HUBJECT

Certificate Policy

ISO 15118-20 V2G PKI
Hubject Plug&Charge

Version 1.1 – August 2026

Hubject GmbH

Hubject Plug&Charge

Certificate Policy (CP)
for the Hubject ISO 15118-20 V2G PKI

Hubject GmbH

EUREF-Campus 22

10289 Berlin

Germany

Version 1.1 - August 2026

www.hubject.com/pki

support@pnc.hubject.com / security@hubject.com

Document Control

Document Information		
Document Status	DRAFT	
Document Classification (Confidentiality)	PUBLIC	
Document Classification (Integrity)	STANDARD	
Document Classification (Availability)	STANDARD	
Review and Release		
Review by	F. Weber (Hubject)	25.08.2026
Review Cycle	Annual	
Approved by	**Approved on**	**Signature**
C. Hahn	26 August 2026 | 07:12:58 CEST	DocuSigned by: Christian Hahn 4D30A5D8C277420...

History

Version	Author	Comments	Date
1.1	F. Weber (Hubject)	Update of Logo and Formatting	25.08.2026
1.0	F. Weber (Hubject)	Formatting and preparation for release	12.03.2026
0.9	F. Weber (Hubject)	Integration feedback C-Level	20.02.2026
0.9	F. Weber (Hubject)	Reflection of changes regarding operations considering SAE	05.12.2025
0.8	F. Weber (Hubject)	Update of formatting, document controls and official review, updated to incorporate US SAE requirements: • Updated Ch. 1.1 • Updated Ch. 1.2	26.11.2025
0.7	F. Weber (Hubject)	Update of CP according to SAE Electric Vehicle Public Key Infrastructure Certificate Policy (CP) V1.2: • Updated Ch. 1.2 • Updated Ch. 1.5.4 • Updated Ch.4.9.7 • Updated Ch.4.9.9 • Moved a section from Ch. 6.6.3 to Ch. 6.5.3 • Updated Ch. 6.8 • Updated Ch. 7.1.3 • Updated Ch. 8.1 • Updated Ch. 8.4	04.06.2025
0.6	F. Weber (Hubject)	• Added OID Allocation Strategy to Ch. 1.2 • Added VC to Ch. 1.3.3 • Added DC to Ch. 1.4.1 • Added DRA to Ch. 3.2.2 • Updated Ch. 4.2.1 • Added Ch. 4.2.4 • Updated Ch. 4.3.1 • Updated Ch. 6.3.2 • Updated certificate profiles according to feedback re RFC and noted deviations from ISO	04.06.2025
0.5	F. Weber (Hubject)	• Annual Review • Added Document Control Page • Updated Version Details and Dates • Minor Formatting • Implementation of comments based on testing results	25.04.2025
0.4	A. Ziska (secunet)	Adjustments for SAE CP	30.09.2024
0.3	A. Ziska (secunet)	Minor editorial changes	12.09.2024
0.2	A. Ziska (secunet)	Incorporating Input after internal review	28.08.2024
0.1	A. Ziska (secunet)	Initial version	16.08.2024

List of Abbreviations

CA	Certificate authority
CN	Common name
CPO	Charge point operator
CPS	Certificate provisioning service
CRL	Certificate revocation list
CSR	Certificate signing request
DN	Distinguished name
EE	End-entity
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
MO	Mobility operator
OCSP	Online certificate status protocol
OEM	Original equipment manufacturer
PA	Policy Authority
PE	Private environment
PCID	Provisioning certificate identifier
PKI	Public key infrastructure
PnC/P&C	Plug&Charge
RFC	Request for comment
SAE	SAE International (formerly Society of Automotive Engineers)
SECC	Supply equipment communication controller
V2G	Vehicle to grid

Table 1 – List of Abbreviations

Table of Contents

Table of Contents

1 Introduction

1.1 Overview

This document, “Certificate Policy (CP) for the Hubject ISO 15118 V2G Public Key Infrastructure” (PKI) is the principal statement of policy governing the **Hubject ISO 15118-20 V2G PKI**, referred to in the following as the **“PKI**”.

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.

This CP complies with the PKI architecture, certificate issuance, and lifecycle processes and other requirements set by [ISO 15118-20] for a PKI underlying the ISO 15118 Plug & Charge communication infrastructure. This CP does not intend to impose requirement other than those necessary for compliance with the above specifications and for a secure operation of the PKI.

As long there is no new and/or separate root certificate, this document will be updated in terms of minor changes. Major changes will be based on a new V2G root CA a new OID, and thus a new CP will be published.

The CP is not a legal agreement between Hubject GmbH and participants of the PKI. Instead, contractual obligations between Hubject GmbH and participants of the PKI are established by means of user agreements with such participants. The CP is however cross-referenced in any agreement with participants of the PKI, agreeing and complying with the rules set in this CP.

This document is targeted at:

- Sub CA providers inside the PKI, who operate their Sub CA in terms of their own Certification Practice Statement that MUST comply with the requirements laid down by this CP.
- Relying parties, who need to understand how much trust to place in a certificate issued by a CA of this PKI or a digital signature using a certificate of one of these CAs.

Note: The leaf or end-entity certificates are by definition not part of the PKI.

The CP, however, does not govern any services outside the PKI. For example, how other electronic services provided by Hubject GmbH are based on these PKI services.

The structure of this CP is conforming to [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 stipulations.". Additional subchapters might have been added.

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].

SAE EVPKI ALIGNMENT

Hubject GmbH declares that this Certificate Policy is aligned to the SAE Electric Vehicle Public Key Infrastructure - Certificate Policy (EVPKI CP) Version 1.2 (issued 2024-11-12). Where this CP is more

specific than or different from the SAE EVPKI CP, the Hubject CP defines the local operational practices for the Hubject PKI.

Hubject may deviate from specific requirements of the SAE EVPKI CP where such deviations are justified, do not reduce the security or trustworthiness of the Hubject PKI, and are documented either in this CP or in the corresponding CPS. Any deviation that is relevant for a Sub1-CA or Sub2-CA applying for inclusion in the SAE EVPKI Certificate Trust List (CTL) SHALL be explicitly identified, together with the compensating controls implemented to maintain compliance with the EVPKI trust model.

For any CA (Sub1-CA or Sub2-CA) seeking inclusion in the SAE EVPKI CTL, all applicable SAE EVPKI CP Version 1.2 requirements SHALL be supported where possible, regardless of whether Hubject itself seeks CTL inclusion. In such cases, Hubject MAY support the Sub-CA operator by disclosing necessary information required by the SAE EVPKI Policy Authority and by documenting any deviations and compensating controls.

Hubject SHALL maintain an explicit mapping document showing the alignment of this CP to the SAE EVPKI CP v1.2. This mapping SHALL be published at the Hubject PKI repository alongside this CP.

1.2 Document Name and Identification

This document is the Certificate Policy (CP) for the Hubject ISO 15118-20 SAE V2G PKI.

- Name: Certificate Policy (CP) for the Hubject ISO 15118-20 SAE V2G PKI
- Version(V): 1.1
- OID: 1.3.6.1.4.1. 41525.2.2.1.
- Repository: www.hubject.com/pki

OID Structure and Versioning

The policy OID is structured as follows:
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) hubject(41525) ISO 15118-pki(2) cp(2), major-version(1)

All CP documents published in the 1.X version series will share this OID. Minor updates SHALL increment a subordinate OID (e.g., 1.3.6.1.4.1.41525.2.2.1.1, .2, etc.) to indicate non-breaking revisions. Major updates that result in policy reclassification or incompatibility SHALL be assigned a new root OID.

Subordinate CAs MAY assert additional policy OIDs in their certificates if their CPS augments this CP, provided these OIDs do not conflict with or override the base policy OID.

Policy OID Allocation Strategy

This CP is identified by the OID 1.3.6.1.4.1.41525.2.2.1, which corresponds to the global ISO 15118-20 V2G PKI policy. The Global V2G Root CA defined in this CP is a worldwide trust anchor and therefore asserts a Hubject enterprise OID rather than any region-specific OID such as the SAE EVPKI enterprise OID (1.3.6.1.4.1.55053).

Since the PKI is deployed across multiple regions, including regions with separate policy requirements (e.g., North America), a Sub-CA1 certificate MAY include the anyPolicy OID (2.5.29.32.0) instead of a specific CP OID. This ensures that new region-specific Sub-CA2 certificates can be introduced without requiring reissuance of the Sub-CA1 certificate.

A Sub-CA2 certificate MAY leave the certificatePolicies extension empty to maintain maximum flexibility for future regional expansion. Where a Sub-CA2 intends to issue certificates under a regional regulatory framework (e.g., a Sub-CA2 seeking inclusion in the SAE EVPKI Certificate Trust List (CTL)), the Sub-CA2 SHALL assert the appropriate regional policy OID(s) required by SAE EVPKI CP v1.2 or by local regulatory bodies. The use of the SAE enterprise OID (1.3.6.1.4.1.55053) is limited to such region-specific Sub-CAs and does not apply to the Hubject Global V2G Root CA.

Leaf certificates MUST assert the appropriate policy OID as required by ISO 15118-20, the applicable regional regulatory requirements, and the SAE Electric Vehicle Public Key Infrastructure - Certificate Policy (EVPKI CP) Version 1.2 and any associated SAE EVPKI CTL requirements. Responsibility for correct policy OID assignment in leaf certificates lies with the issuing CA or its delegate.

1.3 PKI Participants

1.3.1 Certification authorities

The ISO 15118 V2G PKI encompasses various top-level Root CAs and subordinate Sub1- and Sub2-CAs in accordance with [ISO 15118-20], as depicted in Figure 1 – Overview certificate structure - Source: Annex H of ISO 15118 -20, below.

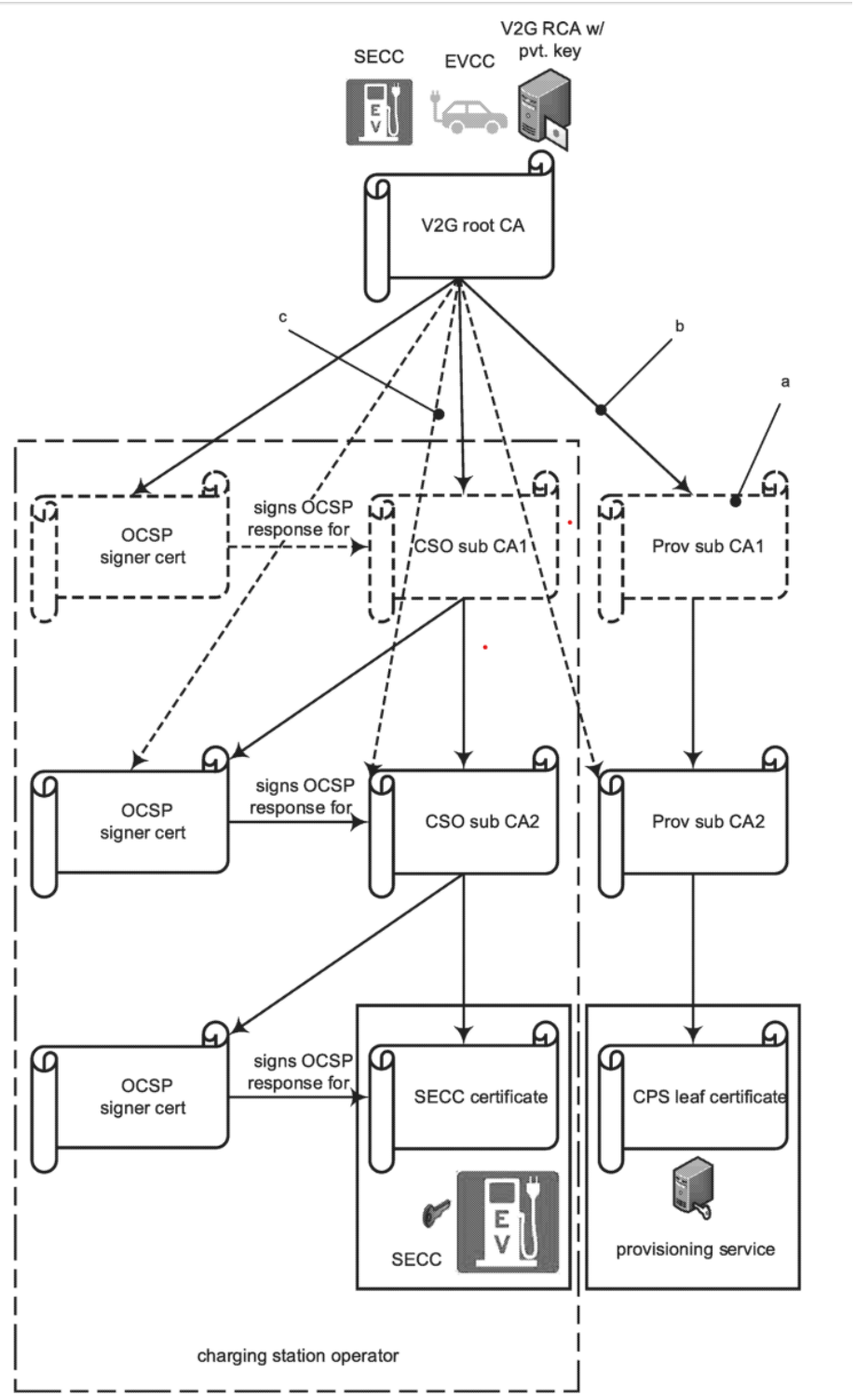

Figure 1 – Overview certificate structure - Source: Annex H of ISO 15118 -20

The following types of CAs are used 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. The V2G Root CA certificate MUST be used to validate the authenticity of any certificate in the PKI[1]. The private keys belonging to the Root CA of the ISO 15118 V2G PKI are the responsibility of Hubject GmbH. The operational business of all CAs belonging to the ISO 15118 V2G PKI is carried out by Technology Nexus Secured Business Solutions AB.[2]
- **OCSP Signer:** The V2G Root CA MAY OPTIONAL 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).
- **CSO Sub1- and Sub2-CA**: These types of Sub CAs are issued by V2G Root CA and are part of V2G PKI. This type of Sub CA issues – via a chain of sub1- and Sub2-CA – EVSE certificates. The CPO Sub CAs are the part of V2G PKI. A cross-certification of the CPO Sub CA public key by the CPO operators is not permitted.
- **CSO OCSP Signer Authority**: A CPO Sub1-CA MAY OPTIONAL delegate the task of signing OCSP responses on its behalf to an OCSP signer authority.
- **Provisioning Sub1- and Sub2-CA:** This type of Sub CAs are issued by V2G Root CA and are part of V2G PKI. The V2G Root CA issues – via a chain of Provisioning Sub1 and Sub2 CA – leaf provisioning certificates. A cross-certification of the Provisioning Sub CA public key by the Certificate Provisioning Service operators is not permitted.

Each Sub1-CA Certificate is issued by a Root CA. Each Sub2-CA certificate is issued by a Sub1-CA. Sub2-CAs MUST not issue certificates for other subordinate CAs, but exclusively for end-entities (see Section 1.3.3).

The respective Sub1-CA and or Sub2-CA operated by the MO or OEM, issued by a V2G Root CA of this PKI, MUST enter a contractual relationship with Hubject GmbH to abide by all the requirements of this CP in relation to their Sub1-CA and subordinate Sub2-CA. These Sub1- and Sub2-CAs MAY implement more restrictive practices based on their internal requirements.

Sub1-CAs and Sub2-CAs within the public V2G PKI MAY be operated by organizations other than Hubject GmbH. The Sub1-CA certificate of such an independent CPO, MO, or OEM will be issued by the V2G Root CA. The respective Sub1-CA provider MUST enter a contractual relationship with Hubject GmbH to abide by all the requirements of this CP in relation to the Sub1-CA.

Sub1- and Sub2 CAs MUST have a Certificate Practice Statement describing how the requirements from the CP will be fulfilled. These Sub1- and Sub2-CAs MAY implement more restrictive practices based on their internal requirements. The Certificate Practice Statement's practical implementation is audited by Hubject GmbH before a CA certificate is issued. See Section 3.2.6 Criteria for interoperation.

[1] MOs and OEMs can decide whether they wish to operate a root CA themselves, along with the associated strict security requirements, or prefer to hand this task over to an existing V2G root CA (OPTIONAL certification). This is not to be regarded as cross-certification, but this is a unique choice by MOs or OEMs.

[2] Technology Nexus Secured Business Solutions AB / Telefonvägen 26, 126 26 Hägersten, Sweden / Represented by managing director: Olivier Dussutour / Contact: Email: contact@nexusgroup.com / Registration: Registered in 2017, Registered Court: Stockholm, Registration Number: 556258-0414 / VAT Identification Number:SE556258041401

This CP applies to the "public charging"[3] part of the V2G PKI, which is referred to as the **"PKI**" in the following sections. The CAs and end-entity certificates within the "Private Environment", as defined in ISO 15118-2, are out of scope of this CP.

The Hubject V2G Public Key Infrastructure, hereafter abbreviated as "PKI", summarizes all authorities whose trust anchors can be traced back to the V2G Root CA using digital signatures and certificates. Furthermore, such authorities SHOULD also be regarded as part of the PKI, which fulfil the requirements of the V2G Root CAs Certificate Policy and, based on this conformity, are granted participation in the infrastructure.

- The OEM Root CA and the Mobility Operator Root CA are not considered part of the PKI but provide the trust anchors of their subordinated CAs. These subordinated CAs can be considered part of the PKI as long as they conform to the CP and can be subordinated to the V2G Root CA through cross certification.
- The leaf or end-entity certificates are by definition not part of the PKI.
- All certificate pools are considered part of the PKI and are protected as such.
- The set of roles, policies, hardware, so□ware and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption at all these CAs are considered as part of the PKI.

1.3.2 Registration authorities

A Registration Authority (RA) is an entity that executes several tasks on behalf of a CA of the PKI. For each CA to which this CP is applied (see Section 1.1), the relevant Certificate Practice Statement SHALL specify which RA(s) will be used.

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.
- Provisioning infrastructure and processes for transmitting the issued certificates to the applicants.
- Identifying and authenticating applications for follow-up certificates.

Each RA MUST provide a separate interface for requesting end-entity certificates with client authentication.

The RAs of Root CA and Sub1-CAs MUST be separated organizationally from the CA. The RAs of Sub-2 CAs MUST be technically and organizationally separated from the CA. Depending on the use case, it MAY be necessary to have one RA per (Sub-)CA. All CAs in the same level and use case MUST have and fulfil the same requirements.

1.3.3 Subscribers

Two different terms are used in this CP:

[3] As illustrated in Figure 1, the certificate hierarchy used in ISO 15118 is also covering a Private Root CA, this is however out of scope of this CP.

- “Subscriber" is the entity which contracts with Hubject GmbH for the issuance of credentials. The subscriber holds the organizational and technical responsibilities.
- "Subject" is the entity to whom the credential is bound. More specifically, the technical component where private key and certificate are stored.

The Subscriber bears ultimate responsibility for the use of the credential, but the Subject is the entity which is authenticated when the credential is presented.

CAs are technically also subjects of CA certificates within the PKI. References to “end-entities” and “Subjects” in this CP, however, apply only to end-entity subjects and are interchangeable.

End-entities, which obtain certificates from a Sub2-CA of the PKI, are the technical systems and components defined in ISO 15118. [ISO 15118-20] is the primary source of information on permitted end-entity types and certificate usages. Informally, we describe the end-entity types of the PKI and their use of certificates below:

- **SECC (EVSE) certificate:** This kind of certificate is used to authenticate the charge point at or in the EV (or EVCC). The corresponding private key is in possession of the SECC. SECC certificates are issued, via a chain of CPO Sub1-CA and Sub2-CA, from the V2G Root CA certificate as mentioned above.
- **Contract Certificate**: This kind of certificate is used in the Plug & Charge use case (i.e. contract-based charging) to represent a contract between a vehicle owner or driver and a secondary actor (the Mobility Operator). It is stored in an EVCC along with the corresponding private key. The EVCC provides the Contract Certificate to the SECC and proves the existence and validity of the corresponding contract. Contract Certificates are derived, via a chain of MO Sub1-CA and Sub2-CA, from the Hubject V2G Root CA or alternatively from a MO Root CA.
- **Leaf Provisioning Certificate:** The MO creates credentials for the EVCC, consisting of a Contract Certificate including a private key, which has been asymmetrically encrypted specifically for that EVCC. The Certificate Provisioning Service is considered trustworthy. It is therefore not required that the EVCC is able to verify the Contract Certificate it has received. The Leaf Provisioning Certificate will be issued by Provisioning Sub2-CA, which is issued from the Provisioning Sub1-CA and Hubject V2G Root CA (See Section 1.3.1).
- **OEM Provisioning Certificate (EVCC certificate):** This kind of certificate is individual for each electric vehicle (installed e.g. at vehicle production) and enables an EVCC to request a valid Contract Certificate for Plug & Charge.
- **Vehicle Certificate:** Introduced in ISO 15118-20, the Vehicle Certificate is used to authenticate the vehicle, independently of a Contract Certificate. It is stored in the EVCC and is linked to the Vehicle Object Identifier (Vehicle OID). This certificate can be used in multiple use cases beyond Plug & Charge, such as certificate-based authorization scenarios. Vehicle Certificates are issued via a dedicated OEM Sub2-CA, typically derived from an OEM Root CA or the Hubject V2G Root CA.

1.3.4 Relying parties

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

- authenticating subjects of the PKI,
- confirming that a message is signed by a legitimate participant,
- encrypting messages.

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

1.3.5 Other participants

None

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

CA certificates and end-entity certificates issued within the PKI MUST be used in accordance with [ISO 15118-20], which is the primary source of information on permitted CA and end-entity types and certificate usages.

Subscribers receiving End-Entity authentication certificates SHALL use the certificates for authentication using TLS version 1.3 or higher and subscribers receiving End-Entity identity certificates for user identity purposes (e.g., contract certificates), as designated by the keyUsage and extKeyUsage fields found within the certificate.

Private keys of certificates MUST only be used in accordance to the certificates *KeyUsage* and *ExtendedKeyUsage* fields.

Subscribers or Sub-CAs SHALL protect their Private Keys from unauthorized use and disclosure and SHALL discontinue use of the Private Key following expiration or revocation of the certificate.

Subscriber or Sub-CA SHALL use the certificate(s) in lawful accordance with the Subscriber agreement, if applicable and the terms of this CP.

To prevent misuse of certificates issued under the same root CA, the domainComponent (DC) attribute in the certificate's distinguished name (DN) is used as a critical scoping mechanism. The DC field explicitly ties the certificate to a particular domain or stakeholder (e.g., CPO, MO, OEM, Provisioning), ensuring that certificates intended for one domain are not inappropriately used in another domain. This mechanism prevents scenarios such as a CSO leaf certificate being used to sign a contract installation package, which is normally the role of a Provisioning leaf certificate.

This domain-based separation is essential to maintain trust boundaries and proper operational security within the PKI, and an overview mapping of DC values to stakeholder objects is recommended to provide clarity and support governance processes.

1.4.2 Prohibited certificate uses

Certificates issued by CAs of the PKI MUST be used for services in accordance with ISO 15118-20 use cases und SHALL not be used for other purposes.

Applications that MUST NOT be used include, but are not limited to:

- Any export, import, use, or activity that contravenes any local or international laws or regulations;
- Any usage of certificates in conjunction with illegal activities;
- Any usage of certificates for personal use or purposes not related to the community's operation;
- Any use of a certificate after it has been revoked;
- Any use of a certificate after it has expired; and

- Any use not expressly permitted in Section 1.4.1.

1.5 Policy Administration

1.5.1 Organization administering the document

This document is administered by Hubject GmbH, EUREF Campus 22, 10829 Berlin. The organization can be contacted regarding this CP as stated in Section 1.5.2.

1.5.2 Contact person

Questions regarding this CP SHOULD be addressed to the following address:
support@pnc.hubject.com and security@hubject.com.

1.5.3 Person determining CP suitability for the policy

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

1.5.4 CP and CPS approval procedures

This Certificate Policy (CP) SHALL be reviewed regularly and updated as necessary, including in response to significant changes in the PKI ecosystem or compliance requirements. All modifications to the CP, including both minor and major revisions, MUST be reviewed and approved by Hubject GmbH, which acts as the Policy Authority (PA) in accordance with the governance model of the V2G PKI.

- Minor updates MAY result in incremented sub-identifiers of the current policy OID.
- Major updates MUST result in a new CP OID.
- Versioning and publication procedures SHALL follow the rules defined in Section 1.2.2 and be published via the official repository: https://www.hubject.com/pki.

Any Certification Authority (CA) operating within this PKI MUST develop a Certificate Practice Statement (CPS) that aligns with this CP. The CPS MUST be approved before the CA begins operations.

- CAs SHALL submit their CPS to Hubject GmbH or their designated Superior CA for approval.
- The Superior CA MUST approve a Subordinate CA's CPS if it determines compliance with the Root CA's CP.
- A Subordinate CA MUST meet all approved CPS requirements prior to commencing certificate issuance.
- All CPS approval requests SHALL be submitted via the contact information provided in Section 1.5.2.

1.5.5 Interaction with SAE EVPKI Policy Authority

Where Hubject or any Hubject-issued Sub-CA requests recognition or inclusion in the SAE EVPKI CTL, Hubject MAY comply with the EVPKI governance and Policy Authority actions.

The SAE EVPKI Policy Authority (EVPKI PA) is responsible for the governance of the SAE EVPKI ecosystem, including Root CA onboarding, CTL management, and operational compliance processes defined in the SAE EVPKI CP v1.2.

Where Hubject or any Hubject-issued Sub-CA requests recognition or inclusion in the SAE EVPKI CTL, Hubject MAY comply with the EVPKI governance and Policy Authority actions including decisions, and validation procedures of the EVPKI PA.

The EVPKI PA does not act as the Policy Authority for any Hubject Root CA or Subordinate CA. Hubject GmbH remains the sole Policy Authorities for their respective Root CA as defined in Section 1.5.5. The role of the EVPKI PA is limited to governing the EVPKI trust ecosystem and determining CTL inclusion.

1.6 Definitions and Acronyms

See the “List of Abbreviations” at the beginning of the document.

2 Publications and Repository Responsibilities

2.1 Repositories

The V2G Root CA, MO Root CAs, and MO Sub1- and Sub2-CAs MUST generate and publish CRLs.

The V2G Root CA, CPO Sub1-, and Sub2-CAs MUST provide an OCSP service. All other CAs MAY provide an OCSP service.

The CRL/OCSP access method and address MUST be asserted in the certificates Authority Information Access extension:

- accessMethod=id-ad-ocsp
- accessLocation=URL of the responder.

Accessing information in the repositories and the use of the CRL/OCSP service MUST be publicly available without restrictions and free of charge. Writing access to the repositories MUST be limited to dedicated employees and IT systems of Hubject GmbH.

All CAs in the PKI MUST provide relying parties with information (e.g. on their web pages or in contract material) on how to access certificates in the repository, and if applicable, how to access CRLs and the OCSP responder.

SAE EVPKI CTL / CTL metadata

Hubject SHALL cooperate with SAE EVPKI CTL operators to validate submitted CA metadata and to correct any discrepancies identified during CTL onboarding or review processes.

2.2 Publication of Certification Information

Each CA of the PKI MUST publish the following information, e.g. on its web page:

- A link to the corresponding V2G PKIs CP
- The V2G Root CA certificate and its SHA256 fingerprint
- The CA MAY publish their own CPS document or alternatively SHALL publish an independently issued audit report. A CA MAY redact any information it deems confidential from its publicly available CPS.

Each CA of the PKI MAY publish the following information, e.g. on its web page:

- The Sub1- and Sub2-CA’s certificates and their fingerprints

This information MUST be publicly available without restrictions and free of charge. The web page MUST be TLS (minimal version 1.2) protected. The V2G Root CA publishes this CP on the web page https://www.hubject.com/pki

The V2G Root CA publishes the finger print of all its active V2G Root Certificates on the web page https://www.hubject.com/pki for an out-of-band verification.

Information on certificate revocation MUST be published as CRL (using standard access methods, i.e. LDAP or HTTP).

2.3 Time or Frequency of Publication

The latest versions of this of the documents and data mentioned in **Error! Reference source not found.** MUST be published promptly.

2.4 Access Control on Repositories

The information published in the repositories MUST be accessible for the PKI participants of the PKI. Read-only access to such information MUST be unrestricted.

Write-access to repositories MUST be restricted to V2G Root CA, Sub1-CAs, Sub2-CAs, and Certificate Provisioning Service. Access controls, logical and physical security measures MUST be implemented to prevent unauthorized persons from adding, deleting, or modifying the published information. Every write access to the repositories MUST be logged and archived.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

Inside the PKI, a consistent hierarchy for naming MUST be used. All issued certificates comprise distinguish names (DN) according to [RFC 5280]. Each participant in the PKI MUST be uniquely identifiable 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” MAY be added more than once.

Each issuing Sub1-CA MUST declare a unique subject namespace towards the superordinate V2G Root CA.

Each issuing Sub2-CA MUST declare a unique subject namespace towards the superordinate Sub1-CA. The issuing Sub1- and Sub2-CAs MUST not use subject DNs outside the stipulated namespace.

The uniqueness of subject DNs MUST be ensured by the issuing (Sub) CA. The subject DNs has a limit of 64 characters.

CAs MUST assign DNs in the form of a X.500 [4]UTF8 to the issuer and subjectDN fields.

3.1.2 Need for names to be meaningful

End-entity subscriber 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 B of [ISO 15118-20].

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

The CA or RA MUST verify that names used in to-be-issued certificates represent an unambiguous identifier for the Subject and that the Subject contains the verified identification of the Sub-CA or Subscriber. The RA MUST use the verified company name or Subscriber name as the organizationName field in the Subject DN of the issued certificate.

3.1.3 Anonymity or pseudonymity of subscribers

CA and end-entity subscribers MUST not use pseudonyms. Requests for anonymity or pseudonymity in a certificate MUST be rejected.

3.1.4 Rules for interpreting various name forms

Rules for interpreting DN forms are specified in X.500.

3.1.5 Uniqueness of names

The subject DNs within the PKI MUST be unique. See 3.1.1

3.1.6 Recognition, authentication and role of trademarks

Certificate applicants SHALL not use names in their certificate applications that infringe upon the Intellectual Property Rights of others. Hubject SHALL not be required to determine whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark, and Hubject SHALL be entitled, without liability to any certificate applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

See Section 3.2.6 Criteria for interoperation and 4.2.1 Performing identification and authentication functions.

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.

[4] ITU-T Recommendation X.500 Series (1994) – ISO/IEC 9594, 1-9:1994, Information Technology – Open Systems Interconnection – The Directory

The method to prove possession of a private key SHALL be a PKCS#10 Certificate Request. The PKCS#10 Certificate Request [11] MUST be submitted by the applicant in a secure manner[5]. 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.

Generating the key material for an end-entity certificate by the issuing CA is OPTIONAL. In this case the issuing CA and the subscriber MUST provide an infrastructure for secure delivery of private keys as well as their storage at the end-entity.

3.2.2 Authentication of organization identity

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

The RA SHALL verify that the identity of the organization:

- Is not on a government watch list at the CA's location;
- If the organization is on a watch list, it is up to RA's discretion to continue with the Authentication;
- Conducts business at the address provided; and
- The verified organization or trade name is used in the organizationName field of the certificate as a way for relying parties to Authenticate the organization name.
- Determine that the organization exists by using at least one third-party identity proving service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or recognized authority that confirms the existence of the organization,
- Confirm by telephone, confirmatory postal mail, or comparable procedure that the organization has authorized the certificate application, and that the person submitting the certificate application on behalf of the certificate applicant is authorized to do so.

Validation procedures for issuing CA certificates SHALL be documented in the Certificate Practice Statement of the CA that issues the CA certificate (V2G Root CA or a Sub1-CA).

Each Sub1-CA MUST have a person who is responsible for the registration of organizational entities. This person MUST be known and approved by the V2G Root CA. The V2G Root CA MUST archive the appropriate list.

Device Registration Accountability

In cases where certificates are issued to devices under the control of a validated organization (e.g., CSOs issuing leaf certificates for EVSEs), the RA SHALL ensure that the organization maintains proper registration and accountability of the devices it manages.

Specifically, the RA MUST verify that the requesting organization has established a valid enrolment and registration process for devices (e.g., EVSEs) under its control. This serves to bind device identities to a known and authenticated organizational entity.

[5] Secure manner implies that integrity and authenticity of the Certificate Request can be assured.

Device-level validation requirements (including pre-registration enforcement) are described in Section 4.2.1.

3.2.3 Authentication of individual identity

The RA SHALL verify:

- That the individual is authorized by the organization to be named in the certificate;
- That the individual's identity has been verified by the RA or Authorized Entity; and
- That the request was received from a certified/approved organization or Authorized Entity.

3.2.4 Non-verified subscriber information

Subscriber information that is not verified by the CA or RA SHALL NOT be included in Certificates.

3.2.5 Validation of authority

The person responsible for registration of organisational entities MUST be known and approved by the V2G Root CA, see Section 3.2.2. The V2G Root CA MUST archive the appropriate list.

3.2.6 Criteria for interoperation

If a new Sub1-CA or Sub2-CA is to be introduced as part of the PKI, it MUST be verified by the V2G Root CA. The V2G Root CA MUST check if the Certificate Practice Statement of the new Sub1- or Sub2-CA complies with the CP of the PKI. A responsible operator of the new Sub1-CA or Sub2-CA MUST be identified and registered at the V2G Root CA.

The approval procedure includes an audit for any Sub1-CA or Sub2-CA before joining the PKI. This approval process is described in a document which is available on request from Hubject GmbH. The audit includes a Sub CAs Certificate Practice Statement review and an on-site inspection.

After the successful conclusion of the approval, the Sub1- or Sub2-CA receives an affirmation answer from the V2G Root CA.

Audit documentation, forms and approval document MUST be archived by the V2G 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, the subscriber MUST 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 PKI.[6]

[6] 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.

3.3.2 Identification and authentication for re-key after revocation

After the revocation of a CA certificate, the superordinate CA SHALL perform a root cause analysis of the problem that led to the revocation and create a documented plan to resolve the problem with fixed deadlines.

The issuance of a new CA certificate and re-key SHALL NOT be performed prior to the completion of the above plan and SHALL follow the same procedure as the initial enrolment described in section 3.2.

certificate re-keying for CA-related devices like OCSP signer MUST be handled the same way as a new certificate request. See chapter 3.2.

The issuance of a new End Entity certificate for a Re-Key SHALL follow the same procedure as the initial registration process as described in section 3.2.

3.4 Identification and Authentication for Revocation Request

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

One of the following procedures for authenticating the revocation requests MUST be employed:

- Receiving a digitally signed email from the subscriber or an authenticated and authorized intermediary that requests revocation with reference to the certificate (certificate serial number) to be revoked. The signing certificate MUST be issued by a trustworthy certification authority.
- Receiving a written and signed message on corporate letter sheet from the subscriber or an authenticated and authorized intermediary that requests revocation with reference to the certificate (certificate serial number) to be revoked.
- Using an API after authentication provided by the CA operator
- The name of the sender of these revocation requests MUST be known to the CA and MUST be on a list of authorized parties for revocation.

Please refer to Section 0 for reasons for revoking a certificate.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

The term certificate application refers to the following processes:

a) Initial registration for a certificate
b) Application for a certificate
c) Re-key for a certificate

4.1.1 Who can submit a certificate application?

Below is a 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

Prospective subscribers SHALL submit sufficient information to allow the CA or RA to successfully perform the required verification.

The CA or RA SHALL develop processes that verify the prospective subscriber's identity for all certificate types generated for the EV Charging PKI according to Section **Error! Reference source not found.**.

Prospective subscribers or an Authorized Entity SHALL:

- Complete a certificate application;
- Provide the requested information;
- Respond to verification requests in a timely manner;
- Generate the Key Pair, if required;
- Deliver the Public Key of the Key Pair to the RA, if required; and

The items in the list above MAY be completed in any order that is convenient for the RA and prospective subscribers that does not defeat security, but all SHALL be completed before certificate issuance.

The process for approving Sub CAs is described in Section 3.2.6.

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

Applications for certifications of Sub CAs MUST be addressed to the responsible person at the superordinate CA. Subscribers of Sub CA certificates enter 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.

During this contracting process or, at the latest, prior to the certification process, the applicant MUST cooperate with superordinate CA to determine the appropriate distinguished name and the content of the certificates to be issued by the applicant

The process for identifying end-entities for certificates is in the sole responsibility of the issuing Sub CA. The process for identification and authentication MUST assure that only authenticated requests will result in issued certificates.

Pre-Registration Requirement for End-Entity Devices

For certificate requests pertaining to EVSEs or other connected devices under the authority of a CSO, the issuing Sub CA or its delegated RA MUST enforce that each device is pre-registered within the RA's system prior to accepting the certificate signing request (CSR).

The pre-registration MUST include a unique identifier for the device and its association with a verified organization.

If a CSR is received for an unregistered device, it SHALL be rejected.

This requirement ensures traceability of device certificates, prevents unauthorized issuance, and enforces policy-aligned enrolment across the PKI. The implementation of this check SHOULD be documented in the Sub CA's CPS.

4.2.2 Approval or rejection of certificate applications

The superordinate CA MUST approve an application for a Sub CA certificate if the following criteria are met:

- Successful identification and authentication of all required subscriber information in terms of Section 3.2.6 Criteria for interoperation and 4.2.1 Performing identification and authentication functions.
- Audit trail has been finished successfully. See 3.2.6 Criteria for interoperation.
- Payment (if applicable) has been received.

The superordinate CA MUST reject a certificate application if:

- identification or authentication of all required subscriber information in terms of Section 4.2.1 Performing identification and authentication functions cannot be completed, or
- the audit trail (see 3.2.6 Criteria for interoperation) finished unsuccessfully, or
- Payment (if applicable) has not been received.

The CA MAY reject any certificate Application if the CA believes that issuing a certificate MAY bring the CA into disrepute. The CA SHALL log all certificate Application rejections and the reason for the rejection.

Approval or rejection of certificate applications for end-entities by the Sub CAs is in the sole responsibility of the Sub CAs. The approval process MUST assure that only authenticated requests will result in issued certificates.

4.2.3 Time to Process Certificate Applications

The V2G Root CA, Sub1-CAs, and Sub2-CAs MUST begin processing certificate applications within a reasonable time of receipt. CAs or RAs MUST process certificate Applications within a reasonable time of receipt of all necessary documents as specified in their CPS.

A certificate application SHOULD remain active until rejected or processed.

4.2.4 Mandatory Registration with the RA

All stakeholders requesting certificates under this PKI — including but not limited to CSOs, OEMs, EVSEs, and other end-entities — MUST be registered with the responsible Registration Authority (RA) prior to submitting a Certificate Signing Request (CSR).

The registration process SHALL include:

- Entity classification (e.g., CSO, OEM, EVSE)
- Legal and operational identity information
- Unique identifiers for devices (if applicable)
- The association with a validated organization

The RA is responsible for:

- Validating submitted identity data according to Section 3.2.2
- Maintaining an authoritative and auditable registry
- Rejecting CSRs from entities that are not pre-registered

Delegation of registration duties to third-party RAs is permitted, provided the CA ensures all validation, logging, and compliance obligations are fulfilled in accordance with this CP.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

The certificate MUST be created following the approval of a certificate Application and issued by the CA. The certificate MUST be made available to the applicant. All CA actions MUST be logged and archived.

If using a RA, upon receiving the certificate request, the CA MUST:

- Authenticate the RA using a credential provided to the RA by the CA;
- Receive the PKCS #10 CSR generated by the Subscriber or Sub-CA from the RA, if applicable;
- Generate a CSR, if necessary;
- Generate a certificate using the Public Key in the CSR, along with any additional certificate profile information provided by the Subscriber or Sub-CA, or the RA on behalf of the Subscriber or Sub-CA; and
- Ensure delivery of the certificate to the Subscriber or Sub-CA.

MO Sub2-CAs MUST provide a user interface or an API to other consumer-facing systems for revocation. The MO SHALL be checked by Hubject GmbH before its authorized to get Sub2-CA certificates.

Enforcement of RA Pre-Registration Checks

When operating in conjunction with a Registration Authority (RA), the CA MUST ensure that the RA verifies the pre-registration of the certificate subject (e.g., EVSEs or OEM components) prior to accepting and forwarding a Certificate Signing Request (CSR).

The RA MUST reject CSRs for entities that are not registered in its authoritative database. This includes all entities categorized as end-entities under the CSO or OEM namespaces.

The CA MUST obtain confirmation from the RA — through automated or manual means — that the subject identity has been pre-registered and validated before proceeding with certificate issuance.

4.3.2 Notification to subscriber by the CA of issuance of certificates

CAs SHALL notify the respective subscribers that they have created such certificates and provide subscribers with access to the certificates by notifying them about the availability of and the means for obtaining the certificates. End-entity certificates SHALL be made available to the subscribers either by allowing them to download them from a repository or through an automated IT process (e.g. REST-Interface).

4.4 Certificate Acceptance

Once downloaded, the Subscriber or Sub-CA SHOULD check the contents of the certificate without delay before installing it. If the Subscriber or Sub-CA detects any problems with the issued certificate (e.g., incorrect information, wrong Validity Period, etc.), the Subscriber or Sub-CA SHALL notify the RA about the problem.

4.4.1 Conduct constituting certificate acceptance

An issued certificate SHALL be deemed to have been accepted when it has been downloaded, installed and used and the Subscriber or Sub-CA has not notified the CA or RA of a problem with the certificate or its contents, or thirty (30) days after the certificate's issuance, whichever comes first.

4.4.2 Publication of the certificate by the CA

CAs inside the PKI MUST publish the certificates they issue in a publicly accessible repository inside the PKI based on the corresponding use cases as described in Section 2.

4.4.3 Notification of certificate issuance by the CA to other entities

Notifying other entities is OPTIONAL.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

The regulations of Section 1.4 Certificate Usage apply.

4.5.2 Relying party public key and certificate usage

Before any act of reliance, relying parties MAY independently assess the following:

- The appropriateness of the use of a certificate for any given purpose and determine that the certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by Section 1.4;
- That the certificate is being used in accordance with the keyUsage and extKeyUsage extensions included in the certificate; and
- The status of the certificate and all the CAs in the chain that issued the certificate.

If any of the certificates in the certificate chain have been revoked/expired, the Relying Party SHOULD NOT rely on the certificate or other Revoked certificates in the certificate chain to establish trust.

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 PKI, neither for Sub CA certificates nor for end-entity certificates.

4.6.1 Circumstance for certificate renewal

Not applicable, see 0.

4.6.2 Who MAY request renewal?

Not applicable, see 0.

4.6.3 Processing certificate renewal requests

Not applicable, see 0.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable, see 0.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable, see 0.

4.6.6 Publication of the renewal certificate by the CA

Not applicable, see 0.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable, see 0.

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.

The certificate re-key process for end-entity certificates is in the sole responsibility of the issuing Sub CA. 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, for the subscriber SHOULD 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. More specifically, as described in Section 3.2, the identity of the certificate and it's CP compliance MUST be rechecked.

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.

The certificate re-key process for end-entity certificates is in the sole responsibility of the issuing Sub CA. It MUST be assured, that only authenticated and authorized requests will result in issued certificates.

4.7.4 Notification of new certificate issuance to subscriber

Notification of issuance of a re-keyed certificate to the subscriber is in accordance with Section 0.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Installing a certificate or a certificate constitutes the subscriber's acceptance of the certificate.

4.7.6 Publication of the re-keyed certificate by the CA

Publication of a re-keyed certificate is in accordance with Section 0 An issued certificate SHALL be deemed to have been accepted when it has been downloaded, installed and used and the Subscriber or Sub-CA has not notified the CA or RA of a problem with the certificate or its contents, or thirty (30) days after the certificate's issuance, whichever comes first.

Publication of the certificate by the CA.

4.7.7 Notification of certificate issuance by the CA to other entities

Notifying other entities is OPTIONAL.

4.8 Certificate Modification

Certificate modification MUST not be used in the PKI.

4.8.1 Circumstance for certificate modification

Not applicable, see 4.8.

4.8.2 Who MAY request certificate modification?

Not applicable, see 4.8.

4.8.3 Processing certificate modification requests

Not applicable, see 4.8.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable, see 4.8.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable, see 4.8.

4.8.6 Publication of the modified certificate by the CA

Not applicable, see 4.8.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable, see 4.8.

4.9 Certificate Revocation and Suspension

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period.

CAs that issue CRLs, SHALL issue CRLs covering all unexpired revoked certificates issued under this CP, except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

CAs that issue CRLs, SHALL make public a description of how to obtain revocation information for the certificates they issue via the issued certificate's cRLDistributionPoints extension.

4.9.1 Circumstances for revocation

In case of one of the circumstances listed below, Sub1- or Sub2-CA certificate MUST be revoked by the issuing CA:

- The issuing CA has reason to believe or strongly suspects that there has been a compromise of the Sub1- or Sub2-CA's private key.
- The issuing CA has reason to believe that the Sub1- or Sub2-CA has breached a material obligation, representation, or warranty under the contract between the subscriber and the issuing CA.
- The issuing CA has reason to believe that the Sub-CA certificate was issued in a manner not materially in accordance with the stipulations of this CP or the certificate was issued without the authorization of the entity. In this case, it also SHALL be checked that the issuing CA is trusted again.
- The Sub-CA's organization name expressed in the Sub-CA certificate changes.
- Other information within the Sub-CA certificate is incorrect or has changed.
- The continued use of the Sub-CA certificate is harmful to the PKI
- The termination of the business relationship between the operator of a subordinate CA and the responsible party of the respective superordinate CA SHOULD lead in the revocation of the subordinate CA

When considering whether certificate usage is harmful to the PKI, the issuing V2G Root CA considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the subscriber
- Did the Sub-CA immediately notify Hubject GmbH of a known or suspected compromise of its private key?

CA certificates MUST 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 based on a security incident MUST be confirmed by a Risk Commission.

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

4.9.2 Who MAY request revocation?

Only Hubject GmbH MUST be entitled to process the revocation of the V2G Root CA certificate, but every PKI participant MAY initiate a request for revocation.

Sub-CAs MUST be entitled, through their duly authorized representatives, to request the revocation of their own certificates at the superordinate CA, but only Hubject MUST be entitled to process the authorization.

Revocation of contract certificates: If the contract certificate has been issued by the Hubject ISO 15118 PKI, then the MO SHALL revoke the specific certificate, as enabled by the interface, deleteSignedContractData.

Revocation of provisioning certificates: Only Hubject GmbH MUST be allowed to process the revocation of a provisioning certificate, which are used for signing the contractData, but every PKI participant MAY initiate a request for revocation of provisioning certificates.

Revocation of EVSE certificates: Only the CPO SHALL process the revocation of an end-entity certificate, but every PKI participant MAY initiate a request for revocation of the EVSE leaf certificate.

Revocation of OEM provisioning certificates: Only the OEM SHALL process the revocation of an end-entity certificate, but every PKI participant MAY initiate a request for revocation of the OEM provisioning certificate.

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

For Contract Certificates MOs MUST provide a B2C interface for end customers to revoke their own Contract Certificate. Accordingly, MO Sub2-CAs MUST provide a user interface or an API to other consumer-facing systems for revocation. The MO MAY revoke a Contract Certificate too in special cases, e.g. in case of breach of the consumer contract. The authorization of the issuance process is described in Section 4.3.1.

4.9.3 Procedure for revocation request

Prior to the revocation of a Sub-CA certificate, the superordinate CA MUST verifiy that the revocation has been requested by the certificate’s subscriber according to Section 4.9.2.

The requests from Sub-CAs to revoke a Sub-CA certificate SHALL be authenticated by their superordinated entities to ensure that the revocation has in fact been requested by the respective Sub-CA. For acceptable procedures see Section 0

The revocation of end-entity certificates MUST follow the rules and processes of the respective issuing Sub2-CA and of the business context. It MUST be assured that only authenticated and authorized requests will result in revoked certificates.

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 or as defined in B2B contracts. Differences in the revocation request grace period MAY occur between CA certificates or end-entity certificates.

The Revocation Grace Period is defined in the Incident Management Process governed by the Risk Commission.

PKI Participants SHALL request revocation as soon as they identify the need for revocation and at least within twenty-four (24) hours after detecting the need for revocation.

4.9.5 Time within which CA MUST process the revocation request

CAs MUST process certificate revocation requests as quickly as practical upon receipt of an authenticated revocation request. Once a certificate has been revoked the revocation MUST be reflected in supported OCSP responses issued within one (1) hour, and in supported CRLs within twenty-four (24) hours.

The Issuer CA SHALL maintain a continuous 24/7 ability to internally respond to any high priority revocation requests.

SAE EVPKI revocation and status check obligations

To comply with SAE EVPKI CP v1.2 expectations for inter-PKI revocation behaviour, the CA SHALL ensure:

- OCSP: For CAs whose certificates are included in the SAE EVPKI CTL or which issue SECC, Contract, or Provisioning certificates trusted by EVs, an OCSP responder MUST be provided and accessible at the AuthorityInfoAccess location stated in issued certificates. OCSP responses SHOULD be fresh and reflect revocations within one (1) hour of revocation event publication when the CA operates an OCSP responder.
- CRL: The CA MUST publish CRLs for all unexpired revoked certificates and expose the CRL distribution point in the certificates cRLDistributionPoints extension. NextUpdate and CRL issuance frequency SHALL be consistent with SAE EVPKI CTL requirements and the CA's published CPS. If both OCSP and CRL are provided, the AuthorityInfoAccess entry for the OCSP responder MUST be present and accurate.
- CTL synchronisation: Hubject SHALL provide revocation metadata to the SAE EVPKI CTL operator per CTL submission requirements to ensure CTL consumers can accurately reflect certificate status.

These obligations are in addition to the Hubject timing requirements already described (OCSP 1h reflection / CRL 24h maximum latency) and, in case of any conflict the more restrictive measurement (as defined by SAE EVPKI CTL inclusion conditions) shall apply.

4.9.6 Revocation checking requirement for relying parties

The EVCC MUST verify the certificate chain of the SECCincluding certificate status check via OCSP service.

The contract certificate pool MUST verify the revocation status of all certificates that are involved in the provisioning of a new contract certificate. The revocation information MUST be retrieved either via CRLs or OCSP responders before delivering the contract certificate and related data in a CertificateInstallationRes or CertificateUpdateRes message.

Other relying parties SHOULD check the status of certificates which they rely on, as far as reasonable and feasible, via consulting the most recent CRL or the OCSP service of the CA that issued the certificate in question.

Relying parties MAY maintain a cache of the CRL locally for a period of one (1) week.

Fall-back operation: In the event certificate status checking is not available, relying parties SHOULD use the cached version of the CRL until the latest CRL can be downloaded or the online availability of the certificate status service.

4.9.7 CRL issuance frequency

In line with the OCSP update policy (see Section 4.9.9), this CP defines the following maximum update intervals for Certificate Revocation Lists (CRLs):

- **V2G Root CA:** CRLs SHALL be issued at least annually and upon any certificate revocation.
- **CPO Sub1-CA and MO Sub1-CA:** CRLs SHALL be issued at least every 7 days, and upon any certificate revocation, with a maximum interval of 4 weeks. Issuance is performed manually.
- **CPO Sub2-CA:** A complete CRL SHALL be generated and provided to the OCSP responder daily. Additionally, a delta CRL SHALL be published immediately upon any certificate status change.
- **MO Sub2-CA:** CRLs SHALL be issued automatically and online, immediately after revocation of any end-entity certificate.

General Rules

- For all end-entity certificates (except SECC certificates), CRLs containing their status MUST be updated at least every 7 days.
- A revoked certificate MUST be removed from the CRL after it has expired. This SHALL be done by default during the next full CRL generation.
- CRLs MUST be published within 24 hours of a revocation event, regardless of the normal issuance schedule.

4.9.8 Maximum latency for CRLs

The CA SHALL publish CRLs/CSSs within four (4) hours of generation, except for CA Compromise emergencies, which SHALL be published immediately, but no later than within fifteen (15) minutes of generation. Furthermore, each CRL/CSS SHALL be published no later than the time specified in the nextUpdate field of the previously issued CRL/CSS for the same scope.

4.9.9 On-line revocation/status checking availability

The V2G Root CA, CPO Sub1-CA, and CPO Sub2-CA MUST provide an Online Certificate Status Protocol (OCSP) service. Other Certification Authorities (CAs) in the PKI MAY provide OCSP services at their discretion.

All CAs SHALL maintain a web-based repository that enables relying parties to check the revocation status of certificates. CAs SHALL publish instructions for relying parties on how to locate the appropriate repository or OCSP responder for status checking.

OCSP Requirements

- An OCSP responder SHALL be available for all Sub-CA and End-Entity certificates.
- OCSP responses MUST conform to RFC 6960.
- The noCheck extension SHALL be included for CA certificates, if appropriate.
- OCSP responses SHALL be:
    - Updated at least every 24 hours;
    - Valid for no more than 48 hours;
    - For Sub-CA1 and Sub-CA2 certificates: validity MUST NOT exceed 4 minutes.
- The OCSP responder MUST return a response within 1 second for at least 99% of requests.

- OCSP responders MAY return unknown for expired certificates, if configured to do so.

Service Availability

- Online status services (OCSP, CRLs, or CSS) SHALL maintain at least 99.95% uptime.
- Scheduled maintenance downtime MUST be announced at least 30 hours in advance.
- Scheduled downtime SHALL NOT exceed:
  - Four (4) hours per calendar week, and
  - Sixteen (16) hours per calendar year.

4.9.10 On-line revocation checking requirements

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].

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.

All relying parties MUST check the status of certificates which they rely on by using the path validation algorithm in Section 6 of [RFC 5280].

If a Relying Party does not check the status of a certificate by consulting the most recent CRL, the Relying Party MUST check the certificate status by consulting the applicable online Repository or by requesting certificate status using the applicable OCSP responder.

4.9.11 Other forms of revocation advertisements available

No stipulations.

4.9.12 Special requirements regarding key compromise

See Section **Error! Reference source not found.**.

The CA SHALL notify its senior management in the event of Compromise, or suspected Compromise, of the CA's Private Key.

PKI participants SHALL be notified of an actual or suspected CA private key compromise. The responsible parties at the subsequent CAs MUST be notified using commercially reasonable efforts.

4.9.13 Circumstances for suspension

PKI MUST not support suspension services for CA or end-user subscriber certificates. The revocation of a certificate MUST be irreversible.

4.9.14 Who can request suspension?

Not applicable, see 4.9.13.

4.9.15 Procedure for suspension request

Not applicable, see 4.9.13.

4.9.16 Limits on suspension period

Not applicable, see 4.9.13.

4.10 Certificate status service

The PKI MUST include a service that provides status information about certificates on behalf of a CA through online transactions (i.e., CRLs and OCSP). Where the certificate status service is identified in certificates as an authoritative source for revocation information or issued a delegated responder certificate, the operations of that authority are considered within the scope of this CP. A certificate status service SHALL assert all the policy OIDs for which it is authoritative, including OCSP servers that are identified in the Authority Information Access (AIA) extension.

The certificate status service is considered an integral part of the CAs and, except where expressly noted, all requirements imposed on CAs apply.

4.10.1 Operational characteristics

The status of V2G Root CA certificates MUST be publicly available. The V2G Root CA publishes this information via the Hubject PKI website https://www.hubject.com/pki/
The status of Sub CA certificates MUST be available via CRL through a CAs website (at a URL specified in the CAs CP), web-based repository and via an OCSP responder (where available).

The status of end-entity certificates MUST be available via CRL, through a web-based repository, and via an OCSP responder (where available).

A certificate status service SHALL meet the following requirements:

- The certificate status service SHALL be operated in compliance with this CP;
- Information exchanged between the CA and the certificate status service SHALL be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificate being issued;
- Accurate and up-to-date information from the associated CA SHALL be used to provide the revocation status;

4.10.2 Service availability

Certificate status services SHALL be available 24x7 without scheduled interruption.

4.10.3 Optional features

No stipulations.

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.

For certificates that have expired prior to or upon end of the Subscriber’s agreement, revocation is not required.

CAs SHALL always revoke unexpired certificates at the end of the subscription.

4.12 Key Escrow and Recovery

Key escrow and recovery are not permitted for the PKI.

4.12.1 Key escrow and recovery policy and practices

Not applicable, see 4.12.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable, see 4.12.

5 Physical, Procedural and Personnel Security Controls

All entities performing CA functions SHALL implement and enforce the following physical, procedural, logical, and personnel security controls for a CA. If a PKI relies on a cloud-based CA, it MUST meet all control requirements.

5.1 Physical Controls

The CA SHALL physically protect all CA equipment, including cryptographic modules from theft, loss, and unauthorized access as specified in Section 5.1.2. Unauthorized use of CA equipment is prohibited. The CA SHALL dedicate CA equipment to performing CA functions only.

The CA SHALL implement physical access controls to reduce the risk of equipment tampering, even when the cryptographic module is not installed and activated.

All the CA physical control requirements specified below apply equally to the Root CA and Sub-CAs.

CAs of the PKI MUST implement physical, procedural and personnel security controls.

5.1.1 Site location and construction

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

The CA SHALL select its site location and construction, so that when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, it SHALL provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical access

The CA SHALL have physical Access Controls for CA equipment, as well as remote workstations used to administer the CAs, to:

- Protect all CA equipment from unauthorized access;
- Electronically monitor CA equipment for unauthorized intrusion;
- Ensure an access log is maintained and available for inspection;
- Store all removable media and paper containing sensitive plain-text information in secure containers; and
- require multi-person physical access control to both the cryptographic module and computer systems.

The CA SHALL place all removable cryptographic modules and the activation information used to access or enable cryptographic modules in secure containers when not in use. Activation data SHALL be either memorized or recorded and stored in a manner commensurate with the security afforded by the cryptographic module, and SHALL NOT be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA. Access to the contents of the locked containers SHALL be restricted to individuals holding CA trusted roles, as defined in section 5.2.1, utilizing multi-person access controls, and multi-person integrity while the container is unlocked.

When in active use, the cryptographic module SHALL be locked into the system or container (rack, reader, Server, etc.) using a physical lock under the control of the CA operations staff to prevent unauthorized removal. A security check of the CA facility, or remote workstations used to administer the CAs, SHALL occur prior to leaving the CA facility unattended. The check SHALL verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open,” and secured when “closed,” and for the CA, that all equipment other than the repository/CSS is shut down);
- Any containers housing the cryptographic module are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

The RA SHALL protect its RA equipment from theft, loss, and unauthorized access.

5.1.3 Power and air conditioning

The secure facilities of CAs of the PKI MUST be equipped with primary and Backup power systems to ensure continuous (i.e., 24x7), uninterrupted Access to electric power sufficient for the operations of its Server and network connections to meet its service level agreements and also sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically in case of a shutdown. Also, 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 PKI MUST be protected against water exposure. For this reason, water and soil pipes MUST be avoided.

Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire prevention and protection

The secure facilities of CAs of the PKI MUST be constructed and equipped, and procedures SHALL be implemented, to prevent damaging exposure to flame or smoke.

The fire prevention and protection measures SHALL meet all local applicable safety regulations.

5.1.6 Media storage

CAs of the 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.

The CA SHALL store media not required for daily operation, or not required by policy, to remain with the CA that contains security audit, archive, or backup information in a securely stored location separate from the CA equipment.

5.1.7 Waste disposal

CAs of the 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.

Destruction of media and documentation containing sensitive information, such as Private Key material, SHALL employ methods commensurate with those in the NIST Guidelines for Media Sanitization [SP 800-88-1].

5.1.8 Off-site backup

CAs of the 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 the higher or high level of security as the main location, as it is responsible for the back-up and not fail-over. 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 Persons”. Persons seeking to become Trusted Persons by obtaining a Trusted Position MUST meet the screening requirements of this CP.

Trusted Persons 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 Persons 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
- Executive Management that are designated to manage infrastructural trustworthiness.

The definition of the roles involved, and the role exclusions MUST be described in a Rights and Role concept as part of the CAs CPS.

5.2.2 Number of persons required per task

CAs of the PKI MUST establish, maintain, and enforce rigorous control procedures to ensure the separation of duties based on job responsibility and to ensure that multiple Trusted Persons 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, such as access to and management of CA cryptographic hardware (HSM) and associated key material require multiple Trusted Persons.

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

Access to CA cryptographic hardware MUST be strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device.

Other manual operations such as the validation and issuance of CA certificates require the participation of at least two Trusted Persons as described in Section 6.2.2 Private Key (n out of m) multi-person control.

5.2.3 Identification and authentication for each role

Individuals assigned to trusted roles SHALL be appointed to the trusted role by an appropriate approving authority within the organization managing the trusted roles. Identity proofing of trusted roles SHALL be performed by the approving authority. The identity proofing of the RA SHALL be performed by the CA. Verification of identity SHALL include the personal (physical) presence of such personnel before human resources or other personnel performing security functions through either a face-to-face meeting or through a trusted video conferencing process approved by the PA and a check of well-recognized forms of identification, such as passports and driver’s licenses. These appointments SHALL be annually reviewed for continued need. Any necessary security checks, as defined by the PA and/or the approving authority, for trusted role appointments/approvals SHALL also be performed annually. If a continued need of these appointments is identified and all defined security checks pass, the appointment MAY be Renewed, if appropriate. The CA or RA SHALL record the trusted role approvals and renewals in a secure and auditable fashion. Individuals holding trusted roles SHALL accept the responsibilities of the trusted role in writing, and the CA or RA SHALL record this acceptance in a secure and Auditable fashion.

CAs or RAs SHALL confirm the identity and authorization of all personnel seeking to become trusted persons before such personnel are:

- Issued access devices and granted access to the required CA facilities; and
- Given electronic credentials to access and perform specific functions on CA systems.

CA equipment SHALL require, at a minimum, multi-person authenticated access control for remote access using multi-factor authentication. Examples of multi-factor authentication include: use of a

password or PIN along with a time-based token, digital certificate, or other device that enforces a policy of what a user has and what a user knows.

5.2.4 Roles requiring separation of duties

An individual that performs any Trusted Role SHALL only have one identity when accessing CA or RA equipment. The

CA and RA SHALL have procedures to ensure that no user identity can assume multiple roles.

CA Roles requiring separation of duties include, but are not limited to, the:

- CA Operations Staff:
    - Acceptance, rejection, or other processing of certificate applications, revocation requests, Renewal requests, or enrolment information;
    - Issuance or revocation of certificates, including personnel having access to restricted portions of the Repository;
    - Generation, issuance, or destruction of a CA certificate private key;
- CA Administration Staff:
    - Generation of CA backups;
    - Loading of a CA to a production environment; and
    - Security auditor role.

RA Roles requiring separation of duties include, but are not limited to, the:

- RA Operations Staff:
    - Acceptance, rejection, or other processing of certificate applications, revocation requests, renewal requests, or enrolment information;
    - Generation, issuance, or destruction of a subscriber or Sub-CA certificate private key;
- RA Administration Staff:
    - Generation of RA backups;
    - Loading of a RA to a production environment; and
    - Security auditor role.

Role separation, when required as mentioned above, MAY be enforced by either the CA or RA equipment, or procedurally, or by both means.

5.3 Personnel Controls

Personnel controls plays a critical role in the PKI's overall system security to prevent unauthorized Access to CA and RA systems and CA/RA operations.

5.3.1 Qualifications, experience, and clearance requirements

CAs and RAs MUST require that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any Trusted Role SHALL:

- Have no other duties that would interfere or conflict with their responsibilities, as defined in Section 5.2.1;
- Have demonstrated the ability to perform their duties;
- If necessary, have successfully completed the appropriate training;
- Have not been previously relieved of trusted role duties for reasons of negligence or non-performance of duties (e.g., unauthorized disclosure of confidential information, theft, embezzlement, destruction of property, etc.);
- and do not have any other disqualifications as documented by the CA in its CPS.

The gathered information MUST be documented and archived.

5.3.2 Background check procedures

CAs and RAs MUST conduct background checks for personnel seeking to become trusted persons. Background checks SHALL be done with every new team member joining the team, the background check SHALL follow the 4-eye principles and SHALL be documented. Background checks SHALL be repeated for personnel holding Trusted Positions at least every five (5) years, also these background checks SHALL follow the 4-eye principles and SHALL be documented. Background checks SHALL be done for job rotation scenarios, with every new team member joining the team, also these background checks SHALL follow the 4-eye principles and SHALL be documented.

The factors revealed in a background check that MAY be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing trusted person include (but are not limited to) the following:

- Misrepresentations made by the candidate or trusted person,
- Highly unfavourable or unreliable professional references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information SHALL be evaluated by human resources and such personnel SHALL take actions that are reasonable in light of the type, magnitude, and frequency of the behaviour uncovered by the background check. Such actions MAY include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing trusted persons. The use of information revealed in a background check to take such actions SHALL be subject to applicable law.

Background investigation of persons seeking to become a trusted person includes but is not limited to:

- a confirmation of previous employment,

- a check of professional references,
- a confirmation of the highest or most relevant educational degree obtained,
- a search of criminal records.

CAs and RAs SHALL have a process in place to ensure employees in Trusted Roles undergo background checks at least every ten (10) years.

The gathered information MUST be documented and archived.

5.3.3 Training requirements

CAs of the PKI MUST provide their personnel with the requisite training needed to perform their job responsibilities related to CA operations competently and satisfactorily.

They SHALL also periodically review their training programs, and their training SHALL address the elements relevant to functions performed by their personnel.

Training programs MUST address the elements relevant to the particular environment of the person being trained, including:

- Security principles and mechanisms of the PKI of the CA,
- Hardware and software versions in use,
- All duties the person is expected to perform,
- Threat detection and incident handling
- Incident and Compromise reporting and handling,
- Disaster recovery and business continuity procedures.

The dates, contents of the training courses and the names of the participants MUST be documented and archived.

5.3.4 Retraining frequency and requirements

The persons assigned to trusted roles MUST continuously refresh their knowledge gained in the training using a training environment. Furthermore, trainings SHALL be repeated whenever deemed necessary but at the latest after one year. The participation in the training MUST be documented and archived.

CAs and RAs SHALL provide refresher training and updates to their staff to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily. The participation in the training MUST be documented and archived.

5.3.5 Job rotation frequency and sequence

No stipulations.

5.3.6 Sanctions for unauthorized actions

A formal disciplinary process MUST be defined by the CAs, ensuring that unauthorised actions are appropriately sanctioned. In severe cases, the role assignments and corresponding privileges MAY be withdrawn.

5.3.7 Independent Contractor Requirements

CAs of the PKI MAY permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly defined outsourcing relationships and only under the following conditions:

- the entity using the independent contractors or consultants as Trusted Persons does not have suitable employees available to fill the roles of Trusted Persons, and
- the contractors or consultants are trusted by the entity to the same extent as if they were employees.

Otherwise, independent contractors and consultants SHALL have access to PKI secure facility only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel

CAs of the PKI SHALL provide their personnel with the requisite training and access to other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

The types of auditable events that MUST be recorded by CAs and RAs of the 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 EoL+5 years of the CA-Lifetime.

CAs of the PKI SHALL state in their Certificate Practice Statement the logs and types of events they record.

5.4.1 Types of events recorded

Every CA and RA MUST keep several kinds of audit logs which include, but are not limited to:

- All relevant information that is created during processing automatic requests to the CA is stored in a database. In particular, this includes received request messages as well as issued certificates and information about errors during processing of a request.
- Furthermore, every CA collects internal information about its operation. In particular, this records errors that MAY affect the proper and secure operation of the CA.
- Checklists, forms, etc. regarding the audits for Sub CA audits and certification

In particular, these events must be recorded:

- Physical access to CA/RA Facility
    - Personnel access to room housing CA/RA equipment

  - Access to the CA/RA Server
  - Known or suspected violations of physical security
  - Any removal or addition of equipment to the CA/RA enclosure
- System Configuration:
  - Installation of the operating system
  - Installation of the CA/RA software
  - Installation and removal of hardware cryptographic modules
  - System start-up
  - Any security-relevant changes to the configuration of the CA/RA
  - CA/RA hardware configuration
  - System configuration changes and maintenance
  - Cryptographic module life cycle management-related events (e.g., receipt, use, de-installation, and retirement)
- Account administration:
  - Roles and users are added or deleted
  - The access control privileges of a user account or a role are modified
  - Appointment of an individual to a trusted role
  - Designation of personnel for multi-person control
  - System administrator accounts
  - Attempts to create, remove, set passwords or change the system privileges of the privileged users (trusted roles)
  - Attempts to delete or modify audit logs
  - Changes to the value of maximum authentication attempts
  - Resetting operating system clock
- CA/RA Operational Events:
  - Key generation
  - Start-up and shutdown of CA/RA systems and applications
  - Changes to CA/RA details or keys
  - Records of the destruction of media containing key material, activation data, or personal subscriber information
  - Successful and unsuccessful attempts to log into the CA/RA system
  - The value of maximum authentication attempts is changed

  - Maximum unsuccessful authentication attempts occur during user login
  - A CA/RA administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
  - Attempts to set passwords
  - Attempts to modify passwords
- Certificate Life Cycle Events:
  - Certificate application requests
  - Certificate requests
  - Issuance
  - Refusal to issue certificates
  - Re-Key
  - Renewal
  - Certificate revocation requests
  - Revocation
- Trusted Person Events:
  - Logon and logoff to the CA/RA system
  - Attempts to create, remove, set passwords or change the system privileges of the privileged users
  - Unauthorized attempts to access the CA/RA system
  - Unauthorized attempts to access system files
  - Failed read and write operations on the certificate
  - Personnel changes
  - RA certificates
- Data Events:
  - Any attempt to delete or modify the audit logs
  - All successful and unsuccessful requests for confidential and security-relevant information

Each audit record MUST include the following information (either recorded automatically or manually for each Auditable event):

- The type and description of event;
- The date and time the event occurred;
- Success or failure; and

- The identity of the entity and/or person that caused the event.

5.4.2 Frequency of processing log

The CA SHALL review the Audit log at least once every sixty (60) days, unless the CA is offline, in which case the Audit logs SHALL be reviewed when the system is activated or every sixty (60) days, whichever is later.

The RA SHALL review its Audit logs at least once per quarter.

The CA and RA Compliance Audit reviews SHALL involve verifying that the logs have not been tampered with, that there is no discontinuity or other loss of Audit Data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.

Audit logs SHALL be reviewed manually and automatically in response to alerts based on irregularities and incidents within their CA systems.

Audit log processing SHALL consist of a review of the audit logs and documenting the reason for all unexpected events in an audit log summary.

Audit log MUST be archived at least weekly. An administrator MUST perform a manual archival if the free disk space for audit log is below the expected amount of audit log data produced for one week.

5.4.3 Retention period for audit log

The CA and RA SHALL retain audit logs for at least ten (10) years and thereafter MAY be archived.

The Security Auditor SHALL be the only entity who removes audit logs from the CA or RA system.

The CA and RA SHALL make all audit logs, both electronic and non-electronic, available during a compliance audit.

Log records related to certificate life cycles MUST be kept at least two years after the corresponding certificate expires. Legal regulations MAY require a longer period of archival.

5.4.4 Protection of audit log

Confidentiality of the audit log MUST be guaranteed by a role-based access control mechanism. Internal audit logs MAY only be accessed by administrators and the Log Auditor representing the legal department.

The CA and RA SHALL protect audit logs from unauthorized viewing (i.e., viewing without permission from the CA, RA, or security auditor), modification, deletion, or other tampering. CA and RA system configuration and procedures SHALL be implemented together to ensure that only authorized people archive or delete audit logs. The CA and RA SHALL implement procedures to protect archived data from deletion or destruction.

System configuration and operational procedures SHALL be implemented together by the CA/RA to ensure that:

- Only authorized personnel (i.e., CA, RA, or Security Auditor) have read access to the logs;
- Only authorized personnel (i.e., CA, RA, or Security Auditor) MAY archive audit logs;
- Audit logs are not modified; and
- Audit logs are stored in a secure storage.

Certificate-life-cycle-related audit logs MAY also be accessed by users with the appropriate authorization.

5.4.5 Audit log backup procedures

Incremental backups of audit logs MUST be created daily and full backups MUST be performed weekly.

In the case of an offline CA Audit logs and Audit summaries SHALL be backed up every time the system is activated, or at least every thirty (30) days.

5.4.6 Audit collection system (internal or external)

The Audit log collection system MAY or MAY NOT be external to the CA or RA system.

Where possible, the Audit logs SHALL be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism SHALL be used. Automated Audit processes SHALL be invoked at system or application start-up and cease only at system or application shutdown.

It SHALL NOT be possible to terminate automated Audit logging processes while the CA/RA system is powered ON or still running.

Audit collection systems SHALL be configured such that the Audit log is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated Audit system has failed; affected CA (or RA) operations, except

Revocation status services, SHALL be suspended until the Audit capability can be restored.

5.4.7 Notification to event-causing subject

If anomalies occur, a check MUST be carried out, the CA's responsible persons MUST be informed, and an analysis carried out

5.4.8 Vulnerability assessment

Vulnerability analysis of all IT equipment of CAs of the PKI MUST be performed daily by technical means. From an organizational point of view, vulnerability analysis 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 PKI MUST archive:

- All audit data collected in terms of Section 5.4.
- certificate application information
- Documentation supporting certificate applications
- certificate lifecycle information e.g., creation, revocation, rekey and renewal application information

At a minimum, the following data SHALL be recorded and retained:

- CP releases

- CAs issued and key generation
- Export of CA Private Keys
- CPS reviews
- Contractual obligations
- Modifications and updates to CA system or configuration
- Subscriber identity verification data
- CRL issuance
- All certificates issued, Re-Keyed, Renewed, and Revoked
- Audit logs
- Compliance Auditor reports
- Any attempt to delete or modify the Audit logs
- Remedial action taken as a result of violations of physical security
- certificate request documentation
- Appointment of an individual to a Trusted Role
- Destruction of Cryptographic Modules
- All certificate Compromise notifications

Audit log MUST be archived regularly as described in Section 5.4.5.

All manual decisions and contracts MUST be archived in digital and OPTIONAL in physical form.

5.5.2 Retention period for archive

As long as no legal regulations require a longer archival period, certificate requests and issued certificates MUST be maintained at least two years after the corresponding certificate has expired.

5.5.3 Protection of archive

CAs of the PKI maintaining an archive of records MUST protect the archive in a way, that only the entity's authorized Trusted Persons are able to obtain access to the archive. The archive MUST be protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data SHALL be maintained to ensure that the archive data can be accessed for the time period set forth in this CP.

5.5.4 Archive backup procedures

Entities compiling electronic information SHALL incrementally back up system archives of such information on a daily basis and perform full backups on a weekly basis. Copies of paper-based records SHALL be maintained in an off-site secure facility.

5.5.5 Requirements for timestamping of records

Certificates, CRLs, and other revocation database entries MUST contain time and date information. Such time information SHOULD not be cryptographically based.

The CA and RA SHALL describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive collection system (internal or external)

The internal archive collection system MUST be internal on Hubject GmbH site. In addition, the external archive collection MUST be stored in a trusted safe which MUST offer the higher level of security as the main location.

5.5.7 Procedures to obtain and verify archive information

Only authorized Trusted Personnel MUST be able to obtain access to the archive. The integrity of the information MUST be verified when it is restored.

After receiving a request made for a proper entity, its agent, or a party involved in a dispute over a transaction involving the PKI, the CA or RA MAY elect to retrieve the information from its Records system. The CA/RA SHALL verify the Integrity of the Records information. The CA/RA MAY elect to transmit the relevant information via a secure electronic method or courier.

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 be generated. This process MUST be handled as a new certification application. The new CA certificate MUST be published immediately as specified in Section 2.2.

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

The CA's Private Key SHALL have a validity period as described in Section 6.3.2 and MAY be re-keyed at any time during its validity Period, as per Section 4.7.

If a Sub-CA is to be re-keyed, the Sub-CA SHALL generate a new public-private key pair and submit a CSR to the superordinated CA to request its Sub-CA certificate. The Sub-CA SHALL notify entities relying on its certificate that its CA certificate has been re-keyed. The superordinated CA MAY publish the issued CA certificate in its repository. The new Sub-CA private key is used to re-sign all active End-Entity certificates it has issued.

When the Root CA certificate is to be re-keyed, the Root CA SHALL generate a new key pair and two key rollover certificates:

- One key rollover certificate where the new Public Key is signed by the old private key, indicating that this is the new Root CA public Key; and
- The other key rollover certificate where the old public Key is signed with the new private Key, indicating that this is the old public key being replaced.

The new Root CA certificate SHALL be available for download from the new Root CA's repository. The relying party SHOULD validate both certificates and replace the old Root CA certificate with the

published new Root CA certificate. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users.

The new Root CA private key SHALL be used to re-sign all existing active Tier-1 CAs. There is no need to re-sign existing active Sub-CA or End-Entity certificates issued by the Tier-1 CA, unless the Tier-1 CA is also re-keyed.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling

The CA and RA SHALL have an Incident Response Plan and a Disaster Recovery Plan (DRP).

If compromise of a CA private key is suspected, the CA SHALL stop certificate issuance and follow the procedures outlined in Section 5.7.3. The CA SHALL assess the scope of potential damage in order to determine appropriate remediation procedures.

The CA SHALL notify its superior entity if it experiences one or more of the following:

- Suspected or detected compromise (including compromise of the CA's private key) of the CA systems;
- Physical or electronic penetration of CA systems;
- Any incident preventing the CA from issuing a CRL within twenty-four (24) hours of the issuance of the previous CRL; or
- Any incident preventing the CA from updating the CSS within fifteen (15) minutes of performing an operation on the CA.

The CA SHALL re-establish operational capabilities quickly as possible.

If an incident is detected or the CA system is compromised, the responsible authority and Trusted Persons within Hubject GmbH MUST be informed immediately.

5.7.2 Computing resources, software and/or data are corrupted

If a disaster is discovered that prevents the proper operation of a CAs operating under this CP the CA SHALL respond as follows:

- Notify its Superior entity Sub-CAs, and any cross certified CAs as soon as possible;
- Ensure that the system's Integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of Backup;
- Re-establish CA operations, giving priority to the ability to generate certificate status information within the CSS and CRL issuance schedule;
- If the CA private keys are not destroyed, CA operation SHALL be re-established, giving priority to the ability to generate certificate status information within the CSS and CRL issuance schedule;
- If the CA private keys are destroyed, re-establish CA operations as quickly as possible, giving priority to the generation of a new CA Key Pair;

- If the integrity of the system cannot be restored, or if the Risk is deemed substantial, re-establish system integrity before returning to operation;
- If a CA cannot issue a CRL prior to the time specified in the nextUpdate field of its currently valid CRL, then all CAs that have been issued certificates by the CA SHALL be securely notified immediately. This will allow other CAs to protect their subscribers' interests as relying parties;
- If the CA cannot, within fifteen (15) minutes of corruption of computing resources, software, and/or data, correctly reflect the status of certificates issued by the CA, then all CAs that have been issued certificates by the CA SHALL be securely notified immediately. This will allow other CAs to protect their subscribers' interests as relying parties; and
- If the ability to revoke certificates is inoperative or damaged, the CA SHALL re-establish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. If the CA's revocation capability cannot be established in the time-frame specified in the CPS, the CA SHALL determine whether to request revocation of its certificate(s). If the CA is a Root CA, the CA SHALL determine whether to notify all subscribers using the CA as a trust anchor to delete the trust anchor., only 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 of the last 10 days MUST be restored enabling the continuation of operation.

The corruption of computing resources, software, and/or data MUST be reported to the V2G Root CA. See Section 1.5.2 Contact person

5.7.3 Entity private key compromise procedures

If the CA can obtain accurate information on the certificates it has issued which are still valid (i.e., not expired or Revoked), the CA MAY re-issue (i.e., Renew) those certificates with the notAfter date in the certificates remaining the same as in original certificates; and if the CA is a Root CA, it SHALL provide all relying parties with the new Trust Anchor using secure means.

The CPS SHALL specify the maximum time during which these procedures MUST be completed.

5.7.3.1 Root CA Compromise Procedures

In the case of the Root CA Compromise, the Root CA SHALL notify:

- The PA;
- Any Tier-1 CAs; and
- relying parties so they can remove the trusted self-signed Root CA certificate from their trust stores.

Notification SHALL be made in an authenticated and trusted manner. Initiation of notification to the PA SHALL be made at the earliest feasible time, which SHALL NOT be longer than the time specified in the CPS and no longer than twenty-four (24) hours, beyond the determination of Compromise or loss unless otherwise required by law enforcement. Initiation of notification to relying parties and

Subscribers MAY be made after remediations are in place to ensure continued operation of applications and services. If the cause of the Compromise can be adequately addressed, and it is determined that the PKI can be securely re-established, the Root CA SHALL then generate a new Root CA certificate, solicit requests and issue new Tier-1 CA certificates, securely distribute the new Root CA certificate and two key rollover certificates (see **Error! Reference source not found.**). Tier-1 CAs SHALL follow the procedure for Sub-CA Compromise for their issued certificates.

5.7.3.2 SubCA Compromise Procedures

In the event of a CA key Compromise, the CA SHALL notify the PA, its Superior Entity, and any lower level Sub- CAs. The superordinated CA SHALL revoke the compromised CA's certificate, and the revocation information SHALL be published via a CRL, if supported, or via an emergency certificate status service update immediately in the most expedient, Authenticated, and trusted manner after the notification. The Compromised CA SHALL also investigate and report to the PA, superordinated CA (if applicable) and any lower level Sub-CAs what caused the Compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the Compromise can be adequately addressed and it is determined that the CA can be securely re-established, then, the CA SHALL be re-established. Upon re-establishment of the CA, new Sub-CA (if applicable) and Subscriber certificates SHALL be requested and issued.

5.7.3.3 certificate status service Compromise Procedures

In case of a certificate status service key Compromise, the CA that issued the certificate status service certificate SHALL revoke that certificate, and the revocation information SHALL be published via a CRL, if supported, or via an emergency CSS update immediately in the most expedient, authenticated, and trusted manner. The certificate status service SHALL subsequently be Re-Keyed.

5.7.3.4 RA Compromise Procedures

In case of a RA Compromise, the CA SHALL disable the RA. In the case a RA's key is compromised, the CA that issued the RA certificate SHALL revoke it, and the revocation information SHALL be published in the most expedient, authenticated, and trusted manner. The compromise SHALL be investigated by the CA in order to determine the actual or potential date and scope of the RA compromise. All certificates approved by that RA since the date of actual or potential RA compromise SHALL be revoked. In the event that the scope is indeterminate, then the CA compromise procedures in this section SHALL be followed.

5.7.3.5 Subscriber Compromise Procedures

When a subscriber certificate is revoked because of compromise, suspected compromise, or loss of the private key, the CA SHALL publish a revocation notice via a CRL, if supported, or via a CSS update at the earliest feasible time.

5.7.4 Business continuity capabilities after a disaster

PKI entities operating secure facilities for CA operations develop, test, maintain and, if necessary, MUST implement a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster. Disaster recovery plans address the restoration of information systems services and key business functions.

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, entities SHALL be given as much advance notice as circumstances permit.

Prior to CA termination, and in coordination with its Superior Entity, the CA SHALL:

- Provide notice to its Superior CA;
- Provide notice to all Cross certified CAs and request revocation of all certificates issued to it;
- Issue a CRL revoking all unexpired certificates prior to termination. This CRL SHALL be available until all certificates issued by the CA expire;
- Archive all Audit logs and other Records prior to termination;
- If a Root CA is terminated, use secure means to notify the Subscribers to delete all Trust Anchors representing the terminated CA;
- If necessary, transfer the CRL/CSS service to its Superior Entity;
- Destroy all Private Keys upon termination; and
- Archive Records SHALL be transferred to an appropriate authority specified in the CPS.

Before terminating RA activities, the RA SHALL:

- Provide notice and information about the termination by sending notice by email to Subscribers, relying parties, and cross certifying entities and by posting such information on its web site; and
- Transfer all responsibilities to a successor designated by the CA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

CA and certificate status service keys MUST be generated during a Key Generation Ceremony in a hardware security module (HSM) following the standards specified in Section 0. The key ceremony MUST be documented, and the documentation MUST be archived.

Key Pair generation SHALL be performed using at a minimum the FIPS 140-2 Level described in the table below for the hardware cryptographic modules and key pair generation processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys.

Entity	Minimum Level	Hardware or Software	Key storage restricted to the module on which the key was generated
Root CA certificate	FIPS 140-2 Level 3+	Hardware	Yes
Sub CA certificate	FIPS 140-2 Level 3+	Hardware	Yes
certificate status service	FIPS 140-2 Level 3+	Hardware	Yes
End-Entity certificate	FIPS 140-2 Level 1+	Hardware or Software	No stipulation

CAs SHALL generate CA key pairs in a Key Generation Ceremony, using multi-person control, and HSMs validated to the minimum FIPS level specified in Table above. The CA's Key Pair generation MUST create a verifiable audit trail demonstrating that the security requirements for the procedure were followed. The CA's documentation of the procedure MUST show that appropriate role separation was used. One or more witnesses SHALL validate the execution of the key generation procedures by witnessing the key generation and examining the signed and documented record of the key generation.

Subscribers/End-Entities, or their Authorized entity, SHALL perform Key Pair generation by using a FIPS-approved method or equivalent international standard and either a validated hardware or software Cryptographic Module, as shown in table above

6.1.2 Private key delivery to subscriber

End-entity 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). If the keys are generated outside the subjected device, the private Keys MUST be delivered securely to the Subscriber and:

- The entity who generates a Private Key for a Subscriber SHALL not retain any copy of the key after delivery of the Private Key to the Subscriber;
- The Private Key SHALL be protected from activation, compromise, or modification during the delivery process; and
- Delivery SHALL be accomplished in a way that ensures that the certificates and associated Private Keys are provided to the correct subscriber.

6.1.3 Public key delivery to certificate issuer

Public keys generated by subscribers MUST be delivered to the certificate issuer through the PKCS#10 Requests. The RA SHALL verify the subscriber's identity and deliver the subscriber's Public Key to the CA. The RA SHALL Authenticate to the CA and send the Public Key CSR file to the CA to request a certificate on behalf of the subscriber.

6.1.4 CA public key delivery to relying parties

The public key and the certificate of the V2G Root CA MUST be stored by every Sub-CA and end-entity of the PKI. The subscriber SHALL use a second communication channel for validating the V2G Root CA Certificate fingerprint, before installing it at the end-entities resp. storing it at the Sub-CA.

6.1.5 Key sizes

The curve secp256r1 (NIST P-256) MUST be used for generating the keys. The private/public key lengths MUST be 256 bits.

The issuing CA MUST approve the key size selection for requested CA.

6.1.6 Public key parameters generation and quality checking

Generation of CA keys MUST take place in appropriate HSM (min. FIPS 186-2).

Public key parameters (algorithm and length) for CA keys MUST be verified by the issuing CA.

End-entity public key parameters (algorithm and length) MUST be verified by the issuing CA, so that no non-compliant algorithm and key length can be used. In case of key generation by the issuing CA, the key parameters SHOULD be fixed and reported in the CA configuration or verified and authorized in the request, as applicable. Requests with non-compliant algorithm and key length MUST be rejected.

6.1.7 Key usage purposes

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 0.

6.1.7.1 keyUsage Extension for CA certificates

The table below shows the specific keyUsage extension settings for CA certificates (i.e., Root CAs, Sub-CAs) and specifies that all CA certificates:

- SHALL include a keyUsage extension;
- SHALL set the criticality of the keyUsage extension to TRUE;
- SHALL assert the digitalSignature bit.
- SHALL assert the nonrepudiation bit.
- SHALL assert the keyCertSign bit; and
- SHALL assert the cRLSign bit.

Field	Format	Critical	Value	Comment
keyUsage	Bit String	True	{ id-ce 15 }	Included in all CA certificates
digitalSignature	(0)		1	Set*
nonRepudiation	(1)		1	Set*
keyEncipherment	(2)		-	Depends on use case
dataEncipherment	(3)		0	Not set
keyAgreement	(4)		0	Not set
keyCertSign	(5)		1	Set
cRLSign	(6)		1	Set

encipherOnly	(7)		0	Not set
decipherOnly	(8)		0	Not set

**Deviation from SAE EVPKI v1.1/1.2: While SAE defines the digitalSignature and nonRepudiation key usage bit as set (1) for the CSO Sub-CA1 and Sub-CA2 certificate, Hubject has not set (0) the value of the fields in the certificate profiles, in accordance with best practice of PKI operation (reference: RFC5280 - CA certificates SHOULD NOT assert the digitalSignature or nonRepudiation bits.).*

6.1.7.2 keyUsage Extension for all End-Entity certificates

The table below shows the specific keyUsage extension settings for End-Entity certificates and specifies that all End-Entity certificates:

- SHALL include a keyUsage extension;
- SHALL set the criticality to TRUE; and
- SHALL set the digitalSignature, nonrepudiation, and keyAgreement bits.

Field	Format	Criticals	Value	Comment
keyUsage	Bit String	True	{ id-ce 15 }	Included in all End-Entity certificates
digitalSignature	(0)		1	Set
nonRepudiation	(1)		0	Set
keyEncipherment	(2)		-	Depends on use case
dataEncipherment	(3)		0	Not set
keyAgreement	(4)		1	Set
keyCertSign	(5)		0	Not set
cRLSign	(6)		0	Not set
encipherOnly	(7)		0	Not set
decipherOnly	(8)		0	Not set

6.1.7.3 keyUsage Extension for all OCSP Responder certificates

The table 10 shows the specific keyUsage extension settings for OCSP responder certificates and specifies that all OCSP responder certificates:

- SHALL include a keyUsage extension;
- SHALL set the criticality of the keyUsage extension to TRUE; and
- SHALL assert the digitalSignature bit.

Field	Format	Criticals	Value	Comment
keyUsage	Bit String	True	{ id-ce 15 }	Included in all OCSP Responder certificates
digitalSignature	(0)		1	Set
nonRepudiation	(1)		0	Not set
keyEncipherment	(2)		0	Not set
dataEncipherment	(3)		0	Not set
keyAgreement	(4)		1	Not set
keyCertSign	(5)		0	Not set
cRLSign	(6)		0	Not set
encipherOnly	(7)		0	Not set
decipherOnly	(8)		0	Not set

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Private Key holders SHALL take necessary precautions to prevent the loss, disclosure, Modification, or unauthorized use of their Private Keys in accordance with this section of this CP.

6.2.1 Cryptographic module standards and controls

For key generation for CA keys and CA-related devices like CRL- or OCSP signer, appropriate HSMs MUST be used, which are 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

End-Entity keys SHOULD be generated in a device with

- CSPRNG (Cryptographically Secure Pseudo Random Number Generator) with min. function call PTG.2 to acc. to BSI, deterministic
- Minimal PTG.2 for Sub CA 1 and Sub CA 2 certificates
- Minimal DRG 3 for leaf / end-entity certificates
- All key storage MUST be hardware isolated
- Must be recognisable in the attribute in certificate.

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

Multi-person controls MUST be enforced to protect the private key or activation data, which is needed to activate, back-up or recover CA private keys. CAs of the PKI MUST use “secret sharing” to split the private key and/or activation data needed to operate the private key into separate parts called “secret shares”, which are held by individuals. For the Root CA a six-eyes principle, for subordinated CAs a four-eyes principle MUST be implemented as a minimum.

Access to CA Private Keys backed up for disaster recovery SHALL be under multi-person control.

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

6.2.4.1 Backup of CA Private Keys

One or more copies of all active and non-active private CA keys MUST be stored on dedicated backup media or in dedicated HSM devices. This backup procedure 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

6.2.4.2 Backup of End-Entity Private Keys

Subscriber private keys MAY be backed up or copied but SHALL be held under the control of the Subscriber or other authorized administrator. Subscriber backed up private keys SHALL NOT be stored in plaintext format outside the Cryptographic Module. Storage SHALL ensure security controls consistent with the protection provided by the certificate's Cryptographic Module.

6.2.5 Private Key archival

End-entity private key of PKI MUST not be archived.

6.2.6 Private Key transfer into or from a cryptographic module

Transfer of private keys apart from Section 6.2.4 Private Key Backup MUST not be performed. At no time SHALL the CA Private Key exist in plaintext form outside the cryptographic module.

Private or symmetric keys used to encrypt other Private Keys for transport SHALL be protected from disclosure.

Entry of a Private Key into a Cryptographic Module SHALL use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such Private Key.

6.2.7 Private Key storage on cryptographic module

See Section 0 Private Key holders SHALL take necessary precautions to prevent the loss, disclosure, Modification, or unauthorized use of their Private Keys in accordance with this section of this CP.

Cryptographic module standards and controls.

6.2.8 Method of activating private key

Each CA key MUST be activated before usage. See Section 6.2.2 Private Key (n out of m) multi-person control.

All CAs SHALL protect the Activation Data for their Private Keys against loss, theft, modification, disclosure, or unauthorized use.

6.2.8.1 CA Administrator Activation

Method of activating the CA system by a CA Administrator SHALL require:

- Use of a smart card, Biometric Access device, and/or password in accordance with Section 6.4.1, or security of equivalent strength to Authenticate the CA Administrator before the activation of the Private Key; and

- Commercially reasonable measures for the physical protection of the CA Administrator's workstation to prevent use of the workstation and its associated Private Key without the CA Administrator's authorization.

6.2.8.2 Offline CAs Private Key

Once the CA system has been activated, a m-of-n threshold number of multi-person Private Key holders SHALL be REQUIRED to supply their Activation Data in order to activate an offline CA's Private Key, as defined in Section 6.2.2. Once the Private Key is activated, it SHALL only be active until termination of the CA's session.

6.2.8.3 Online CAs Private Key

An online CA's Private Key SHALL be activated by a threshold number of multi-person Private Key holders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the Private Key is activated, the Private Key MAY be active for an indefinite period until it is deactivated when the CA goes offline.

6.2.9 Method of deactivating private key

After use, CAs SHALL deactivate the Cryptographic Module, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the CPS but no more than thirty (30) minutes. When deactivated, Private Keys SHALL be kept in encrypted form or protected in a HSM. Private Keys SHALL be cleared from memory before the memory is de-allocated. Any disk space where Private Keys were stored SHALL be overwritten before the space is released to the operating system. CA and CSS Cryptographic Modules SHALL be stored in a secure container when not in use.

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

After the key usage period, the private key of CAs of PKI SHALL 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.

Re-use of key material is prohibited.

CA Private Key destruction procedures SHALL employ methods commensurate with those in the NIST Guidelines for Media Sanitization [SP 800-88-1] and be sufficient to ensure that it is impossible to recover any part of the Private Key from any Cryptographic Module, memory or disk space.

If proper destruction of a CA Private Key cannot be guaranteed, then the key SHALL be treated as Compromised and its corresponding Public Key certificate Revoked.

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 Section 0.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

CAs of the PKI SHALL 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 usage period for the Root CA Key Pair SHALL NOT exceed 25 years, in alignment with Annex B of ISO 15118-20. Although SAE J3101 permits usage periods of up to 40 years, the ISO specification imposes a stricter limitation, which takes precedence under this Certificate Policy (CP).

For all other CAs operating under this CP, the validity and key usage periods SHALL conform to the limits set out in Annex B of ISO 15118-20 and are listed in the table below.

A CA's Private Key MAY be used to sign certificates only if the Validity Period of the issued certificate does not exceed the Validity Period of the CA certificate. However, the CA's Private Key MAY continue to be used to sign CRLs and OCSP responder certificates until the CA certificate itself expires.

To minimize risk of compromise, a CA MAY rotate its Private Key before the end of its usage period. From that point forward, only the new key SHALL be used to issue certificates. The older, but still valid, certificate SHALL remain available to verify prior signatures until all certificates signed with the corresponding Private Key have expired.

If the older Private Key is retained to sign OCSP responder certificates or CRLs, it SHALL be protected to the same security level as the active Private Key.

When a CA updates its key pair (generating a new Public Key), the CA SHALL notify all dependent CAs and Subscribers of the change. The validity and the operation period (i.e. key usage or re-keying period) for certificates SHALL be set in accordance with Annex B of [ISO 15118-20] as given below.

- V2G Root CA certificate
    - Validity Root CA: 25 years
- Charging Station Operator Certificates
    - CSO Sub CA1 certificate: 8 years
    - CSO Sub CA2 certificate: 4 years
    - SECC Leaf certificate: up to 12 months
- E-Mobility Service Provider Certificates
    - eMSP Sub1-CA: 12 years
    - eMSP Sub2-CA certificate: 12 years
    - Contract certificate: up to 4 years
- Certificate Provisioning Service Certificates
    - CPS Sub-CA 1: 12 years
    - CPS Sub-CA 2: 12 years
    - Leaf CPS Cert: 8 years
- Vehicle Certificates
    - Vehicle Sub-CA 1: 12 years
    - Vehicle Sub-CA 2: 12 years
    - Vehicle certificate leaf certificate: up to 12 years

- OEM Provisioning Certificates
    - OEM Sub-CA 1: 12 years
    - OEM Sub-CA 2: 12 years
    - OEM Prov. Cert.: up to 12 years
- Cross certificate: up to 12 years
- OCSP signer certificate: up to 1 year

Validity Periods SHALL be nested such that the Validity Periods of issued certificates SHALL be contained within the Validity Period of the CA. CAs SHALL NOT issue certificates with Validity Periods that extend beyond the expiration date of their own CA certificate.

All certificates signed by a specific CA Private Key MUST expire before the end of that Private Key's usage period.

PKI Participants SHALL cease all use of their Private Key after their Validity Period has expired.

Notwithstanding the specifications above, in all cases the CA Private Key MAY be used to sign OCSP responder certificates (if applicable) and CRLs until the CA certificate expires.

After generation of a V2G, within a period of 10 years, a new V2G Root MUST be generated. This MUST be communicated to subscribers of the PKI. One year up front, after 20 years validity of the old V2G Root, the old V2G Root will be transferred to passive mode and new Sub CAs and leaf certificates MUST not be generated anymore from this V2G Root. From that moment, the new V2G Root will be valid and used for Sub CA signing. Ergo, after 5 years only revocation status and OCSP certificates MUST be issued and any other new leaf certificates, MUST be issued under the new V2G Root CA. Every V2G Root MUST be in passive mode, until its validity time has expired.

Active mode implies: the issuance of revocation information and certificates, where passive mode describes the state of the V2G Root certificate, in which its still valid, and does sign OCSP leaf certificates, but does not sign any Sub CA and other leaf certificates.

The usage period for key pairs MUST be the same as the operational 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 MUST end 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 MUST be 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

CAs SHALL use Activation Data to unlock Private Keys, in conjunction with any other Access Control, which have an appropriate level of strength for the keys or data to be protected and SHALL meet the applicable Security Policy requirements of the Cryptographic Module used to store the keys. Two-factor Authentication SHALL be used to Authenticate CA Staff prior to unlocking the CA's Private Keys. To the extent passwords are used as Activation Data, the CA's activation participants SHALL generate

passwords that cannot easily be guessed or cracked. Participants MAY NOT need to generate Activation Data, for example, if they use Biometric Access devices.

CAs SHALL either entail the use of Biometric data or satisfy the policy-enforced at/by the Cryptographic Module. If the CA MUST transmit Activation Data, it SHALL be via an appropriate protected channel, and distinct in time and place from the associated Cryptographic Module. The CA SHALL change its Activation Data upon CA Re-Key.

RA and Subscriber Activation Data MAY be user-selected (e.g., password). The strength of the Activation Data SHALL meet or exceed the requirements for Authentication mechanisms stipulated for Level 3 or higher in [FIPS 140-2], or some other equivalent standard.

Activation data of CA keys is created during the creation of the CA key pair as described in Section 6.1.1. The activation of a CA private key SHALL be done with multi-person control as described in Section 6.2.2 Private Key (n out of m) multi-person control.

6.4.2 Activation data protection

CA Activation Data used to unlock Private Keys SHALL be protected from disclosure by a combination of cryptographic and physical Access Control mechanisms, such as:

- Memorization;
- Biometric in nature; or
- Recorded and secured at the level of assurance associated with the activation of the Cryptographic Module and SHALL NOT be stored with the Cryptographic Module.

In all cases, the protection mechanism implemented by CA Private Key holders SHALL include a facility to temporarily lock the account, or terminate the application, after at maximum ten (10) unsuccessful login attempts.

Every administrator is responsible for keeping and protecting his secrets against the loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.4.3 Other aspects of activation data

No stipulations.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

CA of the PKI functions MUST be implemented on trustworthy systems in accordance with best-practice standards (e.g. ISO 27001).

CAs of the PKI SHALL CA computer security functions SHALL:

- Require Authenticated logins;
- Require users to select strong passwords [SP 800-63-3];
- Provide Security Audit capability;
- Lock the Access to CA services after at maximum ten (10) unsuccessful login attempts;
- Restrict Access Control to CA services;
- Enforce separation of duties for Trusted Roles;

- Require identification and Authentication of Trusted Roles;
- Archive history and Audit Data;
- Employ malicious code protection mechanisms to mitigate the Risk of malicious code on CA system components;
- Employ technical and procedural controls to prevent and detect unauthorized changes to firmware and software on CA systems;
- Require Backups for recovery of keys and the CA system; and
- Enforce domain Integrity boundaries for security critical CA processes.
- RA computer security functions SHALL:
- Require Authenticated logins;
- Require users to select strong passwords;
- Provide Security Audit capability;
- Lock Access to RA services after at maximum ten (10) unsuccessful login attempts;
- Restrict Access Control to RA services;
- Enforce separation of duties for Trusted Roles;
- Require identification and Authentication of Trusted Roles; and
- Archive history and Audit Data.

6.5.2 Computer security rating

No stipulations.

6.5.3 Computer security controls

Vulnerability management SHALL follow an established risk-based approach. Security patches rated with a CVSS base score of 9.0 or above MUST be applied within 45 calendar days of disclosure. Medium to high-risk vulnerabilities (CVSS 4.0–8.9) SHOULD be patched within 90 days. All system components SHALL be monitored for security advisories affecting cryptographic or PKI-related functions.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

The system development controls address various aspects related to the development and change of the CA system through aspects of its life cycle.

The system development controls for the CA SHALL:

- Use software that has been designed and developed under a formal, documented development methodology;
- Procure hardware and software in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
- Develop hardware and software in a controlled and documented environment to demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment;

- Deliver all hardware and software via controlled methods that provide a continuous chain of accountability from the purchase location to the operations location;
- Dedicate hardware and software to performing PKI activities;
- Prevent malicious software from being loaded onto the equipment by implementing and testing in a non- production environment prior to implementation in a production environment.
- Obtain applications required to perform PKI operations from sources authorized by local policy.
- Scan CA hardware and software for malicious code on first use and periodically thereafter; and
- Purchase or develop hardware and software updates in the same manner as original equipment and installed using trusted and trained personnel.

6.6.2 Security management controls

All operating CAs MUST define mechanism and policies for controlling and monitoring the integrity of the CA-Systems. Upon installation and periodically thereafter (at least once per quarter), the integrity of the CA MUST be verified.

A list of acceptable products and their versions for each individual CA system component SHALL be maintained and kept up-to-date within a configuration management system. To reduce the available attack surface of a CA system, only those ports, protocols, and services that are necessary to the CA system architecture are permitted to be installed or operating.

The CA system SHALL maintain a list of ports, protocols, and services that are necessary for the correct function of each component within the CA system. The configuration of the CA system, in addition to any modifications and upgrades, SHALL be documented and controlled. The CA software, when first loaded, SHALL be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

The CA SHALL also have mechanisms and policies in place to control and monitor the configuration of the CA system.

6.6.3 Life cycle security controls

The software used to manage and operate the CAs of the PKI system, when first loaded, SHALL provide a method to verify that the software on the system:

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

Upon installation, and at least once a quarter, CAs of the PKI SHALL validate the integrity of the CA system

CAs SHALL have a plan for receiving notification of software and firmware updates, for obtaining and testing those updates, for deciding when to install them, and finally for installing them without undue disruption. A log SHALL be kept of the notifications, the decision to apply/not apply including reason, and the application of relevant updates/patches. CAs SHALL document any errors in configuration files, either because of human error, source data error, or changes in the environment which have made an

entry erroneous. The CA SHALL correct configuration file errors and document the reason for the error, and the associated correction.

Remediation activities applied to requirements and SHOULD NOT cause unavailability of revocation information.

6.7 Network Security Controls

CA of the PKI functions, 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 (e.g. by TLS and digital signature mechanisms).

The CPS SHALL describe how the CA network security is configured and validated.

6.7.1 Isolation of Networked Systems

The Root CA and its Private Keys SHALL be offline.

Communication channels between the network-connected CA components and the offline Root CA processing components SHALL be protected against attacks. Information flowing into offline Root CA components from the network-connected CA components SHALL NOT lead to any Compromise or disruption of these components.

The components of a CA requiring direct network connections SHALL be minimized. Online CA networked components SHALL be protected from attacks by adequate means to filter unwanted protocols (utilizing Access rules, protocol checkers, etc., as necessary). Data loss prevention tools SHALL be employed to detect inappropriate leakage of sensitive information from CA components.

6.7.2 Boundary Protection

Any boundary control devices used to protect the CA Repository or CA local area network SHALL deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network. CAs, RAs, Repositories, remote workstations used to administer the CAs, and CSS SHALL employ appropriate network security controls. Networking equipment SHALL turn off unused network ports and services. Any network software present SHALL be necessary to the functioning of the equipment.

6.7.2.1 Transmission Confidentiality

Intra-CA communications that cross the physical protection barrier of the certificate signing portion of the CA system SHALL be Confidentiality-protected. Services used by the CA system that are not administered by the CA Administrator SHALL provide protection commensurate with this CP.

Confidentiality of Subscriber or Sub-CA data SHALL be maintained as negotiated between the RA and the Subscriber or Sub-CA or the Subscriber or Sub-CA’s organization.

6.7.3 Network Monitoring

The CA SHALL monitor the CA system to detect attacks and indicators of potential attacks.

6.8 Time Stamping

All components involved in certificate issuance, revocation, audit logging, and status responses SHALL be synchronized with a trusted and traceable time source, such as the NIST Atomic Clock, NIST Network Time Protocol (NTP) service, or an equivalent authoritative reference.

- Asserted times MUST be accurate to within ±100 milliseconds.
- Time sources SHOULD support authenticated NTP or equivalent secure synchronization protocols.
- Clock adjustments SHALL be treated as auditable events (see Section 5.4.1).

Time derived from the trusted time source SHALL be used for establishing:

- Certificate validity periods (e.g., notBefore, notAfter);
- Certificate revocation timestamps;
- CRL publication timestamps;
- OCSP response timestamps;
- Audit log entries.

Both manual and electronic synchronization procedures MAY be employed, provided the resulting timekeeping meets the above accuracy and traceability requirements.

7 Certificate, CRL And OCSP Profiles

This Section describes formats of certificates, CRLs and OCSP.

The certificate profiles as listed below are based on the ISO 15118 certificate profiles but reflect the Hubject stipulated requirements and validity times.

7.1 Certificate Profile

The ISO 15118-20 Annex B defines the relevant certificate profiles for the Hubject ISO 15118 PKI.

A cell's content has the following meaning:

x	required
(x)	OPTIONAL
-	MUST not be present
c	This extension is critical, see IETF RFC 5280. If an implementation recognizes that a “critical” extension is present, but the implementation cannot interpret the extension, the implementation has to reject the certificate.
nc	This extension is non-critical, see IETF RFC 5280. If an implementation recognizes that a “non-critical” extension is present, but the implementation cannot interpret the extension, the extension can be ignored. Therefore, all OPTIONAL fields SHOULD also be “non-critical”. Quote from RFC 5280: “A certificate-using system MUST reject the certificate if it encounters a critical extension it does not recognize or a critical extension that contains information that it cannot process. A non-critical extension MAY be ignored if it is not recognized but MUST be processed if it is recognized."
PCID	Provisioning Certificate ID (max. 18, see [V2G2-ED2-932])
SECCID	Supply Equipment Communication Controller ID
PEID	Private Environment ID

SAE EVPKI certificate profile compliance

The certificate profile tables below define Hubject's X.509 v3 certificate fields and extensions. For CAs or Sub-CAs that seek recognition or inclusion in the SAE EVPKI CTL, the issuing CA MUST ensure that certificate field values and extensions are compliant with the SAE EVPKI CP v1.2 certificate profile requirements (including algorithm OIDs, field presence/criticality, extension mappings, key sizes and certificate validity periods). Any deviations from the SAE profile MUST be documented in a published mapping file and approved by Hubject and by the SAE EVPKI Policy Authority where required.

7.1.1 Version number(s)

Hubject ISO 15118 PKI issues X.509 version 3 certificates which contain the standard fields specified in the tables below:

7.1.1.1 Root CA certificate profile

The certificate profile for the Root CA is defined as follows:

ISO 15118-20 Certificate Profiles	Cluster:	**V2G Root**
	Name:	V2G Root
	Typ:	Root
tbsCertificate	Version	2 (X.509v3)
	SerialNumber	Integer
	Signature	ecdsa-with-SHA512
Issuer	Country	(x)
	Organization	x
	Organization Unit	(x)
	Common Name	x + "V2G"
	Domain Component	-*
Validity		25 years
Subject	Country	(x)
	Organization	x
	Organization Unit	(x)
	Common Name	x + "V2G"
	Domain Component	"V2G"
SubjectPublic KeyInfo	Public Key	x
	Cryptographic Algorithm	id-ecPublicKey
	Parameters	ECParameters (namedCurve secp512r1)
Extensions	AuthorityKeyIdentifier	-
	SubjectKeyIdentifier	x / nc
	KeyUsage	c
	digitalSignature	0/1
	nonRepudiation (contentCommitment)	0/1
	keyEncipherment	0/1
	dataEncipherment	0
	keyAgreement	0/1
	keyCertSign	1
	cRLSign	0/1
	encipherOnly	0
	decipherOnly	0
	ExtendedKeyUsage	-
	CertificatePolicies	-
	BasicConstraints	x / c
	CA	TRUE
	PathLength	-
	CRLDistributionPoints	-
	Authority Information Access (OCSP)	-
	Cryptographic Algorithm	ecdsa-with-SHA512
Signature Value		Octect-String

**Deviation from ISO15118-20: Although ISO 15118-20 permits the optional use of the domainComponent (DC) attribute, this Root CA profile explicitly prohibits the inclusion of the DC attribute. This deviation is introduced to ensure consistent and interoperable structures across all subordinate certificates, and to avoid ambiguity or misinterpretation in trust chain validation.*

7.1.1.2 Charging Station Operator Certificate profiles

The certificate profile for the Sub CA is defined as follows:

ISO 15118-20 Certificate Profiles	Cluster:	Charging Station Operator (CSO)		
	Name:	CSO Sub-CA 1	CSO Sub-CA 2	SECC Leaf Cert
	Type:	Sub	Sub	Leaf
tbsCertificate	Version	2 (X.509v3)	2 (X.509v3)	2 (X.509v3)
	SerialNumber	Integer	Integer	Integer
	Signature	ecdsa-with- SHA512	ecdsa-with- SHA512	ecdsa-with- SHA512
Issuer	Country	(x)	(x)	(x)
	Organization	x	x	x
	Organization Unit	(x)	(x)	(x)
	CommonName	x	x	x
	Domain Component	(x)	(x)	(x)
Validity		8 years	4 years	Up to 12 months
Subject	Country	(x)	(x)	x
	Organization	x	x	x
	Organization Unit	(x)	(x)	(x)
	Common Name	x	x	SECCID
	Domain Component	(x)	(x)	(x) & "CSO"
SubjectPublic KeyInfo	Public Key	x	x	x
	Cryptographic Algorithm	id-ecPublicKey	id-ecPublicKey	id-ecPublicKey
	Parameters	ECParameters (namedCurve secp512r1)	ECParameters (namedCurve secp512r1)	ECParameters (namedCurve secp512r1)
Extensions	AuthorityKeyIdentifier	x / nc	x / nc	x / nc
	SubjectKeyIdentifier	x / nc	x / nc	x / nc
	KeyUsage	x / c	x / c	x / c
	digitalSignature	0*	0*	1
	nonRepudiation (contentCommitment)	0*	0*	0
	keyEncipherment	0/1	0/1	0
	dataEncipherment	0	0	0
	keyAgreement	0/1	0/1	1
	keyCertSign	1	1	0
	cRLSign	1	1	0
	encipherOnly	0	0	0
	decipherOnly	0	0	0
	ExtendedKeyUsage	-	-	(x) / c
	CertificatePolicies	-	-	(x) / nc
	BasicConstraints	x / c	x / c	x / c
	CA	TRUE	TRUE	FALSE
	PathLength	1	0	-
	CRLDistributionPoints	-	-	-
	Authority Information Access (OCSP)	x / nc** id-ad-ocsp / location of the OCSP responder / CRL access point	x / nc** id-ad-ocsp / location of the OCSP responder / CRL access point	x / c id-ad-ocsp / location of the OCSP responder / CRL access point
	Cryptographic Algorithm	ecdsa-with- SHA512	ecdsa-with- SHA512	ecdsa-with- SHA512
Signature Value		Octect-String	Octect-String	Octect-String

**Deviation from SAE EVPKI v1.1/1.2: While SAE defines the digitalSignature and nonRepudiation key usage bit as set (1) for the CSO Sub-CA1 and Sub-CA2 certificate, this profile has not set (0) the value of the fields In accordance with best practice of PKI operation (reference: RFC5280 - CA certificates SHOULD NOT assert the digitalSignature or nonRepudiation bits.).*

***Deviation from ISO 15118-20: Although ISO 15118-20 marks the Authority Information Access (AIA) extension for OCSP as optional but potentially critical (x/c), this profile explicitly sets it to non-critical (x/nc). This deviation aligns with RFC 5280, which states that CA certificates must not mark the AIA extension as critical, to ensure compatibility with relying parties and maintain standards compliance.*

7.1.1.3 E-Mobility Service Provider Certificate profiles

The certificate profile for the E-Mobility Service Provider certificates are defined as follows:

Hubject PKI Certificate Profiles	Cluster:	**E-Mobility Service Provider (eMSP)**		
	Name:	eMSP Sub-CA 1	eMSP Sub-CA 2	Contract Cert
	Type:	Sub	Sub/Leaf	Leaf
tbsCertificate	Version	2 (X.509v3)	2 (X.509v3)	2 (X.509v3)
	SerialNumber	Integer	Integer	Integer
	Signature	ecdsa-with- SHA512	ecdsa-with- SHA512	ecdsa-with- SHA512
Issuer	Country	(x)	(x)	(x)
	Organization	x	x	x
	Organization Unit	(x)	(x)	(x)
	Common Name	x	x	x
	Domain Component	(x)	(x)	(x)
Validity		12 years	12 years	Up to 4 years
Subject	Country	(x)	(x)	(x)
	Organization	x	x	x
	Organization Unit	(x)	(x)	(x)
	Common Name	x	x	EMAID
	Domain Component	(x)	(x)	(x)
SubjectPublic KeyInfo	Public Key	X	x	x
	Cryptographic Algorithm	id-ecPublicKey	id-ecPublicKey	id-ecPublicKey
	Parameters	ECParameters (namedCurve secp512r1)	ECParameters (namedCurve secp512r1)	ECParameters (namedCurve secp512r1)
Extensions	AuthorityKeyIdentifier	x / nc*	x / nc*	x / c
	SubjectKeyIdentifier	x / nc**	x / nc**	x
	KeyUsage	x / c	x / c	x / c
	digitalSignature	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1
	dataEncipherment	0	0	0
	keyAgreement	0/1	0/1	0/1
	keyCertSign	1	1	0
	cRLSign	1	1	0
	encipherOnly	0	0	0
	decipherOnly	0	0	0
	ExtendedKeyUsage	-	-	-
	CertificatePolicies	(x) / nc	(x) / nc	(x) / nc
	BasicConstraints	x / c	x / c	x / c
	CA	TRUE	TRUE	FALSE
	PathLength	1	0	-
	CRLDistributionPoints	(x) / c	(x) / c	(x) / c
	Authority Information Access (OCSP)	(x) / nc*** id-ad-ocsp / location of the OCSP responder / CRL access point	(x) / nc*** id-ad-ocsp / location of the OCSP responder / CRL access point	(x) / c id-ad-ocsp / location of the OCSP responder / CRL access point
	Cryptographic Algorithm	ecdsa-with- SHA512	ecdsa-with- SHA512	ecdsa-with- SHA512
Signature Value		Octect-String	Octect-String	Octect-String

**Deviation from ISO 15118-20: Although ISO 15118-20 permits the Authority Key Identifier (AKI) extension to be marked as critical (x/c), this profile sets it to non-critical (x/nc) in accordance with [RFC 5280](Section 4.2.1.1), which states that this extension must not be marked critical in CA certificates.*

***Clarification to ISO 15118-20: While ISO 15118-20 lists the Subject Key Identifier (SKI) extension without specifying criticality (x), this profile explicitly sets it to non-critical (x/nc) to conform with [RFC 5280](Section 4.2.1.2), which advises that this extension must not be marked critical in CA certificates.*

****Deviation from ISO 15118-20: Although ISO 15118-20 marks the Authority Information Access (AIA) extension for OCSP as optional but potentially critical (x/c), this profile explicitly sets it to non-critical (x/nc). This deviation aligns with RFC 5280, which states that CA certificates must not mark the AIA extension as critical, to ensure compatibility with relying parties and maintain standards compliance.*

7.1.1.4 Certificate Provisioning Service profiles

The certificate profile for client certificates resp. Contract Certificate End-entity certificates are defined as follows:

Hubject PKI Certificate Profiles	Cluster:	**Certificate Provisioning Service (CPS)**		
	Name:	CPS Sub-CA 1	CPS Sub-CA 2	Leaf CPS Cert
	Type:	Sub	Sub	Leaf
tbsCertificate	Version	2 (X.509v3)	2 (X.509v3)	2 (X.509v3)
	SerialNumber	Integer	Integer	Integer
	Signature	ecdsa-with- SHA512	ecdsa-with- SHA512	ecdsa-with- SHA512
Issuer	Country	(x)	(x)	(x)
	Organization	x	x	x
	Organization Unit	(x)	(x)	(x)
	Common Name	x	x	x
	Domain component	(x)	(x)	"CPS"
Validity		12 years	12 years	8 years
Subject	Country	(x)	(x)	x
	Organization	x	x	x
	Organization Unit	(x)	(x)	(x)
	Common Name	x	x	x
	Domain Component	(x)	(x)	(x) & "CPS"
SubjectPublic KeyInfo	Public Key	x	x	x
	Cryptographic Algorithm	id-ecPublicKey	id-ecPublicKey	id-ecPublicKey
	Parameters	ECParameters (namedCurve secp512r1)	ECParameters (namedCurve secp512r1)	ECParameters (namedCurve secp512r1)
Extensions	AuthorityKeyIdentifier	x / nc*	x / nc*	x / c
	SubjectKeyIdentifier	x / nc**	x / nc**	x / nc**
	KeyUsage	x / c	x / c	x / c
	digitalSignature	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1
	dataEncipherment	0	0	0
	keyAgreement	0/1	0/1	0/1
	keyCertSign	1	1	0
	cRLSign	1	1	0
	encipherOnly	0	0	0
	decipherOnly	0	0	0
	ExtendedKeyUsage	-	-	-
	CertificatePolicies	(x) / nc	(x) / nc	(x) / nc
	BasicConstraints	x / c	x / c	x / c
	CA	TRUE	TRUE	FALSE
	PathLength	1	0	-
	CRLDistributionPoints	(x) / nc	(x) / nc	(x) / nc
	Authority Information Access (OCSP)	(x) / nc id-ad-ocsp / location of the OCSP responder / CRL access point	(x) / nc id-ad-ocsp / location of the OCSP responder / CRL access point	(x) / nc id-ad-ocsp / location of the OCSP responder / CRL access point
	Cryptographic Algorithm	ecdsa-with- SHA512	ecdsa-with- SHA512	ecdsa-with- SHA512
Signature Value		Octect-String	Octect-String	Octect-String

**Deviation from ISO 15118-20: Although ISO 15118-20 permits the Authority Key Identifier (AKI) extension to be marked as critical (x/c), this profile sets it to non-critical (x/nc) in accordance with [RFC 5280](Section 4.2.1.1), which states that this extension must not be marked critical in CA certificates.*

***Clarification to ISO 15118-20: While ISO 15118-20 lists the Subject Key Identifier (SKI) extension without specifying criticality (x), this profile explicitly sets it to non-critical (x/nc) to conform with [RFC 5280](Section 4.2.1.2), which advises that this extension must not be marked critical in CA certificates.*

7.1.1.5 Vehicle Certificate profiles

The profiles for the Vehicle certificate chain are defined as follows:

Hubject PKI Certificate Profiles	Cluster:	**EV Manufacturer: Vehicle certificates**		
	Name:	Vehicle Sub-CA 1	Vehicle Sub-CA 2	Vehicle certificate leaf
	Type:	Sub	Sub	Leafs
tbsCertificate	Version	2 (X.509v3)	2 (X.509v3)	2 (X.509v3)
	SerialNumber	Integer	Integer	Integer
	Signature	ecdsa-with- SHA512	ecdsa-with- SHA512	ecdsa-with- SHA512
Issuer	Country	(x)	(x)	(x)
	Organization	x	x	x
	Organization Unit	(x)	(x)	(x)
	Common Name	x	x	x
	Domain Component	(x)	(x)	(x)
Validity		12 years	12 years	up to 12 years
Subject	Country	(x)	(x)	(x)
	Organization	x	x	x
	Organization Unit	(x)	(x)	(x)
	Common Name	x	x	EVCCID
	Domain Component	(x)	(x)	(x) & “EV”
SubjectPublic KeyInfo	Public Key	x	x	x
	Cryptographic Algorithm	id-ecPublicKey	id-ecPublicKey	id-ecPublicKey
	Parameters	ECParameters (namedCurve secp512r1)	ECParameters (namedCurve secp512r1)	ECParameters (namedCurve secp512r1)
Extensions	AuthorityKeyIdentifier	x / nc*	x / nc*	x / nc*
	SubjectKeyIdentifier	x / nc**	x / nc**	x / nc**
	KeyUsage	x / c	x / c	x / c
	digitalSignature	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1
	dataEncipherment	0	0	0
	keyAgreement	0/1	0/1	0/1
	keyCertSign	1	1	0
	cRLSign	1	1	0
	encipherOnly	0	0	0
	decipherOnly	0	0	0
	ExtendedKeyUsage	-	-	(x) / c
	CertificatePolicies	(x) / nc	(x) / nc	(x) / nc
	BasicConstraints	x / c	x / c	x / c
	CA	TRUE	TRUE	FALSE
	PathLength	1	0	-
	CRLDistributionPoints	(x) / c	(x) / c	(x) / c
	Authority Information Access (OCSP)	(x) / nc*** id-ad-ocsp / location of the OCSP responder / CRL access point	(x) / nc*** id-ad-ocsp / location of the OCSP responder / CRL access point	(x) / nc*** id-ad-ocsp / location of the OCSP responder / CRL access point
	Cryptographic Algorithm	ecdsa-with- SHA512	ecdsa-with- SHA512	ecdsa-with- SHA512
Signature Value		Octect-String	Octect-String	Octect-String

**Deviation from ISO 15118-20: Although ISO 15118-20 permits the Authority Key Identifier (AKI) extension to be marked as critical (x/c), this profile sets it to non-critical (x/nc) in accordance with [RFC 5280](Section 4.2.1.1), which states that this extension must not be marked critical in CA certificates.*

***Deviation from ISO 15118-20: Although ISO 15118-20 allows the Subject Key Identifier (SKI) extension to be marked as critical (x/c), this profile sets it to non-critical (x/nc) in accordance with RFC 5280, Section 4.2.1.2, which states that this extension must not be marked critical in CA certificates.*

****Deviation from ISO 15118-20: Although ISO 15118-20 marks the Authority Information Access (AIA) extension for OCSP as optional but potentially critical (x/c), this profile explicitly sets it to non-critical (x/nc). This deviation aligns with RFC 5280, which states that CA certificates must not mark the AIA extension as critical, to ensure compatibility with relying parties and maintain standards compliance.*

7.1.1.6 OEM Provisioning Certificate profiles

The profiles for the OEM certificate chain are defined as follows:

Hubject PKI Certificate Profiles	Cluster:	**EV Manufacturer: OEM Provisioning**		
	Name:	OEM Sub-CA 1	OEM Sub-CA 2	OEM Prov. Cert.
	Type:	Sub	Sub	Leafs
tbsCertificate	Version	2 (X.509v3)	2 (X.509v3)	2 (X.509v3)
	SerialNumber	Integer	Integer	Integer
	Signature	ecdsa-with- SHA512	ecdsa-with- SHA512	ecdsa-with- SHA512
Issuer	Country	(x)	(x)	(x)
	Organization	x	x	x
	Organization Unit	(x)	(x)	(x)
	Common Name	x	x	x
	Domain Component	(x)	(x)	(x)
Validity		12 years	12 years	up to 12 years
Subject	Country	(x)	(x)	(x)
	Organization	x	x	x
	Organization Unit	(x)	(x)	(x)
	Common Name	x	x	PCID
	Domain Component	(x)	(x)	(x) *
SubjectPublic KeyInfo	Public Key	x	x	x
	Cryptographic Algorithm	id-ecPublicKey	id-ecPublicKey	id-ecPublicKey
	Parameters	ECParameters (namedCurve secp512r1)	ECParameters (namedCurve secp512r1)	ECParameters (namedCurve secp512r1)
Extensions	AuthorityKeyIdentifier	x / nc**	x / nc**	x / c
	SubjectKeyIdentifier	x / nc***	x / nc***	x / nc***
	KeyUsage	x / c	x / c	x / c
	digitalSignature	0/1	0/1	1
	nonRepudiation (contentCommitment)	0/1	0/1	0/1
	keyEncipherment	0/1	0/1	0/1
	dataEncipherment	0	0	0
	keyAgreement	0/1	0/1	1
	keyCertSign	1	1	0
	cRLSign	1	1	0
	encipherOnly	0	0	0
	decipherOnly	0	0	0
	ExtendedKeyUsage	-	-	-
	CertificatePolicies	(x) / nc	(x) / nc	(x) / nc
	BasicConstraints	x / c	x / c	x / c
	CA	TRUE	TRUE	FALSE
	PathLength	1	0	-
	CRLDistributionPoints	(x) / c	(x) / c	(x) / c
	Authority Information Access (OCSP)	(x) / nc**** id-ad-ocsp / location of the OCSP responder / CRL access point	(x) / nc**** id-ad-ocsp / location of the OCSP responder / CRL access point	(x) / nc**** id-ad-ocsp / location of the OCSP responder / CRL access point
	Cryptographic Algorithm	ecdsa-with- SHA512	ecdsa-with- SHA512	ecdsa-with- SHA512
Signature Value		Octect-String	Octect-String	Octect-String

**The Domain Component (DC) of the Distinguished Name (DN) designation for the OEM Provisioning Certificate shall in accordance with the specification in ISO 15118-20 not end with 'EV'.*

***Deviation from ISO 15118-20: Although ISO 15118-20 permits the Authority Key Identifier (AKI) extension to be marked as critical (x/c), this profile sets it to non-critical (x/nc) in accordance with [RFC 5280](Section 4.2.1.1), which states that this extension must not be marked critical in CA certificates.*

****Deviation from ISO 15118-20: Although ISO 15118-20 allows the Subject Key Identifier (SKI) extension to be marked as critical (x/c), this profile sets it to non-critical (x/nc) in accordance with RFC 5280, Section 4.2.1.2, which states that this extension must not be marked critical in CA certificates.*

*****Deviation from ISO 15118-20: Although ISO 15118-20 marks the Authority Information Access (AIA) extension for OCSP as optional but potentially critical (x/c), this profile explicitly sets it to non-critical (x/nc). This deviation aligns with RFC 5280, which states that CA certificates must not mark the AIA extension as critical, to ensure compatibility with relying parties and maintain standards compliance.*

7.1.2 Cross certificate and OCSP signer certificate profiles

The profiles for the OCSP signer certificate are defined as follows:

Hubject PKI Certificate Profiles	Cluster:	**Cross certificate and OCSP signer**	
	Name:	Cross certificate	OCSP signer certificate
tbsCertificate	Version	2 (X.509v3)	2 (X.509v3)
	SerialNumber	Integer	Integer
	Signature	ecdsa-with- SHA512	ecdsa-with- SHA512
Issuer	Country	(x)	(x)
	Organization	x	x
	Organization Unit	(x)	(x)
	Common Name	x	x
	Domain Component	(x)	(x)
Validity		Up to 12 years	Up to 1 year
Subject	Country	(x)	-
	Organization	x	x
	Organization Unit	(x)	(x)
	Common Name	x	x
	Domain Component	(x)	(x)
SubjectPublic KeyInfo	Public Key	x	x
	Cryptographic Algorithm	id-ecPublicKey	id-ecPublicKey
	Parameters	ECParameters (namedCurve secp512r1)	ECParameters (namedCurve secp512r1)+
Extensions	AuthorityKeyIdentifier	x / nc	x / nc
	SubjectKeyIdentifier	x / nc	x / nc
	KeyUsage	x / c	x / c
	digitalSignature	0/1	0/1
	nonRepudiation (contentCommitment)	0/1	0/1
	keyEncipherment	0/1	0/1
	dataEncipherment	0	0
	keyAgreement	0/1	0/1
	keyCertSign	1	0
	cRLSign	0/1	0
	encipherOnly	0	0
	decipherOnly	0	0
	ExtendedKeyUsage	-	x / c
	CertificatePolicies	(x) / nc	-
	BasicConstraints	x / c	x / c
	CA	TRUE	TRUE
	PathLength	-	-
	CRLDistributionPoints	(x) / c	-
	Authority Information Access (OCSP)	(x) / c id-ad-ocsp / location of the OCSP responder / CRL access point	-
	Cryptographic Algorithm	ecdsa-with- SHA512	ecdsa-with- SHA512
Signature Value		Octect-String	Octect-String

7.1.3 Certificate extensions

All certificates issued within this PKI MUST include the required X.509 v3 extensions as specified in RFC 5280. Unless explicitly noted otherwise, extensions SHALL be marked as non-critical (critical = false), except where criticality is REQUIRED (e.g., basicConstraints in CA certificates). The profile and criticality of each extension are aligned with SAE EVPKI CP v1.2 and ISO 15118-20. Deviations SHALL be explicitly documented with justification.

7.1.4 Algorithm object identifiers

The algorithm object identifiers conform to the standards, see the tables above.

7.1.5 Name forms

The domainComponent (DC) attribute SHALL NOT be used in the Subject Distinguished Name (DN) of Root CA certificates. This restriction aligns with best practices outlined in RFC 5280 and SAE EVPKI CP v1.2 to ensure global uniqueness and interoperability. The use of DC attributes in Sub-CA or End-Entity certificates MAY be permitted if justified and documented in the CPS.

See Section 3.1.1.

7.1.6 Name constraints

Name constraints are not supported.

7.1.7 Certificate policy object identifier

See extension „CertificatePolicies“ in the certificate profile.

7.1.8 Usage of Policy Constraints extension

Policy constrains extensions are not supported.

7.1.9 Policy qualifiers syntax and semantics

No stipulations.

7.1.10 Processing semantics for the critical Certificate Policies extension

The extension „CertificatePolicies“ is not critical.

7.2 CRL Profile

7.2.1 Version number(s)

The certification revocation lists are issued in the X.509 Version 3 in accordance with RFC 5280 [5]

7.2.2 CRL and CRL entry extensions

The CRLs 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

Critical CRL extensions SHALL NOT be used.

7.3 OCSP Profile

7.3.1 Version number(s)

OCSP responses, if supported by a CA, SHALL conform to the OCSP profile specified in [RFC 6960] as updated by [RFC 8954].

OCSP responses SHALL conform to [RFC 6960] and SHALL either be:

- Signed by the CA that issued the certificates whose revocation status is being checked; or
- Signed by an OCSP responder certificate signed by the Root CA; or
- Signed by an OCSP responder certificate signed by the CA that issued the certificate whose revocation status is being checked. Such OCSP responder certificate MAY contain the extension id-pkix-ocsp-nocheck as defined by [RFC 6960]. This extension indicates that the End-Entity certificate need not obtain a CRL for the OCSP responder's certificate. The OCSP responder SHOULD be a highly trusted component.

7.3.2 OCSP extensions

No stipulations.

8 Compliance Audit and Other Assessments

CAs and RAs SHALL have a Compliance Audit mechanism in place to ensure that the requirements of this CP are being implemented in the appropriate CPS and the policies are being enforced.

CAs and RAs SHOULD have self-Auditing capability and SHOULD complete self-Audits at least annually.

8.1 Frequency or Circumstances of Assessment

All Certification Authorities (CAs) participating in the Hubject ISO 15118-20 PKI SHALL undergo regular compliance audits conducted by an independent assessor approved by Hubject GmbH.

- A compliance audit MUST be completed prior to the initial operation of any new CA and before the issuance of a new Sub-CA certificate.
- External compliance audits SHALL be performed at least annually for all CAs, covering security controls, CP/CPS compliance, and certificate lifecycle management.
- Internal audits MUST be conducted at least every six months, with focus on operational security, incident response, and audit log integrity.

Hubject GmbH MAY delegate the performance of audits and related assessments to a qualified third-party audit firm. All audited entities SHALL cooperate fully with the audit process and grant reasonable access to relevant personnel, records, and systems.

Audits SHALL be performed at the sole expense of the audited entity.

8.2 Identity/Qualifications of the Assessor and Relationship to the Entity

The Compliance Auditor MUST demonstrate competence in the field of Compliance Audits, and MUST be thoroughly familiar with CAs, RAs, and CPs. The Compliance Auditor MUST perform such Compliance Audits as a regular ongoing business activity.

In addition to the previous requirements, the Compliance Auditor MUST be a Certified Information Systems Auditor or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable Risks, mitigation strategies, and industry best practices, and:

- Be an independent public accounting or Auditing firm that has proficiency in examining PKIs, security Auditing, and third-party attestation and be currently licensed to perform WebTrust for CA Audits [SSAE 18, or ISO 27001] standards, or to perform such alternate equivalent Audits approved by the PA; and
- Be a private firm that is independent from the entities (CA or RA) being Audited; and
- Be a member of the American Institute of Certified Public Accountants (AICPA) or equivalent that requires that Audits be completed under defined standards.

To ensure independence and objectivity, the Compliance Auditor MUST NOT have served the entity in developing or maintaining the to-be-Audited CA/RA Facility.

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

The Superior Entity SHOULD identify the parties responsible for providing Auditing services for its Sub-CAs, and MAY allow the Sub-CA to identify a Compliance Auditor for consideration by the Superior Entity.

The Superior Entity SHALL determine whether a Compliance Auditor meets the Audit qualification requirements including checking that the CA is reviewing the Audits of its Sub-CAs for compliance to this CP and their CPS.

Compliance audits MUST be carried out or conducted by Hubject GmbH. Compliance Audits are conducted at the sole expense of the audited Hubject ISO 15118 PKI Sub CA.

In addition to the qualifications already specified in this CP, Sub-CAs and Root CAs that request inclusion in the SAE EVPKI CTL MUST undergo a compliance audit meeting the SAE EVPKI auditor requirements. The auditor SHALL be qualified to perform PKI audits under industry-recognized standards (e.g., WebTrust for Certification Authorities or ISO/IEC equivalent) or other audit standards explicitly accepted by SAE EVPKI. The CA MUST provide the audit report, corrective action plan (where applicable), and attestations required by SAE EVPKI to the SAE EVPKI Policy Authority or CTL operator as part of the CTL inclusion process.

8.3 Topics Covered by Assessment

Audits MUST conform to recognized industry standards, such as WebTrust for CAs, SSAE 18, or ISO/IEC 27001. The scope of the audit SHALL include the CA's and RA's:

- Compliance with this Certificate Policy (CP) and the applicable Certification Practice Statement (CPS);
- Key and certificate lifecycle management;
- Certificate issuance, revocation, and status services;
- Repository and directory integrity;
- Time synchronization accuracy;
- Incident detection and response procedures;
- Internal controls and security operations.

Each audit MUST verify that the audited entity, CA or RA, meets all applicable requirements of this CP.

The audit of a Superior CA SHALL also include a review of the audit results of any Sub-CAs it has directly approved. This SHOULD verify whether:

- Timely responses and mitigations were implemented for deficiencies identified in internal or external audits;
- The Superior CA performs appropriate oversight and follow-up; and
- The approved Sub-CAs are themselves conducting equivalent oversight of any Subordinate CAs they have issued.

For example, a Root CA audit SHALL confirm that the Root CA reviewed and responded to audit findings from Sub-CA1. Sub-CA1 SHOULD do the same for any Sub-CAs it has issued.

8.4 Actions Taken as a Result of Deficiency

After receiving a Compliance Audit report, the Hubject ISO 15118-20 PKI Root CA SHALL contact the audited party to discuss any exceptions or deficiencies shown by the Compliance Audit. The audited Sub CA and Hubject together with the auditor SHALL, in good faith, use commercially reasonable efforts to agree on a corrective action plan for correcting the problems causing the exceptions or deficiencies and to implement the plan.

In the event of the audited Sub CA fails to develop such a corrective action plan or implement it, or if the report reveals exceptions or deficiencies that Hubject and the auditor reasonably believe pose an immediate threat to the security or integrity of the Hubject ISO 15118-20 PKI, then the assessor MAY require temporary suspension of the CA's services or even revocation of CA certificates if severe deficiencies were discovered such that a secure and reliable operation of the CA cannot be guaranteed.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Superior Entity MAY decide to temporarily halt operation of the CA, to Revoke a certificate issued by the CA or RA or take other actions it deems appropriate.

The Superior Entity SHALL provide to the CA its procedures for making and implementing such determinations.

8.5 Communication of Results

Following any Compliance Audit, the audited Sub CA SHALL provide Hubject GmbH with the report and attestations based on its audit within fourteen (14) days after the completion of the audit.

9 Other Business and Legal Matters

9.1 Fees

Hubject GmbH is entitled to charge Sub CAs for the issuance, management, and renewal of Certificates.

Hubject GmbH and the Sub CA operators are entitled to charge end-entity subscribers for the issuance, management, and renewal of Certificates.

Hubject ISO 15118 PKI CAs MAY charge a fee as a condition of making a certificate available in a repository or otherwise making certificates available to relying parties.

Hubject ISO 15118 PKI CAs MAY charge a fee as a condition of making the CRLs required by this CP available in a repository or otherwise available to relying parties. They SHALL, however, be entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added services based on the Hubject ISO 15118 PKI.

9.1.1 Certificate issuance or renewal fees

Certificate issuance or renewal fees are governed in separate mutual agreements.

9.1.2 Certificate access fees

Access to CA certificates is described in 2.2 Publication of Certification Information

9.1.3 Revocation or status information access fees

Access to certificate revocation or status information is described in 2.2 Publication of Certification Information

9.1.4 Fees for other services

Fees for other services are governed in separate mutual agreements.

9.1.5 Refund policy

Not applicable

9.2 Financial Responsibility

9.2.1 Insurance coverage

Hubject ISO 15118 PKI CAs SHALL maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

9.2.2 Other assets

Hubject ISO 15118 PKI CAs SHALL have sufficient financial resources to maintain their operations and perform their duties, and they MUST be reasonably able to bear the risk of liability to subscribers and relying parties.

9.2.3 Insurance or warranty coverage for end-entities

No stipulations.

9.3 Confidentiality of Business Information

The following records SHALL be kept confidential and private:

- Sub CA application records, whether approved or disapproved
- certificate application records
- Hubject ISO 15118 PKI audit trail records
- Contingency planning and disaster recovery plans

9.3.1 Scope of confidential information

9.3.2 Information not within the scope of confidential information

9.3.3 Responsibility to protect confidential information

9.4 Privacy of Personal Information

No stipulation but MUST consider legal regulations.

9.4.1 Privacy plan

No stipulation but MUST consider legal regulations.

9.4.2 Information treated as private

No stipulation but MUST consider legal regulations.

9.4.3 Information not deemed private

No stipulation but MUST consider legal regulations.

9.4.4 Responsibility to protect private information

No stipulation but MUST consider legal regulations.

9.4.5 Notice and consent to use private information

No stipulation but MUST consider legal regulations.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulations., but MUST consider legal regulations

9.4.7 Other information disclosure circumstances

No stipulations., but MUST consider legal regulations

9.5 Intellectual Property Rights

No stipulations., but MUST consider legal regulations.

9.6 Representations and Warranties

Hubject ISO 15118 PKI CAs warrants that:

- their Certificates meet all requirements of this CP and the applicable Certificate Practice Statement, and
- revocation services and use of a repository conform to all requirements of this CP and the applicable Certificate Practice Statement in all aspects.

9.6.1 CA representations and warranties

No stipulations.

9.6.2 RA representations and warranties

No stipulations.

9.6.3 Subscriber representations and warranties

No stipulations.

9.6.4 Relying party representations and warranties

No stipulations.

9.6.5 Representations and warranties of other participants

No stipulations.

9.7 Disclaimers of Warranties

Not applicable

9.8 Limitations of Liability

Hubject is not liable for any loss or damage or any expenses incurred by the other Party, irrespective of the legal grounds on which any such claim MAY be based (breach of obligation, contract, tort etc.).

Notwithstanding the provisions set forth above, Hubject is liable

a. for any loss or damage caused by wilful act or gross negligence;

b. for any death, personal injury or damage to health for which Hubject is held responsible;

c. under the provisions of the German Product Liability Act (Produkthaftungsgesetz); or

d. for any loss or damage caused by any breach of a material obligation under the Hubject Sub-CA Contract (wesentliche Vertragspflicht), i.e. such an obligation the performance of which is essential to the proper implementation of the Hubject Sub-CA Contract Agreement and compliance with which the Partner MAY rely on, for which Hubject is held responsible. The liability of Hubject in the event of a breach of a material obligation under this Agreement is limited to such typical loss or damage as could reasonably have been foreseen, unless Hubject's liability is due to wilful act or gross negligence, death, personal injury or damage to health, or in accordance with the Product Liability Act.

Any exclusion or limitation of Hubject's liability pursuant to the provisions set out hereinabove also applies in respect of any statutory or vicarious agents or employees acting on behalf of Hubject.

Nothing in this Section is to be construed so as to affect the Partner's burden of proof to the Partner’s disadvantage.

9.9 Indemnities

Not applicable.

9.10 Term and Termination

9.10.1 Term

This CP becomes effective the day when it is published. It remains valid until it is replaced by a new version.

9.10.2 Termination

This CP SHALL remain in force until it is replaced by a new version.

9.10.3 Effect of termination and survival

Upon termination of this CP, Hubject ISO 15118 PKI participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, Hubject ISO 15118 PKI participants SHALL use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedures for amendment

Amendments to this CP MAY be made by the Hubject ISO 15118 PKI Policy Management Authority. Amendments SHALL either be in the form of a document containing an amended form of the CP or an update.

Updates supersede any designated or conflicting provisions of the referenced version of the CP.

9.12.2 Notification mechanism and period

Hubject GmbH reserve the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information.

SAE EVPKI notification requirement

Where a revision to this CP or to any subordinate CPS affects Hubject's compliance with SAE EVPKI CP v1.2 or the metadata published to the SAE EVPKI CTL (e.g., changes to certificate profiles, OIDs, root certificates, revocation mechanisms, or audit status), Hubject SHALL:

a) Notify the SAE EVPKI Policy Authority and CTL operator within 30 days of publication of the change; and
b) Publish a mapping document explaining the change and its impact on SAE EVPKI interoperability.

If the change is material and may affect relying parties, Hubject SHALL also publish a 90-day notification period for affected relying parties in accordance with SAE EVPKI change control practices.

9.12.3 Circumstances under which OID MUST be changed

If the CA operator determines that a change is necessary in the object identifier corresponding to a CP, the amendment SHALL contain new object identifiers for the CP. Otherwise; amendments SHALL not require a change in Certificate policy Object Identifier.

9.13 Dispute Resolution Provisions

Not applicable.

9.14 Governing Law

This Document and all disputes and claims arising out of or in connection with this document are governed by German law excluding its conflict of law's provisions. Exclusive place of jurisdiction is Berlin.

9.15 Compliance with Applicable Law

All participants of the Hubject ISO 15118 V2G PKI MUST adhere to the applicable law.

9.16 Miscellaneous Provisions

No stipulations.

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.

9.16.5 Force Majeure

Not applicable.

9.17 Other Provisions

None.

10 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] FIPS PUB 140-2, "Security Requirements for Cryptographic Modules", May 2001

[4] RFC 2560, X.509 Internet Public Key Infrastructure – Online certificate Status Protocol – OCSP. M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, 1999.

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

[6] ITU-T Recommendation X.501 (2005), Information technology - Open Systems Inter-connection - The Directory: Models, 2008.

[7] ISO/IEC 15118-20:2022, 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.

[8] BS, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog2017_Entwurf_markiert.pdf?__blob=publicationFile&v=3

[9] Hubject GmbH Plug&Charge Interface Description v3.0. Available on request.

[10] PKCS#10 – Certificate Request Syntax Specification. https://tools.ietf.org/html/rfc2986

[11] Support Study on the development of a governance framework for the EU Public Key Infrastructure (PKI) based on the standard ISO 15118 as part of the Directorate-General for Mobility and Transport (DG MOVE) from 2023

[12] SAE Electric Vehicle Public Key Infrastructure - Certificate Policy (CP) V1.1 from 2023-07-12

[13] SAE Electric Vehicle Public Key Infrastructure - Certificate Policy (CP) V1.2 from 2024-11-12

Any questions?
support@pnc.hubject.com

Version 1.0 – March 2026

Hubject GmbH