CP
  - Key usage period: less or equal to the validity

- OEM Sub-CA1 certificate
  - Validity: max. 10 years
  - Key usage period: max. 10 years

- OEM Sub-CA2 certificate
  - Validity: max. 10 years
  - Key usage max. 10 years

- OEM Provisioning (EVCC) certificate
  - Validity: up to the OEM
  - Key usage period: up to the OEM

The usage period for key material must not exceed the validity period for their certificates, except that private keys may continue to be used after the operational period for decryption.

The operational period of a certificate ends upon its expiration or revocation. A CA must not issue certificates if their validity period would extend beyond the key usage period of the CA. It follows that the maximal key usage period is the validity period of the CA certificate minus the validity period of the certificates that the CA issues. Upon the end of the key usage period, the CA shall no longer sign certificates with the key. It can sign revocation information until the expiry of all issued certificates.

6.4 Activation data

6.4.1 Activation data generation and installation

During the creation of the CA key pair the corresponding activation data must be generated as described in Section 6.1.1.

6.4.2 Activation data protection

Keeping and protecting the credentials for activation private CA keys against the loss, theft, modification, unauthorized disclosure, or unauthorized use is the sole responsibility of the respective officers.

6.4.3 Other aspects of activation data

No stipulation

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The software and hardware for running CA und RA functions must be implemented on trustworthy systems in accordance with best-practice standards. ISO 2700x may be used as guideline to build up trustworthy system.

Operating the Root CA in an offline environment is recommended.

6.5.2 Computer security rating

As a minimum, assessments must be made in the framework of internal audits. ISO 27001 may be used as guideline to build up trustworthy system

The auditors must have appropriate auditor certifications.

6.6 Life cycle technical controls

6.6.1 System development controls

All CAs must use CA software that has been designed and developed under a development methodology. The design and development process must be supported

by a verification process to influence security safeguard design and minimize residual risk.

6.6.2 Security management controls

Mechanism and policies for controlling and monitoring the integrity of the CA-Systems must be implemented. The integrity of the CA systems must be verified upon installation and periodically thereafter (at least once per quarter).

6.6.3 Life cycle security controls

The software used to manage and operate the CAs of the ISO 15118 V2G PKI system must be checked prior to installation that it is:

- originated from the expected supplier,
- has not been modified prior to installation, and
- is the version intended for use.

This validity and integrity check must be performed regularly at least once a quarter.

6.7 Network security controls

The IT networks must be secured to prevent unauthorized access, tampering, and denial-of-service attacks. Communications of sensitive information must be protected using end-to-end encryption for confidentiality and digital signatures for non-repudiation, authenticity and integrity by implementing state of the art encryption methodology and algorithms (e.g. by TLS and digital signature mechanisms).

6.8 Time stamping

Certificates, CRLs, and other revocation database entries must contain time and date information, but need not be a cryptographically secured timestamp. All time information must be based on a reliable time source.

Time sources and its correctness must be monitored and alerted in case of unexpected changes.

7 Certificate, CRL and OCSP profiles

This section describes formats of certificates, CRLs and OCSP

7.1 Certificate profile

Certificate profiles must comply with profiles described in Annex B of ISO 15118-2 [V2G2-ED2-884].

7.1.1 Version number(s)

All certificates issued must be compliant with RFC5280.

7.1.1.1 Root CA certificate profile

Root CA certificate profiles shall follow requirements as per Table B.1 in Annex B of ISO15118-2.

Additionally:

- AuthorityKeyIdentifier shall be present
- CertificatePolicies for Root CA profiles shall indicate the certificate is a “High Assurance Level" certificate as defined in section XXXX of this document and the certificates shall be issues in a manner that is consistent with “High Assurance Level” requirements.
-

7.1.1.2 Charge Point Operator Certificate profiles

Charge Point Operator certificate profiles shall follow requirements as per Table B.2 in Annex B of ISO15118-2.

Additionally:

- AuthorityKeyIdentifier should be present

7.1.1.3 Mobility Operator Certificate profiles

Mobility Operator Certificate profiles shall follow requirements as per Table B.4 in Annex B of ISO15118-2.

Additionally:

- AuthorityKeyIdentifier shall be present

7.1.1.4 Provisioning certificate profiles

Certificate Installation certificate profiles shall follow requirements as per Table B.3 in Annex B of ISO15118-2.

Additionally:

- AuthorityKeyIdentifier shall be present

7.1.1.5 OEM Provisioning Certificate profiles

OEM Provisioning certificate profiles shall follow requirements as per Table B.5 in Annex B of ISO15118-2.

Additionally:

- AuthorityKeyIdentifier shall be present
- CertificatePolicies SHALL be present and reflect the actual assurance level of the certificate that is present on the EVCC (low, medium, high assurance).

7.1.2 Certificate extensions

Certificate extensions shall follow the requirements described in Table B.1 to B.5 in annex B of ISO15118-2.

7.1.3 Algorithm object identifiers

Algorithm object identifiers shall follow the requirements described in Table B.1 to B.5 in annex B of ISO15118-2.

7.1.4 Name forms

See 3.1.1

7.1.5 Name constraints

Name constraints must not be used

7.1.6 Certificate policy object identifier

See extension „CertificatePolicies“ in the relevant certificate profile.

7.1.7 Usage of Policy Constraints extension

Policy Constrains must not be used

7.1.8 Policy qualifiers syntax and semantics

No stipulation

7.1.9 Policy qualifiers syntax and semantics

No stipulation

7.2 CRL profile

The certification revocation lists must be issued in accordance with RFC 5280

7.2.1 CRL and CRL entry extensions

The CRLs must include the following extensions:

- Version
- Signature algorithm
- Issuer
- Issuing date
- Validity period information
- List of all revoked serial numbers
- Serial number
- Timestamp of revocation

- Signature of CRL

7.3 OCSP Profile

7.3.1 Version number(s)

Version 1 of Online Certificate Status Protocol as defined in RFC2560 must be supported by the OCSP responders.

7.3.2 OCSP extensions

No stipulations

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

A regular compliance audit must be performed at any CA participating the ISO 15118 V2G PKI by an independent assessor.

A compliance audit must be performed before introduction of a new CA and at least every time a new Sub-CA certificate is requested. All parts of the ISO 15118 V2G PKI must be audited at minimum every three years.

8.2 Identity/qualifications of assessor

Audits must be performed by a certified company with demonstrated expertise in computer security or by accredited computer security professionals employed by a competent security consultancy. Such company shall also have demonstrated expertise in the performance of IT security and ISO 15118 V2G PKI compliance audits.

This conformity declaration or certificate must be provided by an independent entity

8.3 Assessor's relationship to assessed entity

The assessor must not have any contractual relationship to the assessed entity.

8.4 Topics covered by assessment

The topics covered by the assessment must include all statements made in the CP of the ISO 15118 V2G PKI.

8.5 Actions taken as a result of deficiency

A process must be established and implemented specifying how deficiencies are assessed and measures to remedy them are taken and implemented.

8.6 Communication of results

The results of the audit, any subsequent measures and their implementation must be documented and archived.

9 Other business and legal matters

9.1 Fees

Not applicable

9.1.1 Certificate issuance or renewal fees

Not applicable

9.1.2 Revocation or status information access fees

Not applicable

9.2 Financial responsibility

Not applicable

9.2.1 Other assets

Not applicable

9.2.2 Insurance or warranty coverage for end-entities

Not applicable

9.3 Confidentiality of business information

Not applicable

9.3.1 Scope of confidential information

Not applicable

9.3.2 Information not within the scope of confidential information

Not applicable

9.3.3 Responsibility to protect confidential information

Not applicable

9.4 Privacy of personal information

Not applicable

9.4.1 Privacy plan

Not applicable

9.4.2 Information treated as private

Not applicable

9.4.3 Information not deemed private

Not applicable

9.4.4 Responsibility to protect private information

Not applicable

9.4.5 Notice and consent to use private information

Not applicable

9.4.6 Disclosure pursuant to judicial or administrative process

Not applicable

9.4.7 Other information disclosure circumstances

Not applicable

9.5 Intellectual property rights

Not applicable

9.6 Representations and warranties

Not applicable

9.6.1 CA representations and warranties

Not applicable

9.6.2 RA representations and warranties

Not applicable

9.6.3 Subscriber representations and warranties

Not applicable

9.6.4 Relying party representations and warranties

Not applicable

9.6.5 Representations and warranties of other participants

Not applicable

9.7 Disclaimers of warranties

Not applicable

9.8 Limitations of liability

Not applicable

9.9 Indemnities

Not applicable

9.10 Term and termination

Not applicable

9.10.1 Term

Not applicable

9.10.2 Termination

Not applicable

9.10.3 Effect of termination and survival

Not applicable

9.11 Individual notices and communications with participants

Not applicable

9.12 Amendments

Not applicable

9.12.1 Procedures for amendment

Not applicable

9.12.2 Notification mechanism and period

Not applicable

9.12.3 Circumstances under which OID must be changed

Not applicable

9.13 Dispute resolution provisions

Not applicable

9.14 Governing law

Not applicable

9.15 Compliance with applicable law

Not applicable

9.16 Miscellaneous provisions

Not applicable

9.16.1 Entire agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 Severability

Not applicable

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable

9.17 Other provisions

10 Glossary

Authorized Intermediary	Firm or person who acts as a link between parties.
CA	Certificate authority
CCCP	Central Contract Certificate Pool
CCP	Contract Certificate pool
CN	Common Name
CPO	Charge Point Operator
CPS	Certificate Provisioning Service
CProvS	Certificate Provisioning Service
CRL	Certificate Revocation List
CSR	Certificate Signing Request
Central OEM EV Provisioning Certificate Pool	Stores and distributes provisioning certificates
COPCP	Central OEM EV Provisioning Certificate Pool
Directory Service	IT service for publishing certificates and/or certificate revocation lists
DN	Distinguished Name
EE	End-entity (see End-entity)
End-entity	Certificate Holder if a leaf-certificate
EVCC	Electric Vehicle Communication Controller
EVSE	Electric vehicle supply equipment
HSM	Hardware secure module
IETF	Internet Engineering Task Force
ISMS	Information Security Management System ISO 27001
ISO 15118 V2G PKI	PKI for secure communication for EV charging and the related ecosystem
MO	Mobility operator
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
PCP	Provisioning Certificate Pool

PE	Private Environment
PCID	Provisioning Certificate Identifier
PKCS#10	Defines a format for a Certificate Signing Request (CSR), acc. to RFC 2986
PKI	Public Key Infrastructure
PKI Operator	Entity which operates a PKI system
PnC/P&C	Plug&Charge
RCP	Root Certificate Pool
RFC	Request for Comment
SECC	Supply equipment communication controller
V2G	Vehicle to Grid

11 References

[1] S. Chokani et. al.: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC 3647, November 2003

[2] IETF: Network Working Group, RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, 1997

[3] RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.

[4] ISO/IEC 15118-2:2014, Road vehicles -- Vehicle to grid communication interface is an international standard defining a vehicle to grid (V2G) communication interface for bi-directional charging/discharging of electric vehicles.

[5] VDE-AR-E 2802-100-1:2017-10 Handling of Certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118