Polestar

VERSION 1.0

# Certificate Policy

## For Polestar V2G PKI

Polestar Performance AB
Assar Gabrielssons väg 9
SE-405 31 Göteborg
Sweden

polestar.com

Registered: Gothenburg, Sweden
Registration no. 556653-3096

## Document information and revision history

| | |
|---|---|
| **Document version** | 1.0 |
| **Classification** | Public |
| **Author(s)** | Anders Runesson, Security Officer, Polestar Information Security |
| **Reviewer(s)** | Wei Guo, Security Officer, Polestar Information Security |
| **Approver(s)** | Andreas Kullman, Polestar CISO |
| | |

| Date | Version | Author | Description |
|---|---|---|---|
| 2023-12-20 | 1.0 | Anders Runesson | First published version |
| | | | |

## Structure

This document conforms to the structure of Certificate Policies and Certification Practice Statements specified in RFC 3647[1]. Sections have been added in a way that retains the document structure in RFC 3647.

## Intended audience

This document is intended for, but not limited to, all subscribers, stakeholders, and participants in the PKI.

## Keywords

Within this document, the key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL”, if written in capitals, are to be interpreted as described in RFC 2119[2]

## Terms and abbreviations

| | |
|---|---|
| Authentication | The process of establishing the truth of an entity’s claim of identity |
| CA | Certification Authority |
| CCP | Contract Certificate Pool |
| CN | Common Name |
| CPO | Charge Point Operator |
| CPS | Certification Practice statement |
| CPS | Certificate Provisioning Service |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| DN | Distinguished Name |

[1] https://www.ietf.org/rfc/rfc3647.txt
[2] https://datatracker.ietf.org/doc/html/rfc2119

| | |
|---|---|
| EE | End Entity |
| eMAID | e-Mobility Account Identifier |
| EVCC | Electric Vehicle Communication Controller |
| EVSE | Electric Vehicle Supply Equipment |
| HSM | Hardware Security Module |
| Identification | The process whereby an entity makes a claim regarding their identity. Precedes authentication. |
| IETF | Internet Engineering Task Force |
| MO | Mobility Operator |
| OCSP | Online Certificate Status Protocol |
| OEM | Original Equipment Manufacturer |
| OID | Object Identifier, global standardized numeric identifiers. See https://en.wikipedia.org/wiki/Object_identifier |
| PCID | Provisioning Certificate Identifier |
| PKI | Public Key Infrastructure |
| PnC, P&C | Plug and Charge based on [ISO15118-2] or [ISO15118-20] |
| RCP | Root Certificate Pool |
| RFC | Request For Comment |
| SECC | Supply Equipment Communication Controller |
| V2G | Vehicle to grid |

## References


| | |
|---|---|
| [ASN.1] | ITU-T Recommendation X.680-X.693 (02/21): Information Technology - Abstract Syntax Notation One (ASN.1) & ASN.1 encoding rules |
| [FIPS 140-2] | https://csrc.nist.gov/pubs/fips/140-2/upd2/final<br>NIST standard - Security Requirements for Cryptographic Modules |
| [FIPS 140-3] | https://csrc.nist.gov/pubs/fips/140-3/final<br>NIST standard - Security Requirements for Cryptographic Modules |
| [FIPS 140] | The text may refer to the FIPS 140 standards without version number in cases where the standards are aligned. |
| [RFC2986] | https://datatracker.ietf.org/doc/html/rfc2986<br>PKCS #10: Certification Request Syntax Specification |
| [RFC3647] | https://www.ietf.org/rfc/rfc3647.txt<br>Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework |

| | |
|---|---|
| [RFC5280] | https://datatracker.ietf.org/doc/html/rfc5280<br>Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile |
| [ISO/IEC 15408] | ISO/IEC 15408 2022: Information security, cybersecurity and privacy protection — Evaluation criteria for IT security<br>*Defines Evaluation Assurance Levels (EAL), also known as Common Criteria* |
| [ISO/IEC 19790] | ISO/IEC 19790:2012: Information technology - Security techniques - Security requirements for cryptographic modules |
| [ISO15118-2] | Standard ISO 15118-2:2014: Road vehicles -- Vehicle-to-grid Communication Interface – Part 2: Network and application protocol requirements |
| [ISO15118-20] | Standard ISO 15118-2:2022: Road vehicles – Vehicle to grid communication Interface – Part 20: 2nd generation network layer and application layer requirements |
| [ISO15118] | The text may refer to ISO15118 without version number in cases where the standards are aligned. |
| [ISO3166-1] | Standard ISO 3166-1:2020: Codes for the representation of names of countries and their subdivisions - Part 1: Country code |
| [X.500] | ITU-T Recommendation X.500 (2005) I ISO/IEC 9594-1:2005<br>Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services |

In some cases the standards [ISO15118] may be referenced along with an identifier in the form [V2Gnn-nnnn], for example [ISO15118-2] [V2G2-932]. This is a specific requirement or motivation that can be found by searching for the text in the standard. In this case searching for “[V2G2-932]” results in a requirement that reads: “CertID shall be an alphanumeric String with at maximum length of 18 characters (i.e. A..Z, a..z, 0..9).”

# 1 INTRODUCTION

## 1.1 Overview

Polestar Performance AB (henceforth referred to as 'Polestar') is a car design and manufacturing company that fully embraces digitalized processes both in design and development, the customer journey, and to drive advanced product functionality that our customers expect. Online communication and information processing in a fully connected landscape is built into our DNA and our products, and requires sophisticated security everywhere and always.

Cryptography is a core pillar of security protecting authentication, confidentiality, and integrity of data and communications. Commonly this is implemented using Public Key Infrastructure (PKI). It is a mature security technology used everywhere across the internet, and is part of the international standards for Plug and Charge (PnC) [ISO15118]. To support PnC in our products Polestar has decided to deploy this PKI for V2G.

This CP aims to comply with [ISO15118]. In case of any conflict between this policy and the ISO standards, the ISO standards will have precedence.

This document defines the operational, procedural, and security requirements in this PKI. These requirements apply to all participating CAs and other participants, subscribers, etc. This will form a trusted context where all participants can rely on the integrity of issued certificates by evaluating this CP and participating CAs Certification Practice Statements (CPS) and Registration Authority agreements (if applicable).

This CP does not govern any entity outside this PKI, even those that depend on the PKI. This is furthermore not a legal or contractual agreement between participants in the PKI, but may be referenced in such agreements.

## 1.2 Document name and identification

This document is Polestar's Certificate Policy for Polestar V2G PKI and is identified by the following:

- Name: Certificate Policy for Polestar V2G PKI
- Version: 1.0
- OID: 1.3.6.1.4.1.59600.2.509.0.1.1

The OID arc 1.3.6.1.4.1.59600 is Polestar's IANA assigned Private Enterprise Number[3].

The CP's full identifier is: 1.3.6.1.4.1.59600.2.509.0.1.1

## 1.3 PKI participants

### 1.3.1 PKI structure

To support all [ISO15118] use cases several CA chains must be established. All CA chains in Polestar's V2G PKI comprises three CA tiers. The root CA certifies policy CAs, and policy CAs certify issuing CAs. An issuing CA SHALL only sign end-entity certificates.

CAs in this PKI MUST strictly abide by the certificate types they are allowed to sign in the following table.

| CA type | Issued by | Allowed to sign certificate types | Other |
|---|---|---|---|
| Root | Self | Policy CA, OCSP signer | CRL files, OCSP responses |
| Policy (Sub 1/Tier 1) | Root | Issuing CA, OCSP signer | CRL files, OCSP responses |
| Issuing (Sub 2/Tier 2) | Policy | End entity, OCSP signer | CRL files, OCSP responses |
| End entity | Issuing | MUST NOT sign certificates | |

[3] See https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

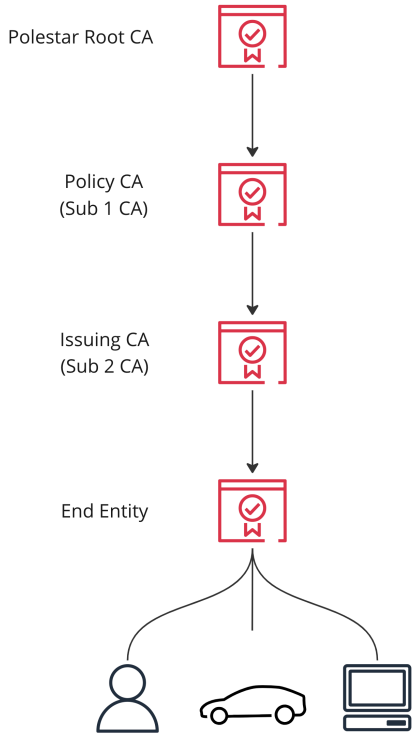


*Figure 1 Schematic view of Polestar PKI CA chains*

### 1.3.1.1 CA chains

Polestar's V2G PKI is designed to fulfill the requirements in [ISO15118-2] and [ISO15118-20]. To fully support the standards three different signing algorithms must be supported. This requires three separate CA chains, one for [ISO15118-2] and two for [ISO15118-20], each chaining up to a different root CA. The chains differ in the type of signing algorithms they support, in accordance with the V2G ISO standards.

[ISO15118-2] requires certificates to be signed using ECDSA with named curve secp256-r1. [ISO15118-20] requires two different signature algorithms - ECDSA with named curve secp521-r1 OR Ed448. Supporting different signing algorithms require separate CA chains, as defined in the following table.

| Chain root CA | Supported standard | Signing algorithm |
|---|---|---|
| Polestar ECC-256 Root CA v1 | [ISO15118-2] | ECDSA curve secp256-r1 with SHA256 |
| Polestar ECC-521 Root CA v1 | [ISO15118-20], requirement [V2G20-2647] | ECDSA curve secp521-r1 with SHA512 |
| Polestar ECC-448 Root CA v1 | [ISO15118-20], requirement [V2G20-2319] | ECDSA curve Ed448 with SHA512 |

### 1.3.1.2 V2G Actor types supported

Polestar may opt to act within V2G in different capacities – OEM, MO, CPO, or others. For the purposes of PKI support, Polestar's V2G PKI will adhere to the structures for CA chains in [ISO15118] as they relate to the specific actor types. Different "actor" chains MAY chain to the same root if they use the same signature algorithm.

Private Environment PKI, as defined in [ISO15118], is out of scope for this CP and Polestar's V2G PKI.

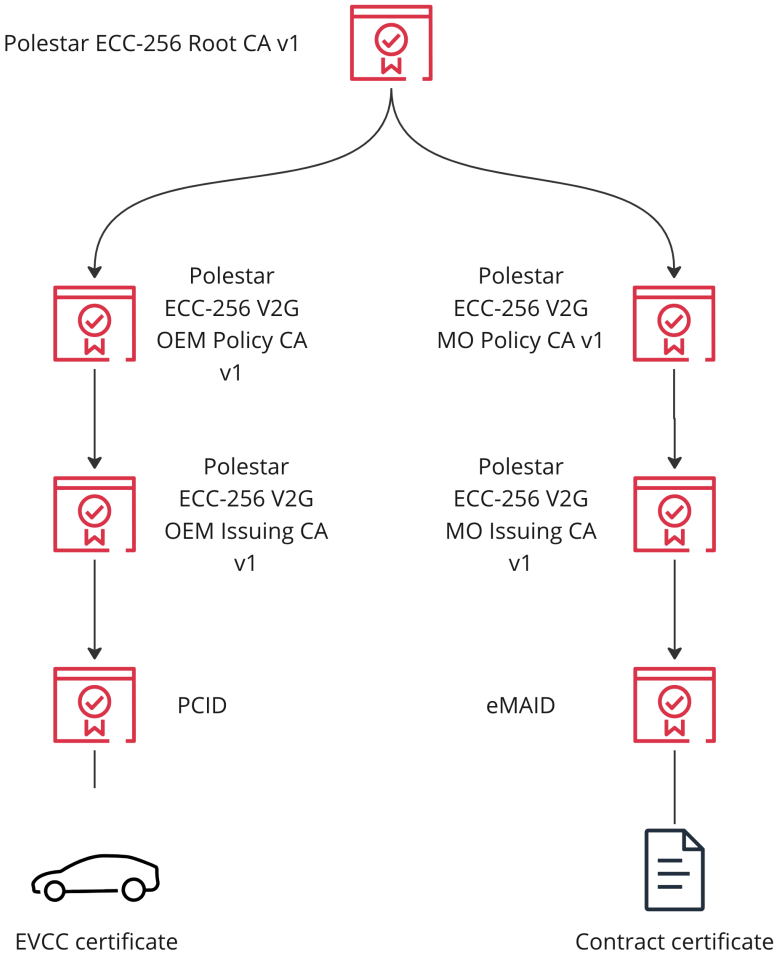


*Figure 2 Polestar ISO15118-2 V2G PKI CA chains for OEM and MO branches*

### 1.3.2 Certification authorities

CAs in this PKI SHALL have, at least, the responsibilities listed below. All items are further specified in other sections in this document.

- Generating signing key pairs for themselves
- Subordinate CAs will submit Certificate Signing Requests to a superordinate CA for signing for each key pair
- Provide means for a Registration Authority to submit Certificate Signing Requests from prospective subscribers (issuing CAs) or subordinate CAs (root and policy CAs)
- Signing certificate requests after successful validation
- Providing a means to submit revocation requests, and responding to those requests
- Keeping an audit trail of all signing and revocation activities

Each CA in this PKI MUST provide a Certification Practice Statement (CPS) documenting how compliance with this CP is achieved and which parts of this CP is implemented. The same CPS MAY cover more than one CA, if the same organization operates multiple CAs under this CP.

#### 1.3.2.1 Root CA

A root CA acts as the root of trust for a CA chain and eases the administrative burden for participants by creating a single top-level entity that can be trusted, instead of interacting and creating an explicit relation with every end entity directly.

Note that the root CA is not a direct participant in the V2G ecosystem, and MAY sign certificates for policy CAs outside V2G and thus outside this PKI. Such a policy CA – and its CA chain - SHALL NOT be governed by this CP. The root CA SHALL only be considered part of this PKI, and subject to this CP, when it is used in a certificate chain that includes a Polestar V2G Policy CA.

When evaluating trust, relying parties SHOULD verify that the policy CA in the chain is a V2G policy CA.

#### 1.3.2.2 PKI Operator

An organization operating a CA in the Polestar V2G PKI SHALL be a PKI operator. The CAs in the PKI MAY be operated by different PKI operators and discrimination by one PKI operator against another SHALL NOT be permitted.

The same PKI operator MAY operate more than one CA.

### 1.3.3 Registration authorities

Each CA in this PKI SHALL provide a Registration Authority (RA) that is the point of contact for submitting CSR's.

The CA MAY operate the Registration Authority directly, or it MAY use a third party to perform the RA activites on its behalf. Such an arrangement SHALL be governed by a Registration Authority Agreement.

An RA in this PKI SHALL have the following responsibilities:

- Receive requests using a documented and published mechanism and process
- Perform identification and authentication of applicant
  Verify that requests are technically correct and complies with this CP with respect to the certificate profile the applicant has applied for
- Formally accepting or rejecting certificate applications
- Submitting requests to the CA and retrieving the responses
- Sending notifications or certificates back to the applicant
- Registering issued certificates in certificate repositories, where applicable
- Keeping an audit trail of certificate applications
- Registering subscriber contact information and authorized representatives

### 1.3.4 Subscribers

A subscriber is an entity, as described in [RFC3647], who contracts a CA and is authorized to submit certificate requests to the CA. Subscribers in this PKI are always organizational entities, and not natural persons or technical entities.

A subscriber is distinct from the certificate subject, who is the identified entity in a certificate. A subscriber MAY also be a subject, but in this PKI the subjects will normally be technical components and entities such as vehicle ECUs or CAs themselves. Note that in this document, when the term "subject" is used, it refers to end entities and not CAs (unless specified). The terms "end entity" and "subject" are considered interchangeable in this CP.

A subscriber who has applied for a certificate, but not yet received it, is referred to as an Applicant.

A subscriber in this PKI SHALL have the following responsibilities:

- Providing a means of contact and communication between the subscriber and RA
- Providing a list of authorized representatives
- Submitting certificate applications to the RA
- Accepting or rejecting issued certificates
- Using the certificate in accordance with this CP
- Notifying the CA without delay in case
  - The certificate data becomes inaccurate
  - The private key has been compromised
  - The private key has been destroyed or otherwise become unusable

### 1.3.5 Relying parties

Relying parties are all entities which rely on the security provided by the certificates issued by this PKI in any way. This includes any activity that uses authentication, encrypted communication, or digital signatures, where one or more parties uses certificates issued by this PKI.

Relying parties are normally not part of this PKI, or subscribers in this PKI, but they MAY be.

### 1.3.6 Other participants

#### 1.3.6.1 Plug and Charge ecosystem operators

This PKI provides certificates for Plug and Charge, which means that many different parties can be involved in any transaction. Plug and Charge has organized into ecosystems run by a central operator, who is responsible for defining specifics of how interoperability will be achieved, where [ISO15118] does not describe this in sufficient detail.

Ecosystems tend to be geographically consolidated per continent, and Polestar MAY participate in any number of ecosystems simultaneously.

The ecosystem operator has the following responsibilities:

- Provide documentated interfaces for the required certificate operations
    - Certificate repository management (add, remove, query)
    - Certificate request management (for contract certificates)
- Provide documented procedures for requesting and getting access to the ecosystem and interfaces provided, including the certificate pools described in section 161.3.6.2.

### 1.3.6.2 Certificate pool operators

The Plug and Charge ecosystem operator MAY define shared repositories of certificates that participants in the PnC ecosystem can subscribe to and use to look up information about other parties. For the relevant certificate types, those pools are the primary repositories of certificates issued by this PKI.

| Certificate pool | Certificate type |
|---|---|
| Root Certificate Pool (RCP) | Root CA certificates |
| OEM Provisioning Certificate Pool (PCP) | End entity OEM provisioning certificates |
| Contract Certificate Pool (CCP) | End entity contract certificates |

# 1.4 Certificate usage

## 1.4.1 Appropriate certificate uses

This Certificate Policy (CP) regulates use of certificates issued by Polestar's V2G PKI for the purposes of supporting all certificate use cases specified in [ISO15118], except for Private Environment use cases. Use cases outside of [ISO15118] neither supported or permitted.

Certificates signed by a CA in this PKI must only be used within the defined use cases in [ISO15118], and only by participants in this PKI as described in section 1.3 in this PKI.

A CA in this PKI SHALL only use its keys to sign certificates for subscribers, and sign CRL files.

Additionally, a private key whose corresponding public key is certified in a certificate issued in this PKI, must only be used in accordance with the specified KeyUsage and EnhancedKeyUsage attributes in the certificate, and as defined by the respective certificate profile in this CP and in [ISO15118].

Note that the root CA MAY sign a certificate for a Policy CA outside of this PKI. Such a CA will be governed by other CP's than this. See section 1.3.2.1.

## 1.4.2 Prohibited certificate uses

Certificates issued in this PKI SHALL only be used in accordance with this CP (in particular section 1.4.1) and [ISO15118]. Any other usage is not permitted.

# 1.5 Policy administration

## 1.5.1 Organization administering the document

This document is owned and published by Polestar's Information Security team ('InfoSec' henceforth) and may be contacted as noted in section 1.5.2.

## 1.5.2 Contact person

Questions regarding this CP or Polestar's V2G PKI can be addressed to the following email:

pki.support@polestar.com

## 1.5.3 Person determining CPS suitability for the policy

Polestar's InfoSec team is responsible, and solely authorized to, approve or reject a participating CA's CPS.

## 1.5.4 CPS approval procedures

Each CA in the PKI must publish a Certification Practice Statement (CPS) stating the CA's policies and practices, and how the CA will fulfill the requirements in this policy. The CPS shall conform to the standard defined for a CPS in [RFC3647].

The CA shall submit this CPS to the Polestar InfoSec team, who will perform a policy compliance assessment and produce a written statement stating either acceptance of the CPS, or rejection with documentation of identified gaps. Any identified gaps must be closed before the CPS can be accepted.

## 1.6 Definitions and acronyms

See the section Terms and abbreviations at the start of the document.

# 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 Repositories

This PKI maintains and operates one repository on the public internet accessible at: https://pki.polestar.com. The repository will be open and accessible without restriction or fees.

This repository contains:

- Policy documents (this CP document and CPS documents for all CA's in this PKI)
- CA certificates for all CA's in the PKI, including SHA2 fingerprints
    - Also available via http://pki-aia.polestar.com/
- CRL files for all CA's in this PKI that publish them, including SHA2 fingerprints
    - Also available via http://pki-cdp.polestar.com/

Subscribers or relying parties who needs to look up certificates and certificate information should primarily use the ecosystem provided certificate pools (see section 1.3.6). Those repositories are the primary source of certificate information. This CP does not regulate those repositories or their responsibilities. It is the ecosystem operator's responsibility to regulate and document them.

## 2.2 Publication of certification information

This PKI will, using the web repository defined in section 2.1, publish information regarding all CA's in this PKI. This PKI will not provide any other repository for certificates. End entity certificates will only be published in the respective ecosystem operators pool (see section 1.3.6) that is appropriate to the certificate type.

## 2.3 Time or frequency of publication

Any updated documents or files MUST be updated in the repository without undue delay, and no later than the first time the document or file is applicable or valid. Any document or file which has an associated expiry date (such as CRL) SHALL have an updated version published before the expiry date has passed.

In case of decommissioning of a CA there shall be a notice on the repository in advance, stating the final date for publication of updates and the final day of validity.

## 2.4 Access controls on repositories

Content update access is restricted to Polestar's InfoSec team. Read access to other participants in this PKI is not restricted.

# 3 IDENTIFICATION AND AUTHENTICATION

## 3.1 Naming

### 3.1.1 Types of names

Certificate holders in this PKI will be identified via the Subject attribute in the certificate. The name SHALL be a Distinguished Name (DN) conformant to [RFC5280] and [X.500], and the values of the name components SHALL be

set as specified in this section. Which Subject name components a subscriber's certificate shall include is precisely specified in the certificate profiles in section 7.1, and deviations SHALL NOT be permitted.

A DN MAY contain the following components, as required by the relevant certificate profile. Attributes included in the DN MUST be in the following list.

- DC: Domain Component. In V2G sometimes used to identify functions or entity types. Only allowed according to the certificate profiles.
- CN: Common name. An entity SHALL have a globally unique Subject DN. All certificate profiles in this CP allow one single combination of C, O, and DC components per certificate profile, which means that CN's must be unique per certificate profile.
- O: Organization. Organization SHALL be exactly: "Polestar Performance AB", excluding quote marks
- C: 2-letter country code for the entities country as per [ISO3166-1]. See the Attribute Processing section below.

The order of attributes in the Subject field SHALL be encoded in the order listed above. DomainComponent (if included) SHALL be encoded first, and Country SHALL be encoded last.

In some cases in this text, variables are used in the form "<variable>". All allowed variable names are listed in section 3.1.1.1, and shall be processed accordingly.

Wilcards ("*.polestar.com") SHALL NOT be used.

The Subject Alternative Name (SAN) extension SHALL NOT be used.

### 3.1.1.1 Attribute processing

| Variable name | Description |
|---|---|
| <c> | Country code, 2-letter country code as per [ISO3166-1]. For all end entities this shall either be 'SE', or the country code for the country where the end entity shall operate. Sub CA's operating in China MAY use 'CN'. All other entities must use 'SE'. |
| <EMAID> | e-Mobility Account Identifier – used for contract end-entity certificates. See Annex H.1 of [ISO15118-2]. Identifies a contract in Plug and Charge. |
| <g> | Generation, used to distinguish between CA's with the same type (<t> below). A new generation of CA is a separate, parallel hierarchy and shall not be considered the same logical CA (as may be the case of a renewed root certificate). Generation is denoted with a 'v' followed by an integer, starting with "v1" for the first generation. |
| <n> | Number. A PKI operator MAY deploy multiple CA instances that serve the same purpose (i.e signing requests for the same certificate profile) but are operated independently (such as serving different geographical regions). Each such independent instance SHALL have a unique number, which SHALL be sequentially assigned, counting from the creation of the CA key pair.<br>Each such instance SHALL have it's own CA signing key pair, but use the same DN attributes and values except for the Number field. All such CAs act as separate entities in the PKI.<br>For the first such CA instance the number field is optional and MAY be blank. All subsequent CA instances SHALL have its own unique and sequential number based on order of CA signing key generation.<br><br>A CA MUST describe in its CPS the different cases where numbering is used, and how a subscriber can determine which CA to apply to.<br><br>Note: Clustered software installations and similar solutions, where each instance uses the same signing keys and CA certificates, SHALL NOT constitute independent instances. |
| <PCID> | Provisioning Certificate ID. Identifies a vehicles' EVCC when requesting a contract certificate. The ID is technically bound to the charging controller, and not the vehicle. This must not be empty, and must uniquely and globally identify the EVCC. |
| <t> | Type is a combination of certificate usage scope and public key type supported.<br><br>Type SHALL be one of the following for a root CA:<br>• ECC-256<br>• ECC-521<br>• ECC-448 |

| | |
|---|---|
| | Type SHALL be one of the following for sub CA:<br>• ECC-256 V2G<br>• ECC-521 V2G<br>• ECC-448 V2G |

### 3.1.2 Need for names to be meaningful

Names used by subscribers are used determine the identity of the entity using the name. Therefore, the name SHALL use established norms and semantics to facilitate the identification of the Subject entity, and the Issuer entity. It is the subject's responsibility to prove adherence and compliance to the issuing CA.

Names SHALL conform to requirements from [ISO15118-2] and [ISO15118-20] in cases where the standards set any requirements, such as [ISO15118-2] Annex H.

### 3.1.3 Anonymity or pseudonymity of subscribers

Anonymity and pseudonymity SHALL NOT be permitted.

### 3.1.4 Rules for interpreting various name forms

Distinguished Names SHALL be interpreted according to [RFC5280] and [X.500].

### 3.1.5 Uniqueness of names

All entities in this PKI must have unique names. Upon receipt of a certification request an issuing CA shall verify that the requested Subject name, in addition to other requirements, is unique within the PKI.

### 3.1.6 Recognition, authentication, and role of trademarks

Subscribers shall not use names in certification requests that infringe upon the Intellectual Property rights of others. If a CA becomes aware of such an infringement, the CA shall be entitled to denying a certification request, or suspending an issued certificate.

## 3.2 Initial identity validation

### 3.2.1 Method to prove possession of private key

A certificate applicant SHALL prove possession of the private key corresponding to the public key in the certification request. The mechanism used to prove possession SHALL be submission of a Certificate Signing Request (CSR) in PKCS#10 form, described in [RFC2986], which SHALL contain the public key of the applicant, and be signed by the corresponding private key. This enables the RA to verify the applicants possession of the private key.

### 3.2.2 Authentication of organization identity

Organizations identified in a Subject DN's Organization attribute SHALL be validated before a certificate can be issued, in addition to other requirements for issuance. The validation SHALL examine the registered name(s), registered address, place of jurisdiction, and registration status of the organization. The name used in the Organization attribute must be one of the names found during this validation process.

The validation SHALL also verify that the applicant is an authorized representative of the organization.

The CA SHALL document the procedure for organization validation and the documentation of the process in the CPS.

### 3.2.3 Authentication of individual identity

For end-entities, in addition to the stipulations section 3.2.1, the RA SHALL ensure that the requesting entity is authenticated using a suitable technical protocol to support this.

The CA MAY enforce additional requirements, and SHALL document in its CPS any employed procedures.

For individuals interacting with the CA in a non-subscriber role, such as personnel operating a subordinate CA, the CA SHALL enforce validation, and subsequent authentication using a mechanism of their choice. Authentication mechanisms used SHALL be the CA's discretion, but SHALL NOT be based on OTP (One-time Passwords) sent via SMS messages.

For CA CSR's the receiving RA MUST validate thoroughly the identity of the applicant, and the submitted information. If both superordinate and the requesting subordinate CA are operated by the same entity, the validation is not necessary.

Validation methods may include:

- Government issued photo ID examination
- Passport examination
- Correspondance via telephone, postal mail, or email
- Identity based logon using multi factor authentication

The CA SHALL document in its CPS the procedure for validation and the documentation of the process.

### 3.2.4 Non-verified subscriber information

All information included in certificates SHALL be validated by the RA.

### 3.2.5 Validation of authority

No stipulation, see also section 3.2.2

### 3.2.6 Criteria for interoperation

When a new subordinate CA is to be added to the PKI, the superordinate CA must verify that the subordinate complies with its requirements, and that the sub CA has a published CPS that complies with this CP. The operator of the sub CA shall be validated and registered by the superordinate CA. The superordinate CA may request an audit, on-site of off-site, before approving the sub CA. This audit may include review of the CPS, inspection of facilities, and validation of procedures of the sub CA.

The superordinate CA shall respond to the request with a affirmative answer after the sub CA passes its requirements. The superordinate CA must archive all documentation aquired or produced during the approval process. The superordinate CA SHALL have documentation of the requirements and procedures for approving a sub CA.

## 3.3 Identification and authentication for re-key requests

### 3.3.1 Identification and authentication for routine re-key

The requirements for renewal of certificates are identical to the initial request (see 3.2). Renewal without re-keying is not allowed.

### 3.3.2 Identification and authentication for re-key after revocation

The requirements for renewal of certificates are identical to the initial request (see 3.2). Renewal without re-keying is not allowed.

## 3.4 Identification and authentication for revocation request

A CA receiving a revocation request must ensure that the request comes from, or is rightfully submitted on behalf of, the subject identified in the certificate. It is at the CA's discretion to sufficiently validate the request for revocation and what procedures are used for validation but must, at least, ensure that the requestor is the Subject in the certificate, or an authorized representative for the Subject's organization. The procedures must be documented in the CA's CPS.

Polestar's InfoSec team SHALL have the right to request revocation of a certificate from the CA that issued it.

# 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## 4.1 Certificate Application

### 4.1.1 Who can submit a certificate application

Certificate requests can be submitted to a CA in this PKI under the following conditions:

- An authorized representative of a subordinate CA can submit a certification request to a superordinate CA
- A registered subscriber, or an authorized and authenticated representative thereof, may submit a certification request to an issuing CA

Refer to chapter 3 for definitions regarding registration of Subscribers with a CA.

### 4.1.2 Enrollment process and responsibilities

The process for a subscriber to enrol with a CA is described in section 3.2, both for sub-CAs and end entities. The enrolment of end entities with an issuing CA is at the discretion of the issuing CA, but must ensure that all requests are authenticated and validated before issuance, and MUST describe this process in the CAs CPS document.

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

When receiving a certification request from an authorized representative of a subscriber the request SHALL be authenticated and validated by the RA as per section 3.2, and the results MUST be documented and archived. Sections 5.4 and 5.5 specifies logging and archival requirements and procedures.

### 4.2.2 Approval or rejection of certificate applications

The RA MUST reject any certificate request that does not comply with the requirements in this CP (in particular chapters 3, 4, and 7), or the applicable CPS. The RA MAY contact the applicant for clarifications or updates before a decision is made. After the applicant has made all requested information available the RA MUST make a decision to approve or reject the application.

### 4.2.3 Time to process certificate applications

A CA in this PKI MAY provide guarantees to its subscribers regarding processing times for applications, but is not required to do so. If such a guaranteed is provided, in the CPS or a separate subscriber agreement, the CA MUST abide by them. The time required to process an application MUST be reasonable.

If a CA does not provide guarantees regarding processing times, it MUST in its CPS detail expected processing times for applications. The CA MUST, on average, meet this expected processing time.

A CA SHALL plan to handle situations such as downtime due to maintenance gracefully so that no applicant is required to wait longer than the guaranteed or expected processing times. If downtime is expected to last longer than expected processing times, subscribers must be notified of this no later than the time when an application is submitted.

## 4.3 Certificate issuance

### 4.3.1 CA actions during certificate issuance

After successful validation by the RA the CA SHALL issue the certificate, and document and archive the process activities and results. Sections 5.4 and 5.5 specifies logging and archival requirements and procedures.

### 4.3.2 Notification to subscriber by the CA of issuance of certificate

Immediately following the signing of a certificate and the subsequent logging and auditing activities have been completed, the CA MUST make the signed certificate available to the applicant. The applicants receipt of the signed certificate SHALL be sufficient notification that the application has been approved.

If the applicant is an end entity, the notification SHALL happen over the technical channel provided by the CA, and delivery of the certificate to the end entity SHALL be sufficient notification. If the applicant is a CA notification SHALL be sent to the subscriber using the subscriber's registered method of contact.

## 4.4 Certificate acceptance

### 4.4.1 Conduct constituting certificate acceptance

Upon receipt of a certificate issued in this PKI the subscriber SHALL be responsible for inspecting the certificate and its contents. Any action other than notifying the CA that the certificate is not acceptable constitutes acceptance of the certificate.

In particular, installing and using the certificate SHALL constitute acceptance of the certificate.

### 4.4.2 Publication of the certificate by the CA

The CA will publish certificates for end-entities and CA's in this PKI as described in chapter 2.

### 4.4.3 Notification of certificate issuance by the CA to other entities

No stipulations.

## 4.5 Key pair and certificate usage

### 4.5.1 Subscriber private key and certificate usage

Certificates and their corresponding private keys SHALL only be used in the following ways and circumstances (ALL the following apply at all times):

- by the subscriber or end entity they certify
- in accordance with the usage attributes and validity times encoded in the certificate
- subscribers that are not the root CA must also act in accordance with the use cases defined in [ISO15118]

See also section 1.4 for further specifications of acceptable use, and section 6.1 regarding private key security.

### 4.5.2 Relying party public key and certificate usage

A relying party SHALL use a certificate and its public key to perform authentication of and end-entity in this PKI, validate integrity of signed data, or perform encryption of data intended for the end entity. These activities may include a number of substeps, including but not limited to:

- the relying party SHALL validate that the certificate chains to the expected root CA
- the relying party SHOULD validate that the certificate chains to a V2G policy CA
- the relying party SHOULD validate that the certificate has not been revoked

The specific steps taken SHALL follow the requirements from [ISO15118].

## 4.6 Certificate renewal

In this PKI, certificate renewal is defined as requesting a new certificate with the same associated key pair as a previously issued certificate. Renewal of certificates is not allowed in this PKI. All certificate applications MUST use a new and unused key pair. See section 4.7 below for re-keying an existing certificate.

## 4.7 Certificate re-key

Certificate re-key is the process for issuing a certificate to the same entity, using the same subject DN and other certificate data, and using a new key pair for the subscriber. The requirements for this process is the same as for requesting a new certificate for a new subscriber. Every CA in this PKI SHALL handle all certificate applications in the same manner, regardless of whether the request is for a re-key or a new certificate application. See chapter 3 and section 4.3.

## 4.8 Certificate modification

Certificate modification is not allowed in this PKI.

## 4.9 Certificate revocation and suspension

A sub CA or an end entity in this PKI may have its certificate revoked under certain circumstances (see section 4.9.1). A root CA certificate cannot be revoked, as it is self signed and acts as the trust anchor. It does therefore not have a superordinate authority that can revoke it.

### 4.9.1 Circumstances for revocation

A certificate SHALL be revoked by the issuing CA if any of these circumstances apply:

- The subscriber rejected the certificate as per section 4.4
- The CA receives an authorized and validated request from the subscriber to revoke the certificate (see section 4.9.2)
- The CA finds that the certificate does not comply with this CP, the CAs CPS, or the requirements in [ISO15118]
- The CA has reasonable reason to suspect the private key associated with the certificate has been compromised or exposed to unauthorized parties
- The CA becomes aware that the subscriber has lost control over the private key, or that the key has been destroyed.

A subscriber SHALL notify the CA in case they have lost control of the private key or if it has been destroyed.

A subscriber SHALL notify the CA that a certificate has become invalid in case the subscriber's circumstances change in a way that makes the current certificate inapplicable, outdated, or in any other way not compliant with the requirements in this CP. Examples of such an event is a name change of a subject. A CA SHOULD in this case decide to revoke the certificate. The criteria for this decision is up to the CA, but MUST be documented in the CAs CPS statement.

### 4.9.2 Who can request revocation

The following SHALL always be able to request revocation of a certificate:

- Polestar's Root V2G CA
- The CA that issued the certificate
- The subscriber who was responsible for the request of the certificate
- Polestar's InfoSec team

Any other participant MAY request revocation of any certificate, but the CA SHALL follow the criteria in section 4.9.1, and any additional criteria specified in its CPS when deciding to proceed with revocation.

### 4.9.3 Procedure for revocation request

Revocation of a certificate MUST be preceded by the issuing CA validating that the requestor is authenticated as per section 3.4 and that circumstances specified in section 4.9.1 exists.

### 4.9.4 Revocation request grace period

The process to revoke a certificate SHALL be started as soon as possible after the decision to revoke the certificate has been made. A CA MAY choose to implement a grace period during this process. The CA MUST document the grace period in its CPS.

### 4.9.5 Time within which CA must process the revocation request

A CA MUST in its CPS document the maximum time to completely process a revocation request. A CA MAY specify different revocation times for different certificate profiles.

### 4.9.6 Revocation checking requirement for relying parties

A relying party SHALL be responsible for checking whether a certificate is revoked during the validation process, as specified in [ISO15118]. As per [ISO15118], revocation checking of OEM certificate chains is optional, and revocation checking of CPO certificate chains is mandatory.

Additional requirements MAY be set by ecosystem operators or other parties. It is the relying party's own responsibility to follow such requirements. Polestar's V2G PKI provides revocation sources for all CA chains.

### 4.9.7 CRL issuance frequency (if applicable)

A CA in this PKI SHALL regularly issue a new CRL, even if no changes have happened.

- CRL of root CA: Issued no later than every 7 months
- CRL of policy CA: Issued no later than every 7 months
- CRL of issuing CA: Issued no later than every 10 days

Additionally, every CA in this PKI MUST issue a new CRL whenever a certificate signed by the CA has been revoked.

Every time a CRL is issued it SHALL be a full CRL. Delta CRLs SHALL NOT used by this PKI.

A certificate that has expired SHALL NOT be included in any CRL, even if it was revoked. An OCSP responder MAY respond with 'unknown' status for expired certificates.

### 4.9.8 Maximum latency for CRLs (if applicable)

A new CRL SHOULD be posted to the repository promptly after creation, with no undue delay. If the creation happens on normal schedule it MUST be posted to the repository before the validity period of the previous CRL expires.

### 4.9.9 On-line revocation/status checking availability

All CAs in this PKI SHALL provide a URL at which certificates can be checked for revocation. This URL SHALL be accessible by all parties without restriction or cost. A CA MUST in a CPS, service agreement, or similar, stipulate response times and uptime limits for its status checking services. Availability MUST be at least 99%, and response times MUST NOT be longer than 3 seconds for OCSP responders, and MUST NOT be longer than 15 seconds for CRLs.

### 4.9.10 On-line revocation checking requirements

No stipulations beyond section 4.9.6.

### 4.9.11 Other forms of revocation advertisements available

No stipulations.

### 4.9.12 Special requirements re key compromise

No stipulations.

### 4.9.13 Circumstances for suspension

Certificate suspension, when a certificate is temporarily marked as invalid and later reinstated, SHALL NOT be used in this PKI.

## 4.10 Certificate status services

No stipulations beyond section 4.9.

## 4.11 End of subscription

A subscription ends when a subscriber does not request a new certificate to replace an existing certificate when it expires, or is revoked.

## 4.12 Key escrow and recovery

Key escrow MUST NOT be used in this PKI.

# 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

## 5.1 Physical controls

The security controls guarding the physical aspects of the CA SHALL provide robust protection against unauthorized access to the CA's equipment, records, and staff and their working environment.

Additionally, the controls must work toward enabling continuous operation of the CA so that no preventable downtime occurs. This means that the operator of the CA MUST work proactively with the physical environment to ensure that facility services are functional, robust, and that backup equipment or fault-tolerant versions of systems, are deployed where necessary. The operator MUST also ensure that systems are in place to prevent or minimize damage from catastrophic events such as fire, floods, power outages, etc

The operator SHALL ensure that facilities designed for human access can be accessed by authorized personnel whenever needed and that working conditions therein remain within parameters at all times with regard to for example temperature, humidity, and light.

### 5.1.1 Site location and construction

The facility SHALL be so constructed as to deter and prevent unauthorized access, and detect any attempt to do so.

### 5.1.2 Physical access

All access to the CA MUST be monitored and audit records MUST be generated and archived according to chapter 5.4. All access MUST be by authorized personnel only.

### 5.1.3 Power and air conditioning

The power equipment and air conditioning equipment SHALL be constructed to ensure continuous operation and staff access.

### 5.1.4 Water exposures

The operator of the CA SHALL design the facilities to reasonably protect against water damage or flooding of the facilities to ensure continuous operation and staff access.

### 5.1.5 Fire prevention and protection

The operator SHALL design the facilities to reasonably protect against fire in the facilities to ensure continuous operation and staff access.

### 5.1.6 Media storage

The operator of the CA SHALL take sufficient measures to protect CA data stored on media (digital or otherwise) from damage, theft, or unauthorized modification using access controls, backups, and redundant storage, as necessary.

### 5.1.7 Waste disposal

The CA operator SHALL have procedures in place for waste disposal that prevents any disclosure of data to unauthorized parties. Data that has passed its retention period MUST be destroyed.

### 5.1.8 Off-site backup

The CA operator SHALL keep at least one (1) full backup of the CA in an off-site location so that operations can resume in case of destruction of the productive environment or any of its components. The CA operator MUST ensure no data is lost during such an event.

The off-site backup MUST ensure the same level of security as the productive environment. All requirements on the CA in this CP also apply equally to the off-site facility and the off-site backup.

## 5.2 Procedural controls

### 5.2.1 Trusted roles

The CA SHALL in its CPS define all roles needed for the operation of the CA, and the duties of each role. All tasks carried out within the CA MUST be defined as the responsibility of one or multiple roles.

The role design SHALL adhere to the principles of least privilege and separation of duties.

Roles and tasks SHALL be defined, designed, and assigned so as to minimize risk of, and opportunity for, collusion or assigning the same person multiple sensitive permissions.

Appointment of a person to a trusted role SHALL be subject to the personnel controls in section 5.3.

The following tasks MUST be performed by staff appointed to a Trusted Role. This CP does not specify names of the roles or fully define all their responsibilities and split of tasks between them, but defines minimum requirements and which tasks that MUST NOT be performed by a single role. The minimum persons for each task is defined in section 5.2.2.

- Validation of information in a certificate application or revocation request
- Acceptance and rejection of certificate application or revocation request
- Issuing or revoking certificates
- Activating HSMs and CA private keys

- Backup and restore of HSMs and private keys
- Backup and restore of CA service and data

Note that the statement “performing a task” does not have to mean actively and personally engaging in every single execution, such as validating requests and issuing certificates. An issuing CA MAY employ automated solutions to process high volumes of applications, in which case “performing a task” means to create and control the automated means to perform the task. The staff in the Trusted Role must be exclusively in control of the automated execution, and are fully responsible for the execution.

### 5.2.2 Number of persons required per task

All CAs in this PKI SHALL identify security sensitive tasks in its CPS, and the required roles needed to perform those tasks. Security sensitive tasks SHALL require multiple persons actively participating to prevent abuse.

Security sensitive tasks is up to the CA to define, but SHALL include at minimum:

- Generation or destruction of a CA private key or HSM
- Issuing or revoking a CA certificate
- Signing CRLs (for root and policy CAs)
- Backup and restore activities for HSMs or private keys

For root and policy CAs the execution of the these tasks have to be done on the site where the CA hardware and software is located and by physically interacting directly with the CA.

### 5.2.3 Identification and authentication for each role

The CA SHALL in its CPS document the required authentication mechanisms used for personnel. As a minimum all personnel executing security sensitive tasks MUST use multi factor authentication. The CA SHALL NOT use One-Time Passwords based on SMS text messages.

### 5.2.4 Roles requiring separation of duties

The CA SHALL document in its CPS which roles can and cannot be held by the same person at the same time. At minimum, the access to perform the following tasks MUST NOT be granted to the same person:

- Activating HSMs
- Activating key stores or key pairs and performing cryptographic operations with those keys
- Backing up HSMs

## 5.3 Personnel controls

### 5.3.1 Qualifications, experience, and clearance requirements

Each CA SHALL ensure that staff has the requisite skills, experience, and qualifications to perform their tasks.

Staff in a trusted role SHALL pass screening and background checks before appointment. The details of the screening procedure and requirements for passing SHALL be documented in the CPS.

### 5.3.2 Background check procedures

The CA SHALL define in its CPS the procedure for background checks, and SHALL be designed to support the CAs trustworthiness. The process SHALL validate that the employee’s competence is adequate, and that their background does not raise suspicion that the appointment may cause doubts regarding the CAs integrity.

### 5.3.3 Training requirements

The PKI operator organization SHALL ensure that all staff have the requisite training for the job function.

The PKI operator SHALL have documentation regarding the training requirements.

### 5.3.4 Retraining frequency and requirements

The PKI operator organization SHALL provide adequate training to ensure that staff continuously update their skill as necessary for the job function. The organization SHALL also actively review the staff’s skill level, and arrange for staff to attend training pertinent to the CA operation periodically.

The PKI operator SHALL provide documentation regarding the retraining requirements and frequency.

### 5.3.5 Job rotation frequency and sequence

No stipulation.

### 5.3.6 Sanctions for unauthorized actions

Unauthorized actions SHALL lead to sanctioning of the offending person. The person MAY be removed from any appointment to a trusted role.

### 5.3.7 Independent contractor requirements

Tasks in this PKI MAY be outsourced by a PKI operator to subcontractors. In such cases all requirements in this CP still holds, just as if the person was employed directly by the PKI operator. The PKI operator SHALL retain all responsibility and accountability even if tasks are outsourced to a third party.

### 5.3.8 Documentation supplied to personnel

Staff SHALL have access to sufficient and complete documentation in order to perform their duties. Staff SHOULD NOT have access to documentation beyond what they need to perform their duties.

## 5.4 Audit logging procedures

Information about all significant activities SHALL be captured by the CA or RA and recorded in an audit log. Audit logging from all CA and RA activities SHALL at least contain date- and timestamps of the event, the identity of the originator of the event, and the event type as defined in the following section. Logs must be stored in such a way that modification or deletion of log files – intentional or otherwise – will be detected and can be recovered.

Logs MUST be stored in either physical or digital form, and which form chosen is at the CAs discretion.

### 5.4.1 Types of events recorded

Both successful and unsuccessful events SHALL be captured. In this section the term “CA system” is used to denote both the actual CA software, as well as any supporting systems or platforms like HSM’s, operating systems, database systems, programming runtimes and API’s, etc. The letters ‘C’, ‘R’, ‘U’, ‘D’ will be used in different combinations to denote Create, Read, Update, and Delete operations.

System level events:

- Account management: CUD events regarding accounts, groups, roles, and such artifacts that grant access to the CA systems.
- Authentication settings: CUD events regarding authentication of personal or machine accounts with access to the CA systems
- Network connections established between CA systems
- Log in and, where possible, log out events of CA systems
- Security settings: CUD events for security parameters of CA systems
- Operational settings: CUD events for runtime parameters of CA systems (including stopping and starting software or operating systems)
- Software lifecycle: Software installation, upgrading, patching, and removal
- Database: CRUD events regarding CA data inside database or application storage

RA events:

- Receipt of certificate application
- Receipt of a revocation request
- Submission of a certificate request to the CA
- Receipt of a signed certificate from the CA
- Distribution of a signed certificate to a subscriber

CA events:

- Receipt of a certificate request from RA
- Receipt of a revocation request
- Signing of a certificate
- Sending a signed certificate to RA
- CRUD events for key pairs
- Data exports from CA database or cryptographic material
- Usage of cryptographic material belonging to the CA.

Administrative events:

- Access management: addition, modification, or removal or staff members access permissions

### 5.4.2 Frequency of processing log

Audit logs SHALL primarily be processed automatically whenever possible to detect anomalies and security incidents in CA systems as quickly as possible. For offline CAs or other situations where automated processing is not possible the logs SHALL be inspected manually on each activation of the CA.

CAs that process logs automatically MUST also ensure that the results of automatic processing is acted upon if anomalies are detected.

Log processing and review SHALL entail verifying that the logs have not been tampered with and that the recorded events are expected and can be traced back to the normal CA activities. Any deviations SHALL be reported immediately to the relevant personnel and to the owners of this CP, see section 1.5.2.

### 5.4.3 Retention period for audit log

System level events defined in 5.4.1 SHALL be logged and retained until both the following are fulfilled:

- the next full audit has been performed
- at least 3 years has passed

RA, CA, and administrative events defined in 5.4.1 SHALL be logged and retained until until the CA ceases its operation, at which point it SHALL be archived by Polestar.

A PKI operator MAY scrub personal information from such logs as per legal or contractual requirements. The requirements for scrubbing personal data SHALL be documented by the PKI operator and the PKI operator SHALL notify Polestar before a purge occurs. Before scrubbing is done, a time period audit SHALL be performed.

### 5.4.4 Protection of audit log

Each PKI operator SHALL protect the integrity of the audit log in transit and storage. The audit log SHALL be protected by access control measures as defined in each CAs CPS. The CPS MUST document which roles are permitted what type of access to the logs, and under which circumstances.

### 5.4.5 Audit log backup procedures

Audit logs SHALL be included in the backup procedures for the CA and MUST be backed up – fully or incrementally - at least daily for online CA systems.

Audit logs for offline systems are recorded manually. The generated audit logs MUST be stored in safe locations with protections against device failures.

### 5.4.6 Audit collection system (internal vs. external)

No stipulation

### 5.4.7 Notification to event-causing subject

No stipulation

### 5.4.8 Vulnerability assessments

Vulnerability scanning SHALL be employed to assess online systems regarding runtime vulnerabilities in software or hardware. A vulnerability management process SHALL be employed that in addition to the above also assesses policies, offline services, procedures, and practices used by the CA. The results SHALL be documented and shared with the owner of this CP, see section 1.5.2.

## 5.5 Records archival

### 5.5.1 Types of records archived

PKI operators in this PKI MUST archive at least:

- All logs generated in section 5.4 in accordance with requirements in that section
- Certificate application information and any supporting documentation
- CA certificates
- Signed certificates
- Certificate revocation information and the latest CRL
- Key ceremony reports
- Audit log review logs
- Audit reports according to chapter 8
- Configuration sets and changes to configuration, using some form of version control
- Policy documents including historical versions

### 5.5.2 Retention period for archive

Each PKI operator SHALL maintain the archive for a CA it operates until the CA ceases operation.

When a CA ceases to operate, the PKI operator SHALL turn over the archive to Polestar, who will assume the responsibility to store and maintain the archive for the duration of the retention period.

### 5.5.3 Protection of archive

The archive SHALL be protected by procedures and technical controls to ensure that is will be available and protected from unauthorized tampering for its entire life span.

### 5.5.4 Archive backup procedures

No stipulation. Every PKI operator SHALL document the backup parameters in the CPS.

### 5.5.5 Requirements for time-stamping of records

All records SHALL contain accurate time stamps.

### 5.5.6 Archive collection system (internal or external)

No stipulation

### 5.5.7 Procedures to obtain and verify archive information

Only persons in appropriate Trusted roles may obtain the archive. Restored archives must be verified for integrity.

## 5.6 Key changeover

Re-key requirements are specified in section 4.7. When a CA certificate is approaching its renewal period it SHALL prepare by generating a new key pair, and requesting a new CA certificate. The CA SHALL make the new certificate available to subscribers before the renewal period has passed, see sections 2.2 and 4.4.2.

A CA key changeover SHOULD provide overlap between the new and the old CA certificate so that subscribers always chain to a currently valid CA certificate for the full validity period of the subscribers certificate.

## 5.7 Compromise and disaster recovery

### 5.7.1 Incident and compromise handling procedures

Each CA in this PKI SHALL have a described Incident Management procedure for handling both operational incidents and security incidents. If a security incident has occurred that can be reasonably suspected to affect the integrity of the CA, the CA must be stopped until the incident has been resolved. An investigation into the root cause SHALL always be performed, and included in any report that is submitted to the owner of this CP, as per below.

Operational incidents SHALL be notified to the owner of this CP (see section 1.5.2) if they affect operations in such a way that subscribers will be impacted.

Security incidents MUST likewise be notified, regardless of impact, to the owner of this CP (see section 1.5.2).

Notifications MUST happen within 24 hours of the PKI operator becoming aware of them, but they SHOULD be sent as soon as possible.

A CA MAY delay up to two hours for initial analysis of events, to determine whether it should be classified as an incident or false alarm before notification. If no determination can be made in that time, notification MUST be sent about a suspected incident.

### 5.7.2 Computing resources, software, and/or data are corrupted

Each CA SHALL have a documented plan to recover the CA systems and all supporting functions to a normal running state in case of corruption of the computing environment. The CPS SHALL outline the procedures for recovery.

### 5.7.3 Entity private key compromise procedures

Each CA SHALL in its CPS document its procedures in case of a compromised private key. At least, the procedures SHALL include

- notification to all subscribers of the compromise. Notification MUST happen within the time frame specified in 5.7.1.
- the CA MUST stop all operations, in particular any automated interfaces for certificate issuance.

If a CA determines it can recover a secure and operationally stable environment, it MAY do so. The CA SHALL

- Request revocation of its CA certificate to its superordinate CA immediately
- Generate a new CA key pair and request a new CA certificate
- Distribute the new CA certificate
- Restart the operations so subscribers can reapply for new certificates.

### 5.7.4 Business continuity capabilities after a disaster

Each CA in this PKI SHALL hava a documented Business Continuity Plan (BCP) that is continually developed and tested. In the BCP the CA SHALL describe how situations where business continuity is impacted can be either avoided, or the impact minimized. The BCP SHALL describe values for Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all components of the CA.

## 5.8 CA or RA termination

When a decision about terminating a CA or RA has been made its subscribers SHALL be notified by the CA as soon as possible. The following information MUST be given to subscribers as soon as possible:

- The date when CA services will be terminated (i.e shut off)
- The last date for requesting new certificates from the CA
- If the CA will be replaced, information for subscribers how contact the new CA

Termination of a CA SHOULD NOT happen before the CAs certificate expires. If termination is needed prematurely the following MUST be done:

- All active certificates issued by the CA must be revoked with a status of ‘Cessation of operation’
- A CRL MUST be issued that covers the entire remaining validity period of the terminated CAs certificate
- The CA signing key MUST be destroyed on the day of termination.

Certificate lifespans SHOULD not be impacted by CA certificate terminations. That means termination of a CA SHOULD be decided well in time before the point when certificates with the maximum allowed lifespan cannot be signed by the CA.

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 Key pair generation and installation

### 6.1.1 Key pair generation

Key pairs for a CA in this PKI MUST be generated during an audited Key Generation Ceremony. The ceremony SHALL be documented and audited, and the documentation SHALL be archived according to section 5.5. Attendants SHALL attest the authenticity of the audit log.

Key generation for all CAs in this PKI SHALL be done in a Hardware Security Module certified to at least one of the following specifications, and at least to the level listed for each:

- [ISO/IEC 19790] level 3
- [FIPS 140] level 3
- [ISO/IEC 15408] EAL level 4

Key pairs for end-entity subscribers in this PKI SHALL be generated by the subscriber or a trusted intermediary. End entity subscribers MAY use an intermediary party to facilitate the requests and key pair generation which is then installed in the subscriber device. The subscriber SHALL be responsible for ensuring the security of the intermediary and the communication channels and mechanisms used to transport and install the key pair in the subscriber device. The security controls protecting a private key during transport MUST reasonably ensure that no unauthorized access to the private key is possible, and that the private key SHALL NOT be stored anywhere else than in the subscriber device.

### 6.1.2 Private key delivery to subscriber

Key pairs for subscribers in this PKI SHALL NOT be generated by the CA. There is no need for a CA to distribute private keys, and it is not permitted in this PKI.

### 6.1.3 Public key delivery to certificate issuer

Public keys are generated by the subscriber and submitted to the CA by using PKCS#10 encoded Certificate Signing Requests.

### 6.1.4 CA public key delivery to relying parties

The root CA SHALL publish its CA certificate to the Plug and Charge ecosystem operator's mechanism, as per section 1.3.6 and on Polestar's online PKI repository described in section 2.1. All relying parties MUST retrieve the root CA certificates from one of these locations and install them locally in whatever fashion is appropriate for them.

### 6.1.5 Key sizes

Certificates applications in this PKI MUST use public keys compliant with [ISO15118]. Certificate applications with key types or sizes not explicitly allowed by [ISO15118] MUST be rejected.

### 6.1.6 Public key parameters generation and quality checking

Public key parameters MUST be validated by a CA when requested to sign a certificate. The parameters MUST comply with [ISO15118] and the certificate profiles in section 7.1. Requests that do not comply with this requirement MUST be rejected by the CA.

### 6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Usage of keys signed into subscriber certificates in this PKI MUST be used as defined in [ISO15118]. Any use outside of this is not permitted. See section 1.4. Allowed key usage is also encoded into the KeyUsage attribute in certificates, as per the certificate profiles in section 7.1.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic module standards and controls

HSM' used by CAs in this PKI SHALL be certified to at least one of the following specifications, and at least to the level listed for each:

- [ISO/IEC 19790] level 3
- [FIPS 140] level 3
- [ISO/IEC 15408] EAL level 4
- A standard approved by Polestar's InfoSec team offering similar security guarantees as the standards above.

A CA in this PKI MUST NOT use private keys stored outside of an HSM.

A CA in this PKI SHALL document in its CPS to which standards their HSM devices are certified.

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

All CAs in this PKI MUST enforce multi-person control for creating new keys on an HSM, and copying, backing up, or restoring private keys to or from an HSM.

The CA's procedures for multi-person access control SHALL be documented in its CPS.

#### 6.2.2.1 Root and policy CA

For root CAs and policy CAs the HSMs storing the CA private keys MUST enforce multi-person access control to prevent any single individual to access and activate key material. Activation data and access keys or cards MUST also be protected in a tamper-evident manner so any attempt to bypass the controls will be detected.

#### 6.2.2.2 Issuing CAs

For CAs signing end-entity certificates there is no added requirement beyond section 6.2.2.

### 6.2.3 Private key escrow

Key escrow SHALL NOT be used in this PKI.

### 6.2.4 Private key backup

CA private keys in this PKI MUST use some form of backup to protect against failures, including catastrophic loss of a facility. See section 6.2.6 for requirements on private key transfers.

The private key backup strategy MUST allow for private keys to be destroyed from backups when a key is slated for destruction.

Backup keys MUST be regularly tested to ensure the restore process works.

The CA SHALL document the backup procedures in its CPS, including restore testing.

### 6.2.5 Private key archival

Private key archival SHALL NOT be used in this PKI.

### 6.2.6 Private key transfer into or from a cryptographic module

Private keys MAY be transferred for the purposes of backup and restore procedures, as per section 6.2.4.

Private keys MAY be transferred between HSM devices for the purposes of configuring clustering or failover technologies to support high availability.

When private keys are transferred out of an HSM device it must be protected by encryption (key wrapping) using the HSM manufacturer's supported mechanism. The key MUST be protected before leaving the HSM device, and the protection MUST remain until the key is stored in the destination HSM.

A private key for a CA in this PKI SHALL NOT be stored or transported in plain text form outside an HSM.

### 6.2.7 Private key storage on cryptographic module

No stipulation beyond section 6.2.1.

### 6.2.8 Method of activating private key

A CA SHALL require activation of the HSM and key before the key is in an operative state. Activation MUST be performed by a person in a trusted role, and adhere to the m-of-n control requirements in section 6.2.2 and activation data requirements in section 6.4.

### 6.2.9 Method of deactivating private key

If a HSM is facing a predictable and extended period of inactivity (such as an HSM used in an offline CA system) the key and HSM MUST be deactivated. The CA SHALL document in its CPS how it defines a predictable period of inactivity, and the procedures for protecting a HSM in an inactive state.

### 6.2.10 Method of destroying private key

When a CA certificates validity period has expired the CA SHALL destroy the private key, including backup copies. The destruction SHALL use the HSM manufacturer's mechanism for destroying keys.

### 6.2.11 Cryptographic Module Rating

See section 6.2.1

## 6.3 Other aspects of key pair management

### 6.3.1 Public key archival

Each CA SHALL archive its own CA certificates, and therefore its public keys. Root and policy CAs SHALL also archive the CA certificates it has signed.

### 6.3.2 Certificate operational periods and key pair usage periods

This CP defines validity period and key (pair) usage period as follows:

- **Validity period**: the time span during which signatures made with the key pair is to be considered valid with respect to time. When validating a certificate a relying party MUST consider the certificate invalid if the validity period encoded in the NotAfter attribute has expired for ANY certificate in the chain.
- **Key (pair) usage period**: The period during which the key pair will be used to sign new certificates. After this period has elapsed the private key SHALL NOT sign any new subscriber certificates. OCSP signer certificates and CRL files may be signed during the entire validity period, however.

Validity period and key pair usage period SHALL start immediately when the certificate becomes valid.

Validity period and key pair usage period will end immediately if a certificate is revoked.

A CA SHALL NOT sign any new certificates with a key pair after its key pair usage period has ended. That means that it must request a new certificate from its superordinate CA in order to sign new certificates after the key pair usage period ends.

For end entity certificates the validity period and key pair usage period are typically equal. For CA certificates and OCSP signer certificates, refer to the following table for *maximum* periods. A sub CA MAY choose shorter periods.

| Certificate type | Validity period | Key usage period |
|---|---|---|
| Root CA | 40 years | 20 years |
| Policy CA | 30 years | 5 years |
| Issuing CA | 25 years | 1 years |
| OEM provisioning | 20 years | No longer than the validity period |
| Contract | 1 day - 2 years | No longer than the validity period |
| OCSP responder | 13 months | No longer than the validity period |

# 6.4 Activation data

## 6.4.1 Activation data generation and installation

Activation data for a CA key SHALL be generated when the key is generated. The exact nature of the activation data (PINs, passwords, hardware tokens, etc) SHALL be described by the CA in its CPS. The documentation SHALL include the following properties regarding credentials:

- Strength (i.e password length, complexity, etc)
- Rotation periods – max age of secrets before they must be changed
- Circumstances under which rotation must happen. Knowledge based credentials MUST be changed whenever a person who has had access to the credential loses the access

## 6.4.2 Activation data protection

Each CA MUST protect the activation data from unauthorized access. It SHALL describe the security controls for activation data in its CPS.

## 6.4.3 Other aspects of activation data

No stipulation.

# 6.5 Computer security controls

## 6.5.1 Specific computer security technical requirements

CAs is this PKI MUST ensure that CA systems apply robust technical controls to ensure the trustworthiness of the provided services. On computer systems that means applying technical controls to support the security requirements in this CP. On a high level that means computer systems at least must implement the following:

- Secure identity lifecycle controls
    - Ensure identities are personal, valid, and current
    - Ensure identities are deleted/deactivated when no longer needed
- Strong authentication controls
    - Strong passwords
    - Rotation of knowledge-based secrets
    - Multifactor authentication where technically possible
- Role-based access controls
    - Segregation of concerns
    - Least privilege
- System hardening
    - Implement a local security baseline based on an established hardening framework (such as STIG or CIS benchmarks) to strengthen security of a running operating system
- Network security controls
    - Reducing attack surface on network connections by closing unnecessary ports/services
- Auditing and logging
    - Changes to security parameters or runtime parameters
    - Access attempts, successful and failed, must be logged

- Backup
    - Systems must use backups to enable recovery of the service including all data after a failure

### 6.5.2 Computer security rating

No stipulation.

## 6.6 Life cycle technical controls

### 6.6.1 System development controls

The CA SHALL have a described process for the development and/or sourcing of systems and components comprising or supporting the CA systems. This process SHALL include risk analysis to capture the security aspects of any system or component before it is used in production CA systems or supporting systems.

### 6.6.2 Security management controls

CA systems and supporting systems SHALL implements security management controls to prevent execution of unauthorized software and prevent unauthorized modifications to runtime or security parameters of both computer systems and networks.

The controls SHALL also include checks of the integrity of software and firmware.

### 6.6.3 Life cycle security controls

Each CA SHALL describe in its CPS the policy regarding software and hardware lifecycle management. This includes software update and patching frequency and deployment stragegy, hardware lifespan, and hardware disposal procedure.

## 6.7 Network security controls

The network architecture for CA systems or supporting systems MUST be designed to provide a high level of security to prevent unauthorized access. The network MUST implement at least the following:

- Surface minimization (close unnecessary ports)
- Block network connections by default, with a documented process for allowing connections
- Remote access MUST use identity based strong authentication with role-based access controls
- Enforce encryption of connections over untrusted networks
- Strongly encourage encryption of connections on other networks, and require documentation of exceptions

## 6.8 Time-stamping

All CAs in this PKI SHALL use a reliable time source and document the time source in its CPS. The CPS SHALL include information of the frequency of time synchronization, procedure to discover discrepancies, and corrective procedures.

# 7 CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 Certificate profiles

Symbols in the tables are interpreted as follows:

| | |
|---|---|
| x | Required |
| (x) | Optional |
| - | MUST NOT be present |

| | |
|---|---|
| nc | Extension MUST be marked as non-critical |
| c | Extension MUST be marked as critical |
| <text> | Variable data, as specified in section 3.1 and in the Attribute Processing section (7.1.1) below |
| String starting with ”id-” | OID name |
| N.N.N.N | OID value, string of numbers separated by dots. |
| ”text” | Literal value. Certificate SHALL contain exactly this string, excluding quotation marks. |

### 7.1.1 Attribute processing

| Variable name | Description |
|---|---|
| <Signing CA name> | Used for OCSP responders. Replace with the Subject name of the CA for whom this responder signs OCSP responses and signs the responder’s certificate. |
| <Issuer CRL file> | File name of the signing CAs CRL file. Used in the CRL Distribution Point attribute. |

### 7.1.2 Version number(s)

All certificates shall be based on X509 version 3 (indicated by numeric value “2” in the version attribute encoded in certificates) and contain data as defined throughout section 7.1.

### 7.1.3 Guidance

1. [ISO15118-2] erroneously states that signatureValue in certificates shall be encoded as OCTET STRING. It SHALL be encoded as BIT STRING.
2. Root certificates SHALL NOT include revocation attributes (CRLDistributionPoints or AIA (OCSP))
3. Non-root CA certificates SHALL contain at least one of CRLDistributionPoints or AIA (OCSP) URLs for revocation checking. Both are marked as optional in the profiles below, but at least one is mandatory.
4. SerialNumber SHALL be non-sequentially generated and include at least 64 bits of random data.

### 7.1.3.1 OEM provisioning certificate profiles (ISO15118-2)

| | | Name | OEM Root CA | OEM Policy CA | OEM Issuing CA |
|---|---|---|---|---|---|
| | | Role | Root | Intermediate | Issuing |
| **Certificate** | | signatureAlgorithm | id-ecdsa-with-SHA256 | id-ecdsa-with-SHA256 | id-ecdsa-with-SHA256 |
| | | signatureValue | bit string | bit string | bit string |
| | | | | | |
| **tbsCertificate** | | Version | 2 | 2 | 2 |
| | | SerialNumber | Integer, 20 octets | Integer, 20 octets | Integer, 20 octets |
| | | Signature | id-ecdsa-with-SHA256 | id-ecdsa-with-SHA256 | id-ecdsa-with-SHA256 |
| | **Issuer** | Country | SE | SE | SE |
| | | Organization | Polestar Performance AB | Polestar Performance AB | Polestar Performance AB |
| | | Common Name | Polestar <t> Root CA <g> | Polestar <t> Root CA <g> | Polestar <t> OEM Policy CA <n> <g> |
| | **Validity** | | 40 years | 30 years | 25 years |
| | **Subject** | Country | SE | SE | SE |
| | | Organization | Polestar Performance AB | Polestar Performance AB | Polestar Performance AB |
| | | Common Name | Polestar <t> Root CA <g> | Polestar <t> OEM Policy CA <n> <g> | Polestar <t> OEM Issuing CA <n> <g> |
| | | Domain Component | - | - | - |
| | **SubjectPublic KeyInfo** | Public key | x | x | x |
| | | Cryptographic algorithm | id-ecPublicKey | id-ecPublicKey | id-ecPublicKey |
| | | Parameters | ECParameters | ECParameters | ECParameters |
| | | namedCurve | secp256r1 | secp256r1 | secp256r1 |
| | **Extensions** | AuthorityKeyIdentifier | x | x | x |
| | | SubjectKeyIdentifier | x | x | x |
| | | KeyUsage | x / c | x / c | x / c |
| | | digitalSignature | 0 | 0 | 0 |
| | | nonRepudiation | 0 | 0 | 0 |
| | | keyEncipherment | 0 | 0 | 0 |
| | | dataEncipherment | 0 | 0 | 0 |
| | | keyAgreement | 0 | 0 | 0 |
| | | keyCertSign | 1 | 1 | 1 |
| | | cRLSign | 1 | 1 | 1 |
| | | encipherOnly | 0 | 0 | 0 |
| | | decipherOnly | 0 | 0 | 0 |
| | | ExtendedKeyUsage | - | - | - |
| | | id-kp-clientAuth | - | - | - |
| | | id-kp-serverAuth | - | - | - |
| | | CertificatePolicies | - | - | - |
| | | BasicConstraints | x / c | x / c | x / c |
| | | isCA | 1 | 1 | 1 |
| | | PathLength | - | 1 | 0 |
| | | cRLDistributionPoints | - | (x)/nc http://pki-cdp.polestar.com/<Issuer CRL file> | (x)/nc http://pki-cdp.polestar.com/<Issuer CRL file> |
| | | AIA (OCSP) | - | (x)/nc http://pki-ocsp1.polestar.com/ | http://pki-ocsp1.polestar.com/ |

| | | | |
|---|---|---|---|
| | | Name | OEM Provisoning cert |
| | | Role | Leaf |
| **Certificate** | | signatureAlgorithm | id-ecdsa-with-SHA256 |
| | | signatureValue | bit string |
| | | | |
| **tbsCertificate** | | Version | 2 |
| | | SerialNumber | Integer, 20 octets |
| | | Signature | id-ecdsa-with-SHA256 |
| | **Issuer** | Country | SE |
| | | Organization | Polestar Performance AB |
| | | Common Name | Polestar <t> OEM Issuing CA <n> <g> |
| | **Validity** | | 20 years |
| | **Subject** | Country | - |
| | | Organization | Polestar Performance AB |
| | | Common Name | <PCID> |
| | | Domain Component | ”OEM” |
| | **SubjectPublic KeyInfo** | Public key | x |
| | | Cryptographic algorithm | id-ecPublicKey |
| | | Parameters | ECParameters |
| | | namedCurve | secp256r1 |
| | **Extensions** | AuthorityKeyIdentifier | x |
| | | SubjectKeyIdentifier | x |
| | | KeyUsage | x / c |
| | | digitalSignature | 1 |
| | | nonRepudiation | 0 |
| | | keyEncipherment | 0 |
| | | dataEncipherment | 0 |
| | | keyAgreement | 1 |
| | | keyCertSign | 0 |
| | | cRLSign | 0 |
| | | encipherOnly | 0 |
| | | decipherOnly | 0 |
| | | ExtendedKeyUsage | - |
| | | id-kp-clientAuth | - |
| | | id-kp-serverAuth | - |
| | | id-kp-oCSPSigning | - |
| | | Id-pkix-oCSP-nocheck | - |
| | | CertificatePolicies | - |
| | | BasicConstraints | x / c |
| | | isCA | 0 |
| | | PathLength | - |
| | | cRLDistributionPoints | - |
| | | AIA (OCSP) | http://pki-ocsp4.polestar.com/ |

### 7.1.3.2 Mobility Operator certificate profiles (ISO15118-2)

| | | Name | MO Root CA | Mo Policy CA | Mo Issuing CA |
|---|---|---|---|---|---|
| | | Role | Root | Intermediate | Issuing |
| **Certificate** | | signatureAlgorithm | id-ecdsa-with-SHA256 | id-ecdsa-with-SHA256 | id-ecdsa-with-SHA256 |
| | | signatureValue | bit string | bit string | bit string |
| | | | | | |
| **tbsCertificate** | | Version | 2 | 2 | 2 |
| | | SerialNumber | Integer, 20 octets | Integer, 20 octets | Integer, 20 octets |
| | | Signature | id-ecdsa-with-SHA256 | id-ecdsa-with-SHA256 | id-ecdsa-with-SHA256 |
| | **Issuer** | Country | SE | SE | SE |
| | | Organization | Polestar Performance AB | Polestar Performance AB | Polestar Performance AB |
| | | Common Name | Polestar <t> Root CA <g> | Polestar <t> Root CA <g> | Polestar <t> MO Policy CA <n> <g> |
| | **Validity** | | 40 years | 20 years | 10 years |
| | **Subject** | Country | SE | SE | SE |
| | | Organization | Polestar Performance AB | Polestar Performance AB | Polestar Performance AB |
| | | Common Name | Polestar <t> Root CA <g> | Polestar <t> MO Policy CA <n> <g> | Polestar <t> MO Issuing CA <n> <g> |
| | | Domain Component | - | - | - |
| | **SubjectPublic KeyInfo** | Public key | x | x | x |
| | | Cryptographic algorithm | id-ecPublicKey | id-ecPublicKey | id-ecPublicKey |
| | | Parameters | ECParameters | ECParameters | ECParameters |
| | | namedCurve | secp256r1 | secp256r1 | secp256r1 |
| | **Extensions** | AuthorityKeyIdentifier | x | x | x |
| | | SubjectKeyIdentifier | x | x | x |
| | | KeyUsage | x / c | x / c | x / c |
| | | digitalSignature | 0 | 0 | 1 |
| | | nonRepudiation | 0 | 0 | 1 |
| | | keyEncipherment | 0 | 0 | 0 |
| | | dataEncipherment | 0 | 0 | 0 |
| | | keyAgreement | 0 | 0 | 0 |
| | | keyCertSign | 1 | 1 | 1 |
| | | cRLSign | 1 | 1 | 1 |
| | | encipherOnly | 0 | 0 | 0 |
| | | decipherOnly | 0 | 0 | 0 |
| | | ExtendedKeyUsage | - | - | - |
| | | id-kp-clientAuth | - | - | - |
| | | id-kp-serverAuth | - | - | - |
| | | CertificatePolicies | - | - | - |
| | | BasicConstraints | x / c | x / c | x / c |
| | | isCA | 1 | 1 | 1 |
| | | PathLength | - | 1 | 0 |
| | | cRLDistributionPoints | - | (x)/nc http://pki-cdp.polestar.com/<Issuer CRL file> | (x)/nc http://pki-cdp.polestar.com/<Issuer CRL file> |
| | | AIA (OCSP) | - | (x)/nc http://pki-ocsp1.polestar.com/ | http://pki-ocsp1.polestar.com/ |

| | | Name | Contract cert |
|---|---|---|---|
| | | Role | Leaf |
| **Certificate** | | signatureAlgorithm | id-ecdsa-with-SHA256 |
| | | signatureValue | bit string |
| | | tbsCertificate | |
| **tbsCertificate** | | Version | 2 |
| | | SerialNumber | Integer, 20 octets |
| | | Signature | id-ecdsa-with-SHA256 |
| | **Issuer** | Country | SE |
| | | Organization | Polestar Performance AB |
| | | Common Name | Polestar <t> MO Issuing CA <n> <g> |
| | **Validity** | | Up to 2 years |
| | **Subject** | Country | - |
| | | Organization | Polestar Performance AB |
| | | Common Name | <EMAID> |
| | | Domain Component | - |
| | **SubjectPublic KeyInfo** | Public key | x |
| | | Cryptographic algorithm | id-ecPublicKey |
| | | Parameters | ECParameters |
| | | namedCurve | secp256r1 |
| | **Extensions** | AuthorityKeyIdentifier | x |
| | | SubjectKeyIdentifier | x |
| | | KeyUsage | x / c |
| | | digitalSignature | 1 |
| | | nonRepudiation | 1 |
| | | keyEncipherment | 1 |
| | | dataEncipherment | 0 |
| | | keyAgreement | 1 |
| | | keyCertSign | 0 |
| | | cRLSign | 0 |
| | | encipherOnly | 0 |
| | | decipherOnly | 0 |
| | | ExtendedKeyUsage | - |
| | | id-kp-clientAuth | - |
| | | id-kp-serverAuth | - |
| | | id-kp-oCSPSigning | - |
| | | CertificatePolicies | - |
| | | BasicConstraints | x / c |
| | | isCA | 0 |
| | | PathLength | - |
| | | cRLDistributionPoints | (x)/nc http://pki-cdp3.polestar.com/<Issuer CRL file> |
| | | AIA (OCSP) | http://pki-ocsp3.polestar.com/ |

### 7.1.4 Certificate extensions

All approved extensions, and their values, are specified in the profile tables above. No other extensions are permitted in this PKI.

### 7.1.5 Algorithm object identifiers

All identifiers for algorithms MUST be used in accordance with [ISO15118]. See the identifiers in the tables above.

### 7.1.6 Name forms

See section 3.1.

### 7.1.7 Name constraints

Name contraints are not supported in this PKI.

### 7.1.8 Certificate policy object identifier

CP identifiers will not be encoded into certificates. The relevant extensions are not permitted in this PKI.

### 7.1.9 Usage of Policy Constraints extension

Policy constraints are not supported in this PKI.

### 7.1.10 Policy qualifiers syntax and semantics

No stipulations.

### 7.1.11 Processing semantics for the critical Certificate Policies extension

The Certificate Policies extension is not permitted in this PKI.

## 7.2 CRL profile

### 7.2.1 Version number(s)

The CRLs SHALL be based on X.509 version 2 (encoded as numeric value 1 in CRL files) in [RFC5280].

### 7.2.2 CRL and CRL entry extensions

The following extensions SHALL be encoded into CRL files:

- Authority Key Identifier
- CRL Number

## 7.3 OCSP profile

### 7.3.1 OCSP profile (ISO15118-2)

| | | Name | OCSP Responder |
|---|---|---|---|
| | | Role | OCSP signer cert |
| **Certificate** | | signatureAlgorithm | id-ecdsa-with-SHA256 |
| | | signatureValue | bit string |
| | | | |
| **tbsCertificate** | | Version | 2 |
| | | SerialNumber | Integer, 20 octets |
| | | Signature | id-ecdsa-with-SHA256 |
| | **Issuer** | Country | SE |
| | | Organization | Polestar Performance AB |
| | | Common Name | <Signing CA name> |
| | **Validity** | | Up to 13 months |
| | **Subject** | Country | SE |
| | | Organization | Polestar Performance AB |
| | | Common Name | Polestar OCSP responder |
| | | Domain Component | - |
| | **SubjectPublic KeyInfo** | Public key | x |
| | | Cryptographic algorithm | id-ecPublicKey |
| | | Parameters | ECParameters |
| | | namedCurve | secp256r1 |
| | **Extensions** | AuthorityKeyIdentifier | x |
| | | SubjectKeyIdentifier | x |
| | | KeyUsage | x / c |
| | | digitalSignature | 1 |
| | | nonRepudiation | 0 |
| | | keyEncipherment | 0 |
| | | dataEncipherment | 0 |
| | | keyAgreement | 0 |
| | | keyCertSign | 0 |
| | | cRLSign | 0 |
| | | encipherOnly | 0 |
| | | decipherOnly | 0 |
| | | ExtendedKeyUsage | x / nc |
| | | id-kp-clientAuth | - |
| | | id-kp-serverAuth | - |
| | | id-kp-oCSPSigning | x |
| | | Id-pkix-oCSP-nocheck | x |
| | | CertificatePolicies | - |
| | | BasicConstraints | x / c |
| | | isCA | 0 |

| | | | |
|---|---|---|---|
| | | PathLength | - |
| | | cRLDistributionPoints | - |
| | | AIA (OCSP) | - |

### 7.3.2 Version number(s)

The OCSP responder MUST support at least version 1 of the OCSP specification [RFC2560].

### 7.3.3 OCSP extensions

No stipulations.

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

## 8.1 Frequency or circumstances of assessment

Every participating CA and/or RAs in this PKI SHALL undergo regular compliance audits to ensure adherence to this CP and the CAs CPS.

- Each root or policy CA SHALL perform a full audit before any end entity certificates are issued from the certificate chain. A full audit SHALL happen at least every 3 years.
- Each issuing CA SHALL perform a full audit before it starts issuing certificates to end entities. A full audit SHALL happen at least every 3 years.

If any nonconformance is discovered, the next full audit SHALL happen within 12 months of the failed audit.

CAs and RAs in this PKI SHALL participate in the audit as directed by Polestar. The audited part SHALL bear their own costs for the efforts of the audit.

## 8.2 Identity/qualifications of assessor

The audit SHALL be performed by Polestar, or an auditor appointed by Polestar. Appointment SHALL be the sole discretion of Polestar.

## 8.3 Assessor's relationship to assessed entity

The assessor MUST NOT be an employee of the assessed entity or in any similar type of dependent relationship. The assessor MUST NOT be in a relationship with the assessed entity that compromises the ability to do a fair and balanced assessment.

## 8.4 Topics covered by assessment

All statements in this CP and the corresponding CPS MUST be covered by the assessment. The assessment SHALL verify:

- That issued certificates and the certificate application processes comply with the requirements in this CP. These requirements are described in chapters 3, 4, and 7.
- The CAs procedural, physical, and technical security controls are effective and comply with the requirements in this CP. These requirements are described in chapters 4, 5, and 6.

### 8.4.1 Root and Policy CAs

The assessment SHALL contain a full review of all signature operations and all access to the CA hardware and software.

### 8.4.2 Issuing CAs

For an issuing CA the volume of certificates will be too large to validate each certificate manually. Similarly, technical logs, access logs and the like will also be too large for manual inspection. The PKI operator is expected to perform monitoring via automated tools that can generate reports regarding policy compliance.

The compliance assessment SHALL be based on small random samples of data (certificates and logs), and the output of automated tools. If a CA issues multiple types of certificates, e.g certificates based on different profiles (see chapter 7), the sampling SHALL include certificates from all issued certificate types.

## 8.5 Actions taken as a result of deficiency

The assessor SHALL describe any deficiencies found in an audit report shared with Polestar. The PKI operator SHALL inform Polestar and take actions to mitigate or solve any flaws, weaknesses, or risks found during assessments without undue delay. The result of the mitigations and corrections SHALL be documented and submitted to Polestar.

## 8.6 Communication of results

The assessors report SHALL be communicated to Polestar within 14 days of completion of the assessment.

# 9 OTHER BUSINESS AND LEGAL MATTERS

## 9.1 Fees

Polestar will not collect any fees from any of the participants in this PKI, for the services provided as part of this PKI described in this CP. Polestar MAY collect fees from other services, such as consulting services, that are outside the scope of this CP.

## 9.2 Financial responsibility

### 9.2.1 Insurance coverage

CAs in this PKI SHALL have a reasonable level of insurance to cover liabilities caused by their own services and/or operations.

### 9.2.2 Other assets

CAs SHALL be sufficiently financed to maintain operations and processes to the degree required by this CP.

### 9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

## 9.3 Confidentiality of business information

### 9.3.1 Scope of confidential information

The following types of information SHALL be kept confidential. This is the minimum required set of information that shall be kept confidential, and participating CA MAY opt to keep additional information types private (except for information covered by section 9.3.2.

- CA private keys
- Passwords, PINs, access tokens, and similar data
- User names
- Audit logs
- Certificate application records

### 9.3.2 Information not within the scope of confidential information

The following information SHALL NOT be kept confidential by any participant in this PKI.

- CA certificates
- CRL files
- OCSP signer certificates
- This Certificate Policy

### 9.3.3 Responsibility to protect confidential information

Each participating CA is responsible for ensuring the confidentiality of the information they produce.

## 9.4 Privacy of personal information

Each CA in this PKI MUST consider laws, regulations, and contractual obligations in the markets where they operate and where their subscribers reside to ensure that they are in compliance. Privacy by design SHALL be a foundational design principle for all CAs in this PKI.

This PKI SHALL NOT sign certificates for persons, or include personally identifiable information in a signed certificate. This minimizes the risk for exposure of private information.

### 9.4.1 Privacy plan

No stipulation.

### 9.4.2 Information treated as private

No stipulation.

### 9.4.3 Information not deemed private

No stipulation.

### 9.4.4 Responsibility to protect private information

No stipulation.

### 9.4.5 Notice and consent to use private information

No stipulation.

### 9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

### 9.4.7 Other information disclosure circumstances

No stipulation.

## 9.5 Intellectual property rights

No stipulation.

## 9.6 Representations and warranties

No stipulation.

## 9.7 Disclaimers of warranties

No stipulation.

## 9.8 Limitations of liability

No stipulation.

## 9.9 Indemnities

No stipulation.

# 9.10 Term and termination

## 9.10.1 Term

This CP becomes effective on the date it is published, and remains effective until a new version is published.

## 9.10.2 Termination

This CP becomes effective on the date it is published, and remains effective until a new version is published.

## 9.10.3 Effect of termination and survival

Participants in this PKI are bound to the terms of this CP for as long as certificates are within their validity period.

# 9.11 Individual notices and communications with participants

No stipulation.

# 9.12 Amendments

This CP SHALL NOT use amendments. If any update is needed it SHALL be made in the form of a new version of this CP.

# 9.13 Dispute resolution provisions

No stipulation.

# 9.14 Governing law

No stipulation.

# 9.15 Compliance with applicable law

No stipulation.

# 9.16 Miscellaneous provisions

## 9.16.1 Entire agreement

No stipulation.

## 9.16.2 Assignment

No stipulation.

## 9.16.3 Severability

No stipulation.

## 9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

## 9.16.5 Force Majeure

No stipulation.

## 9.17 Other provisions

No stipulation.