PKI Policy

Certificate Policy / Certification Practice Statement (CP/CPS) For the Tesla V2G PKI

Prepared For:	Revision:	Completed:	Tesla Proprietary
Tesla Inc.	V 1.1	April 24, 2025	

The first version of the Internal Tesla Unified CP/CPS that was used as the basis for this V2G CP/CPS was prepared exclusively for the use of Tesla employees, authorized agents, and affiliated companies by Komar Consulting Inc.

This V2G CP/CPS is intended to be consistent with the Tesla Unified CP/CPS and can be shared with authorized partners of Tesla.

Written and Published by Tesla, Inc.

PKI Policy

Version	Date	Updated By	Comments	Status
0.1	1/1/2023	Secura	Final review & EV_PKI Audit	Draft
0.2	3/12/2024	Edouard Lafargue Seth Terashima	Improvements to wording, resolution of ambiguities, conciseness.	Draft
0.3	4/19/2024	Edouard Lafargue Seth Terashima Donald Chan		Draft
0.9	9/12/2023	Edouard Lafargue Seth Terashima	Version ready for legal review and EVPKI audit	Release Candidate
1.0	416/2025	Secura	Released Version	
1.1	4/19/2025	Edouard Lafargue	Add contract certificate profile, update critical field on key usage for all profiles	

Document Approval & Acceptance

Name	Status	Date
Nathan Crandall	Approved	04/28/25
Edouard Lafargue	Approved	04/28/25

Table of Contents

5 | Facility Management & Operations Controls 27

1. Introduction

ISO 15118-2:2014 (hereinafter ISO 15118-2) security relies on the ubiquitous use of X.509 certificates to identify and authenticate all actors that are involved in vehicle-grid interoperability applications. This means that for those certificates to provide security assurance, they must be issued by a robust and well– managed public key infrastructure (PKI) or an ecosystem of multiple PKIs, all managed to a consistent level of security.

Those PKIs are called "Vehicle to Grid" PKIs, or "V2G PKIs".

A V2G PKI has many participants. These include:

Vehicle owners who are issued "contract certificates" that represent their subscription to a charging service.

- "Mobility Operators" that sell those subscriptions to vehicle owners.
- "EV Supply Equipment", or simply "chargers", that vehicles connect to in order to receive energy.
- Operators of EV supply equipment, or "Charge Point Operators" in ISO 15118-2 terminology.
- Vehicles.
- Certification Authorities (CAs) that issue X.509 certificates for the actors described above.
- Registration Authorities (RA) that authenticate and verify requestors of certificates issuance from a Certification Authority.
- Subscribers that are issued X.509 certificates. An entity that relies on a certificate, for example to encrypt an email message to a recipient, is known as a Relying Party or Certificate User.

The degree to which a certificate user can trust the certificate is called the assurance level and depends on several factors. These factors include the practices followed by the CA in authenticating the entity identified in the certificate, the operating policies and procedures of the CAs, the overall security of the PKI, and the end-entity's adherence to obligations to protect its private key.

1.1 Overview

The Tesla V2G PKI issues certificates to provide assurance of entities named in certificates and to provide services related to the use of certificates as described in ISO 15118-2.

This Certificate Policy is a statement of the policies associated with all X.509 certificates issued by

Certification Authorities that are governed by this Policy. This Policy may be used for all entities, including Subscribers, Relying Parties, Registration Authorities, and others, that have a relationship with the Tesla V2G CAs governed by this Policy.

1.1.1 Certificate Policy (CP)

The Tesla V2G PKI issues certificates that may include a Certificate Policies extension to specify the level of assurance established by this Policy. Relying Parties can use this information to decide whether to trust a certificate.

The Tesla V2G PKI only offers one assurance level. Therefore, when no assurance level is asserted in a certificate, Relying Parties should assume the certificate provides the assurance level described in this Policy.

1.1.2 Relationship between CP & the Certification Practice Statement (CPS)

A CP asserts an assurance level for certificates issued by a PKI and can be used to determine common interoperability standards and common assurance criteria with other PKI domains.

A CPS states how the internal PKI establishes the level assurance defined in a CP. A CP can be applied to multiple CAs. A CPS provides a detailed and technical statement of the practices and procedures which a CA employs in managing certificates and related infrastructure to support the stipulations of the CP.

Tesla has elected to produce a combined version of the document (referenced as the CP/CPS document).

1.1.3 Scope

The Tesla V2G PKI exists to facilitate trusted electronic transactions for itself and for other entities, related to "Vehicle to Grid" operations such as charging or discharging vehicles, as described in ISO 15118-2.

This CP/CPS document describes a PKI designed to comply with ISO 15118-2, with all operations related to "Plug and charge". As standards evolve, the CP/CPS will evolve accordingly.

1.1.4 Interaction with PKIs External to Tesla

No stipulation.

1.2 Document Identification

This Certificate Policy is called the Certificate Policy/Certification Practice Statement for the Tesla V2G PKI.

The Tesla V2G CP/CPS OID is defined as:

```
{iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) Tesla (49279) PKI Policies
(2) Product Certificate Policies (3)} = {1.3.6.1.4.1.49279.2.3}

Tesla-V2G           ID::={id-certificate-policy 5}
```

For clarity, the certificate policy OID arc branch can be represented as follows:

```
1.3.6.1.4.1.49279          ; Tesla OID Arc
       .2                  ; PKI Policies
             .3            ; Product Certificate Policies
                   .5      ; Tesla ISO 15118 V2G PKI
```

1.3 PKI Participants

The following are roles relevant to the administration and operation of the Tesla PKI.

1.3.1 Policy Approval Authority (PAA)

The Policy Approval Authority (PAA) is a group of individuals responsible for reviewing, maintaining, approving, and updating this CP/CPS. They are also in charge of approving the addition of new CAs to the PKI.

1.3.2 Operational Authority (OA)

The Operational Authority is the Issuer that operates and maintains the PKI under direction from the PAA.

The OA's primary focus is to ensure that policies for secure physical and logical Access, data sharing, and communications across the ecosystem are realized through the execution and management of the CP requirements by the PKI Participants.

1.3.3 Certification Authorities

A Certification Authority (CA) is an entity that:

- Issues, signs, and revokes X.509 certificates that bind a Subscriber's public key and the Subscriber's X.500 Distinguished Name.
- Publishes certificate status data in Certificate Revocation Lists (CRLs).
- Implements operational practices to achieve the requirements of the CP.

Tesla operates a multi-tiered V2G PKI hierarchy of CAs to issue certificates to Subscribers. The hierarchy follows the structure described in ISO 15118-2 Annex E described below:

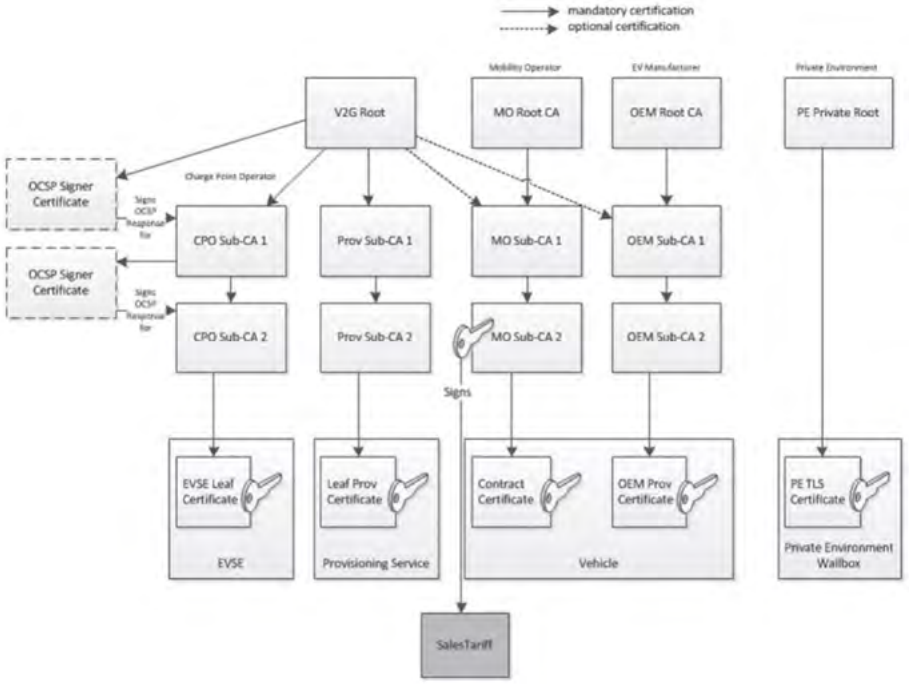

Figure 1 ISO 15118-2 Reference PKI structure

A CA may register Subscribers itself, or it may delegate this function to one or more separate agents, known as Registration Authorities (RA), in accordance with this Policy.

Where necessary, this Policy distinguishes the different users and roles accessing the Tesla V2G issuing CAs for CA functions. Where this distinction is not required, "CA" is used to refer to the total CA entity, including the software and its operations.

While it follows the general structure of the ISO 15118-2 PKI, the Tesla V2G PKI:

- Does not support a PE Private Root.
- Only implements a single V2G Root, and no separate MO Root CA.
- The Tesla OEM Root CA is part of the internal Tesla Product PKI and is not in scope for this document.

1.3.4 Registration Authority (RA)

A Registration Authority is an entity that is delegated authority by the CA to authenticate, collect, and verify Subscriber information for inclusion in X.509 certificates. An RA may make requests to issue or revoke certificates, but an RA does not sign certificates.

1.3.5 Subscribers

A Subscriber is an entity (user, device, application, or service) whose X.500 Distinguished Name appears in the Subject field of a certificate, with the exception that Certification Authorities (CAs) are not Subscribers.

Tesla V2G Subscribers include the following:

- Vehicle chargers, which are issued EVSE (EV Supply Equipment) Certificates. .
- Tesla vehicles, which are issued EV OEM Provisioning Certificates.
- Tesla Plug and Charge users, who are issued Plug and Charge Contract Certificates.

1.3.6 Relying Parties

Relying Parties are entities that rely on a Tesla Certificate for a purpose specifically enumerated as a supported function in Section 1.4.1. Relying Parties include:

- Tesla vehicle chargers
- Tesla vehicles
- Third-party chargers
- Third-party vehicles
- Mobility Operators
- Any other entity with an explicit contractual right to rely on certificates issued from this CA.

1.3.7 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued within the Tesla V2G PKI must be used in accordance with the use-cases described in ISO 15118-2.

The Tesla PAA may authorize additional uses at its discretion.

1.4.2 Prohibited Certificate Uses

Certificates issued within the Tesla V2G PKI must not be used for any purpose not explicitly allowed, or for any purpose prohibited by applicable laws.

1.5 Policy Administration

1.5.1 Organization administering the document

This CP/CPS is administered by the Tesla Policy Approval Authority (PAA).

1.5.2 Contact Person

Inquiries, suggestion, or notices regarding this document should be directed to:

Tesla Product Security
PKI operations
1501 Page Mill Road
Palo Alto, CA 94304

Email: vulnerabilityreporting@tesla.com

1.5.2.1 Incident Handling

The Operational Authority supports all investigations of incidents relating to the compromise or misuse of Private keys associated with a certificate signed by this CA. If you believe a private key issued by this CA may have been compromised, immediately contact the Operational Authority and request the creation of an incident.

Contact email: vulnerabilityreporting@tesla.com

1.5.3 CP/CPS Approval Procedures

The Tesla Operational Authority (OA) shall submit any requests for revision to the Tesla V2G CP/CPS to the PAA for approval.

The PAA shall accept or reject the CP/CPS. If rejected, the OA shall resolve the identified discrepancies and resubmit the revised CP/CPS to the PAA for approval. This process shall continue until the CP/CPS is approved.

1.6 DEFINITIONS AND ACRONYMS

See sections 11 and 12 in this document

---

2 Publication & Repository Responsibilities

2.1 Repositories

This document can be accessed at https://developer.tesla.com/docs/charging/public-key-infrastructure along with a copy of the Tesla V2G Root Certificate Authority certificate.

Certificate Revocation List distributions points and OCSP responder locations are not currently publicly accessible. Future revisions of this document will include public locations when they are deployed.

2.2 Publication of Certification Information

This document is kept in a version-controlled repository. Modifications to the publicly facing web page referenced above are subject to proper authentication and authorization, and all changes are subject to approval.

The current version of this CP/CPS document will be available permanently at the location provided in Section 2.2.2 of this document.

2.2.1 Publication of Certificates and Certificate Status

The CAs shall publish in the appropriate repository all CA certificates and CRLs.

2.2.2 Publication of CA Information

This CP/CPS is published at https://developer.tesla.com/docs/charging/public-key-infrastructure. All previous versions will remain available in the Tesla internal document management system.

2.2.3 Interoperability

Where possible, standards-based schemas and transports will be used to store and publish CA information.

2.3 Frequency of Publication

The CP/CPS will be modified as required, subject to the approval process described in Section 1.5.3 of this document.

Upon approval of any modification of this document, the current version will be published to the URI provided in Section 2.2.2. All previous versions will remain available in the Tesla internal document management system.

Certificates are published upon creation.

2.4 Access Controls on Repositories

The PAA shall make this CP/CPS publicly available as described in Section 2.2.2 for read-only access.

The CA shall protect Certificates and CRLs from modification or deletion. The CA shall make the CA certificates and revocation status publicly available for read-only access as described in Section 2.2.2.

---

3 Identification & Authentication

3.1 Naming

3.1.1 Types of Names

All Issuer and Subject Names in certificates issued by the CAs shall follow the X.500 naming standards for Distinguished Names (DN).

All certificates issued by CAs contain an X.501 DN in the Issuer Name and Subject name fields constructed by using all or a combination of any of the following attribute values supported by ISO 151182:

- Common Name (CN)
- Organization (O)
- Organizational Unit (OU)
- Country (C)
- Domain Component (DC)

Subscriber certificates Subject Name fields use the X.501 DN format constructed from the above fields.

Certificates may only contain Subject Name fields that comply with the requirements of ISO 15118-2 Annex F ("Certificate Profiles") for the appropriate certificate profile.

3.1.2 Need for Names to Be Meaningful

DNs must be meaningful to the Relying Parties that have a legitimate need to identify the Subscriber to fulfill their respective roles in ISO 15118-2.

For certificate profiles including an organizationName, The RA must use the verified company name or Subscriber name as the organizationName field in the Subject DN of the issued certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

The RA may assign DNs that are anonymous or pseudonymous from the perspective of Relying Parties that do not have a legitimate need under ISO 15118-2 to identify the Subscriber.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

DNs shall uniquely determine Subscribers.

3.1.6 Recognition, Authentication, & Role of Trademarks

The CA, and its RAs, shall not knowingly issue a certificate including a name that uses a third party's trademark or other Intellectual Property Rights.

Prospective Subscribers shall not knowingly use names in their certificate Applications that belong to someone else.

The CA or RA is not required to determine whether a Prospective Subscriber has Intellectual Property Rights or otherwise has legal agency in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any trademark and/or Intellectual Property Rights, including, without limitation, rights in a domain name, trade name, trademark, or service mark.

The PAA, and any CA shall be entitled, without liability to any Prospective Subscriber, to reject or suspend any Subscriber agreement because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The prospective Subscriber must demonstrate that it rightfully holds a private key corresponding to the public key to be listed in the certificate.

The method to prove possession of a private key shall be a certificate signing request in PKCS #10 format, or another cryptographically equivalent demonstration. This requirement does not apply when a key pair is generated by a CA on behalf of a Subscriber.

In the case a key pair is generated by a CA on behalf of a Subscriber, a secure delivery method must be used to ensure the private key is not disclosed during transport.

3.2.2 Authentication of Organization Identity

The RA shall verify that the identity of the organization:

- Is not on a government watch list at the CA's location;
- If the organization is on a watch list, it is up to RA's discretion to continue with the authentication;
- Conducts business at the address provided; and
- The verified organization or trade name is used in the *organizationName* field of the Certificate as a way for Relying Parties to Authenticate the organization name.

3.2.3 Authentication of Individual Identity

When certificates are issued to individuals the RA shall verify that the request was either issued by an approved organization, authenticated as per Section 3.2.2, or that the individual is authorized by the organization to be named in the certificate.

3.2.4 Non-verified Subscriber Information

The RA must verify all information included in a certificate.

3.2.5 Validation of Authority

The RA must verify the authority of individuals to request certificates and organizations to request certificates for themselves or on behalf of individuals and to act in trusted roles on behalf of the CA.

3.2.6 Criteria for Interoperation

The CA must determine the criteria for interoperability with another PKI subject to the policies defined in this CP. Those criteria are subject to approval by the PAA.

A Sub-CA certificate may be issued to an organization only after the PAA verifies that the Certificate Practice Statement of the Sub-CA complies with the stipulations of this Certificate Policy. At its discretion, the PAA can require an audit of the Sub-CA before approving the issuance of the Sub-CA certificate.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

Certificate re-key requests are treated as applications for new certificates.

3.3.2 Identification and Authentication for Rekey after Revocation

The RA must ensure that a root cause analysis of the issues leading to the need for revocation is performed, and that mitigations preventing the issues from reoccurring are in place before re-key can be authorized.

Subsequent certificate re-key requests are treated as applications for new certificates.

3.4 Identification and Authentication for Revocation Request

Requests to revoke certificates must be authenticated by the CA or the RA before being accepted. The parties that can request revocation of certificates are identified in Section 0 of this Policy.

Acceptable types of revocation requests:

- Request issued to the RA by the Subscriber or an authorized intermediary (see Section 3.2.5 using a pre-agreed secure channel such as secure email, or secure messaging.
- Request issued over an authenticated API operated by the CA.

---

4 Certificate Life-Cycle Operational Requirements

This Section describes the operational requirements imposed upon CAs, RAs, Subscribers, and other PKI participants, with respect to the lifecycle of a certificate.

4.1 Certificate Application

4.1.1 Submission of Certificate Application

The following entities may make an initial application for a certificate:

- -Any prospective Subscriber that operates or relies on EV charging services. - Individuals or organizations signing up for charging services.

All communications among CA, RA, PAA, OA and Subscribers supporting the certificate application and issuance process shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued. Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 CA Certificate Application

For CA certificates, application for the initial certificate is described in Section 3.2.6.

4.1.2.2 Subscriber Certificate Application

The applicant and the RA must perform the following steps for prospective Subscribers:

- Establish and record the identity of Subscriber, according to the requirements described in Section 3.2;
- Obtain a certificate signing request for each certificate; • Agree to any applicable Subscriber agreement, if required.

These steps may be performed in any order that is convenient for the RA and applicants, and that do not defeat security, in accordance with Section 4.1.1; but all steps must be completed prior to certificate issuance.

Public keys shall be delivered to the RA in a way that binds the applicant's verified identification to the public key being certified. This binding shall be accomplished using means that are as secure as the security offered by the keys being certified.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Identification and authentication of certificate applications must conform to the requirements specified in Sections 3.2 and 3.3 of this Policy.

4.2.2 Approval or Rejection of Certificate Applications

For a CA certificates, the PAA shall approve or reject a certificate request. For Subscriber certificates, the RA can approve or reject the certificate request.

4.2.3 Time to Process Certificate Applications

There is no stipulated time limit for the CA to process a certificate application. It is expected that applications will be processed within a reasonable time after all documents required for the application are received.

4.3 Issuance

4.3.1 CA Actions During Certificate Issuance

Upon receipt of a certificate request, the CA must:

- Authenticate the RA
- Verify the integrity of the information in the certificate request including the PKCS#10 CSR if included
- Generate a CSR if necessary
- Issue the certificate to the Subscriber
- Publish the certificate according to the stipulations in Section 4.4.2

4.3.2 Notification to Subscriber of Certificate Issuance

The CAs or the OAs shall notify Subscribers or the RA on behalf of the Subscriber when the certificate is issued and how to retrieve it.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

Unless the Subscriber explicitly rejects it, the certificate shall be deemed accepted.

4.4.2 Publication of the Certificate by the CA

The CA may publish the certificate as described in Section 2.2 of this Policy.

4.4.3 Notification of Certificate Issuance by the CA to other entities

The OA shall notify the PAA upon issuance of any CA certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers shall treat private keys as confidential and exercise due care and diligence to protect the private keys under their control from loss, disclosure, or compromise. Subscribers must:

- Use private keys in accordance with the stipulations described in this Policy.
- Use their certificates and private key only in a manner consistent with the profile of the certificates, including their keyUsage and extKeyUsage extensions
- Not use a certificate past its expiry date.
- Not use a certificate that has been revoked.

4.5.2 Relying Party Public key and Certificate Usage

Certificates contain information about their intended uses. Relying parties should have a basic understanding of the use and purposes of certificates.

Prior to relying on a certificate, Relying Parties must exercise due care and diligence to:

- Comply with all intended uses of the certificate as defined in the certificate extensions
- Assess the status of the certificate and all the CAs in the issuance chain.
- Only perform public key operations using a valid certificate (e.g. neither expired nor revoked)

Revocation status is not part of an issued certificate. Therefore, prior to relying on a certificate, Relying

Parties should ensure that the certificate has not been revoked by checking the most recently published Certificate Revocation List (CRL), OCSP responder data, or an equivalent agreed-upon mechanism.

A Relying Party should use discretion when relying on a certificate and should consider the risk of loss prior to relying on a certificate. Relying on a digital signature or certificate that has not been processed in accordance with applicable standards may result in risks to the Relying Party. The Relying Party is solely responsible for such risks. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the certificate.

4.6 Certificate Renewal

The terms “certificate renewal” and “certificate re-key” are sometimes used interchangeably, although they in fact differ from one another, to describe certificate replacement.

To avoid ambiguity, “certificate renewal” in this Policy means the replacement of a certificate using the same information—including public key information—as the previous certificate, with the exception of certificate validity period, thumbprint and serial number. That is, all certificate information remains the same, except

for the validity period, thumbprint and serial number. Because certificate renewal extends the lifetime of sensitive key material, which consequently results in increased vulnerability of key material to compromise, certificate renewal is not a preferred method for certificate replacement and its use is circumscribed by this Policy. The new certificate may also be signed by a different key.

4.6.1 Circumstance for Certificate Renewal

Only one circumstance for certificate renewal is permitted by this Policy. If the key material is stored on or secured by a smart card, secure element or a hardware security module and a renewal attempt occurs before the expiration of the certificate, certificate renewal is permitted.

A certificate may be renewed only if:

- The certificate is close to its expiration date.
- The private key is secured by a smart card, secure element or a hardware security module.
- The certificate is valid at the time a renew operation is requested.
- The Subject and other identifying information in the certificate do not change and meets the criteria stipulated in Section 3.1.1 of this Policy.

4.6.2 Who may request Renewal

The Subscriber, either directly or via an authorized entity (see Section 3.2.5), may request a certificate renewal.

4.6.3 Processing Certificate Renewal Requests

The CA processing a certificate renewal request must verify that the current certificate has not expired and has not been revoked prior to accepting a request for certificate renewal.

4.6.4 Notification of new certificate issuance to Subscriber

Subject to the same provisions as Section 4.3 of this Policy.

4.6.5 Conduct Constituting Acceptance of a Renewal certificate

Subject to the same provisions as Section 4.4 of this Policy.

4.6.6 Publication of the Renewal certificate by the CA

Subject to the same provisions as Section 4.4 of this Policy.

4.6.7 Notification of Certificate Issuance by the CA to other entities

Subject to the same provisions as Section 4.4 of this Policy.

4.7 Certificate Rekey

Certificate re-key is the preferred method for replacing a certificate prior to its expiration. When a certificate is re-keyed, a new certificate is created that retains the same information that describes the subject of the certificate. A new public/private key pair is created, and the new public key bound to the certificate. Also, a new serial number for the certificate is added. The new certificate may also be signed by a different key.

After a certificate re-key, the previous certificate must not be modified, re-keyed or renewed. The CA may revoke the previous certificate.

4.7.1 Circumstance for Certificate Re-Key

A certificate may be re-keyed only if the certificate is valid at the time a re-key operation is requested, and at least one of the following conditions is met:

- There is a suspected compromise of the private key material
- The certificate is close to its expiration date.

4.7.2 Who may Request Certification of a New Public Key

The Subscriber, either directly or via an authorized entity (see Section 3.2.5), may request a certificate renewal.

4.7.3 Processing certificate Re-Keying requests

Subject to the same provisions as Section 4.3 of this Policy.

4.7.4 Notification of new certificate issuance to Subscriber

Subject to the same provisions as Section 4.4 of this Policy.

4.7.5 Conduct constituting acceptance of a Re-Keyed certificate

Subject to the same provisions as Section 4.4 of this Policy.

4.7.6 Publication of the Re-Keyed certificate by the CA

Subject to the same provisions as Section 4.4 of this Policy.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

Subject to the same provisions as Section 4.4 of this Policy.

4.8 Modification

Modifying a certificate means creating a new certificate that has the same or a different subject Public Key and a different serial number, and the new certificate differs in one or more other fields related to the subject (e.g., Subject e-mail address in the subject alternative name field), from the old certificate.

4.8.1 Circumstance for Certificate Modification

A certificate may be modified only if:

- the certificate is valid at the time a re-key operation is requested
- the certificate DN is pseudonymous or anonymous
- the public key changes
- the new DN meets the criteria of Section 3.1
- no other changes are included request

4.8.2 Who May Request Certificate Modification

The Subscriber, either directly or via an authorized entity (see Section 3.2.5), may request a certificate modification.

4.8.3 Processing Certificate Modification Requests

Subject to the same provisions as Section 4.3 of this Policy.

4.8.4 Notification of New Certificate Issuance to Subscriber

Subject to the same provisions as Section 4.4 of this Policy.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Subject to the same provisions as Section 4.4 of this Policy.

4.8.6 Publication of the Modified Certificate by the CA

Subject to the same provisions as Section 4.4 of this Policy.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Subject to the same provisions as Section 4.4 of this Policy.

4.9 Certificate Revocation & Suspension

4.9.1 Circumstances for Revocation

The RA shall request from the CA that certificate be revoked when the binding between the Subject and the Subject's Public Key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding include, but are not limited to:

- A determination by the CA that Revocation is appropriate and/or needed;
- Identifying information or affiliation components of any names in the Certificate becomes invalid;
- Any information in the Certificate becomes invalid, subject to the terms of the CPS the Certificate is issued under;
- The Subscriber or Sub-CA can be shown to have violated the stipulations of its Subscriber agreement, if applicable, or one or more sections of this CP;
- The original Certificate request was not authorized;
- The Subscriber, Sub-CA or other authorized party asks for its Certificate to be Revoked;
- The Subscriber or Sub-CA is no longer eligible to obtain a Certificate from a CA operating under this CP;
- The Certificate has been delivered based upon wrong or falsified information;
- There is reason to believe the confidentiality of the private key associated with the certificate is no longer ensured or private key associated with the certificate has been compromised; or
- The media holding the private key associated with the certificate is suspected or known to have been compromised.
- Whenever any of the above circumstances occur, the associated certificate may be revoked and placed on a CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire. Revoked certificates shall appear on at least one CRL.

4.9.2 Who Can Request Revocation

Within the PKI, the Revocation of a certificate may be requested by any one of the PKI Participants.

4.9.2.1 Special circumstances

Beyond the individuals or roles that can request revocation of a certificate, a subject matter expert (SME) that is involved in an open incident may request the revocation or suspension (see Section 4.9.13) of one or more certificates, if their assessment is that revocation of the certificate(s) is necessary as part of incident response, and in the interest of preserving the integrity or the interests of Tesla, Tesla's customers, or third parties.

4.9.3 Procedure for Revocation Request

Requests for revocation may be made using an online process, in person, or in writing. Regardless of the method used, authentication of the request must occur to prevent malicious revocations of certificates by unauthorized entities.

Upon receipt of a revocation request, the RA or OA shall authenticate the request. The RA or OA may, at its discretion, take reasonable steps to verify the need for revocation. Upon verification of the validity of the revocation request, the RA or OA shall instruct the CA to revoke the certificate.

The RA or OA shall specify an appropriate revocation reason when the inclusion of the revocation reason does not violate confidentially requirements as stipulated in Section 9.3.

In the event a private key is compromised, time is of the essence to revoke a certificate. In that event, the CA may perform a Revocation without consulting the RA or OA.

Information relating to certificate revocation that may be disclosed through a CRL or otherwise, includes the status of a certificate as revoked along with any one of the following optional descriptions:

- Key compromise
- CA compromise
- Affiliation changed
- Superseded
- Cessation of operation
- Certificate hold
- Remove from CRL
- Privilege withdrawn
- Unspecified

Any other details are considered confidential (see Section 9.3 of this document).

4.9.4 Revocation Request Grace Period

There is no revocation grace period. Authorized parties as listed in Section 4.9.2 are required to request the revocation of a certificate immediately after the need for revocation comes to their attention.

4.9.5 Time Within Which CA Must Process the Revocation Request

Certificates shall be revoked as soon as is practical upon receipt, authentication, and verification of certificate revocation request.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties shall check the appropriate CRL or OCSP responder data to verify the validity of a certificate

each time a certificate is presented, or an agreed upon equivalent method.

CAs, RAs and OAs shall provide Relying Parties with the URI of the CRL and/or OCSP locations.

Relying Parties shall follow the stipulations of ISO 15118-2 for revocation checking requirements.

4.9.7 CRL Issuance Frequency

To ensure timely delivery of revocation information, CRLs are periodically published to repositories.

CRLs are published to their respective repositories according to the following schedule:

- The Root CA will publish base CRL information every year at a maximum with a four week overlap period.
- Issuing CAs will publish base CRLs every seven days at a maximum with a three-day overlap.
- CRLs may be issued more frequently than required. If there are circumstances under which a CA will post early updates, these shall be spelled out in its CPS.

4.9.8 Maximum Latency of CRLs

CRLs shall be published within four hours of generation.

4.9.9 On-line Revocation/Status Checking Availability

The most recent CRL will be available online and accessible by using industry standard protocols.

The online revocation information access locations will be available with a 99.95% availability excluding scheduled downtimes which shall not exceed 4 hours in any calendar week and 16 hours in a calendar year.

4.9.10 On-line Revocation Checking Requirements

Relying Parties should support online status checking. Client software using online status checking is not required to obtain or process CRLs.

A Relying Party must check the status of a certificate on which they wish to rely by using the path validation algorithm in Section 6 of [RFC 5280].

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

4.9.11 Other Forms of Revocation Advertisements Available

No other forms of revocation advertisement are specified by this CP.

4.9.12 Special Requirements Related to Key Compromise

In the event of a CA private key compromise or loss, a CRL from the parent CA (the CA that issued the certificate associated with the compromised CA private key) shall be published at the earliest feasible time.

4.9.13 Circumstances for Suspension

- Suspension is not supported by this Certificate Policy.

4.9.14 Who can Request Suspension

Suspension is not supported by this Certificate Policy.

4.9.15 Procedure for Suspension Request

Suspension is not supported by this Certificate Policy.

4.9.15.1 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

No stipulation beyond Section 4.9.9.

4.10.1 Operational Characteristics

If enabled, OCSP responder data is available using standards-based protocols. These protocols include:

- HTTP to retrieve OCSP data
- HTTP to retrieve CA certificates for chain building

4.10.2 Service Availability

If enabled, the OCSP responder service availability follows the stipulations of Section 4.9.9.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Certificates that have expired prior to or upon end of subscription are not required to be revoked.

See Section 4.9 for a description of certificate revocation before a certificate reaches the end of its expiry date.

4.12 Key Escrow & Recovery

Key escrow refers to the holding of a key material by a third party.

4.12.1 Key Escrow and Recovery Policy and Practices

Escrow is not permitted under this Policy.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

---

5 Facility Management & Operations Controls

This Section provides information on the physical, procedural, and personnel controls that Certification Authorities, Registration Authorities, Operations Authorities and Subscribers are subject to for the protection of their operations and data.

5.1 Physical Controls

All CAs shall be housed in data centers that provide physical, technological, and procedural controls commensurate with the business and security requirements of the CAs.

5.1.1 Site Location & Construction

The CA shall conduct all CA operations within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

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

5.1.2 Physical Access

All CA equipment shall be housed in intruder-resistant facilities that require keycard entry. PKI equipment shall be housed within a dedicated perimeter subject to specific physical access control such as restricted keycard entry requirements and/or physical locks.

See Section 6.2 for details on cryptographic module protection.

5.1.3 Power and Air Conditioning

All critical CA equipment shall be connected to power sources that provide uninterrupted backup power to facilitate the orderly shutdown of equipment in the event of a power failure.

All critical CA equipment shall be located in controlled environments that provide appropriate humidity, filtering of air borne particulate matter, and temperatures, according to manufacturer specifications for CA-related hardware and media.

5.1.4 Water Exposures

All critical CA equipment must be protected against water exposure.

Water exposure from fire prevention and protection measures (e.g. sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention & Protection

All critical CA equipment is stored in facilities that provide fire prevention and protection mechanisms.

5.1.6 Media Storage

All CA media shall be protected from accidental damage. All CA media shall be protected from unauthorized access with controls commensurate to their level of sensitivity.

5.1.7 Waste Disposal

All CA-related sensitive materials shall be disposed using methods in accordance with Tesla data management policies.

5.1.8 Off-Site backup

System backups shall be made on a periodic basis to facilitate the recovery of systems in the event of catastrophic failure or replacement.

At least one copy of the backup shall be stored in a separate physical location that has physical and other security controls commensurate with security requirements of the system being backed up.

Backup of CA private key material is described in Section 6.2.4 of this Policy.

5.2 Procedural Controls

5.2.1 Trusted Roles

Tesla shall assign employees to trusted roles to administer the PKI, provided that individuals filling these roles meet the criteria for verification of identity as set forth in this Policy and associated CPS.

Trusted Persons are personnel identified to fill Trusted Roles and are designated to manage the PKI's trustworthiness.

Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- The validation, authentication, and handling of information in certificate applications;
- The acceptance, rejection, or other processing of certificate applications, revocation requests, renewal requests, or enrollment information;
- The issuance, or revocation of certificates, including (in the case of workstations) personnel having access to restricted portions of its repository;
- Access to safe combinations and/or keys to security containers that contain materials supporting production services;
- Access to Hardware Security Modules (HSMs), their associated keying material, and the secret share splits of the Personal Identification Numbers (PINs) and smart cards that protect access to the HSMs;
- Installation, configuration, and maintenance of the CA;
- Access to restricted portions of the Certificate Repository;
- The handling of Subscriber or Sub-CA information or requests; and • The ability to grant physical and/or logical Access to the CA equipment.

5.2.2 Number of Persons Required per Task

Two or more trusted persons are required for the following:

- CA certificate issuance
- CA private key activation
- CA private key backup/restore

Access and administration controls for CA private key are described in more detail Section 6.2.2 of this Policy.

As an exception, for online CAs only, automated key activation at server start is allowed by this policy.

As an exception, for online CAs only, automated backup of CA private keys is allowed by this policy, only

if encrypted with partitioned credentials requiring two or more persons to use the backups for any further operation (restore for instance).

5.2.3 Identification and Authentication for Each Role

All CA Personnel shall have their identity and authorization verified in person by the Operational Authority before they are:

- Included in the access list for the CA site;
- Included in the access list for physical access to the CA system; • Given a certificate for the performance of their CA role; or
- Given an account on the CA system.
- Each of these certificates and accounts (except for the CA signing certificates) shall:
- Be directly attributable to an individual;
- Not be shared; and
- Be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls.

Each administrator is identified by the following criteria each time any work needs to be performed on the CAs console:

- Electronic badge for physical access.
- Electronic credentials backed by two-factor authentication for logical access.

5.2.4 Separation of Duties

• The PKI implements multi-person control for a variety of operations as described in Section

5.2.2 and Section 6.2.2 of this document.

• Role separation, when required, may be enforced by either the CA or RA equipment, or procedurally, or by both means.

5.3 Personnel Controls

All personnel performing duties with respect to the operation of a CA shall:

- Be bound by contract not to disclose sensitive CA security-relevant information or Subscriber information; and
- Not be assigned duties that may cause conflict with their CA duties.

5.3.1 Qualifications, Experience, & Security Clearance Requirements

The qualifications of each candidate, for PKI Operations staff and PKI Administrators, shall be evaluated by the Operations Authority, who shall have final say on all PKI staffing.

The role of the CA Administrator requires a trained person who is familiar with the PKI and technically competent.

5.3.2 Background check requirements

Background checks are carried out by Tesla when a person is hired or contracted, including for roles related to the PKI.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA or RA shall receive training. Training shall be conducted in the following areas:

- CA (or RA) security principles and mechanisms
- All PKI software versions in use on the CA (or RA) system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Stipulations of this policy

5.3.4 Retraining Frequency & Requirements

All individuals responsible for PKI roles shall be made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency & Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Personnel who perform unauthorized actions may be subject to disciplinary action as per Tesla Human Resources Policy.

5.3.7 Independent Contractor Requirements

Contractors fulfilling trusted roles are subject to all personnel requirements stipulated in this policy.

5.3.8 Documentation Supplied to Personnel

All PKI participants shall have access to an electronic version of this Policy.

Additional documentation shall be provided to PKI participants commensurate with their roles and respective obligations and duties.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CA and RA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, a paper form, or other physical mechanism shall be used. All security audit logs, both electronic and nonelectronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in section 5.4.2 shall be maintained in accordance with Section 5.5.2.

5.4.1 Access and change log

All operations on the PKI shall be documented in a version-controlled document management system that

must contain:

- Date of the access or change.
- Name of operator(s).
- List of all operations.

5.4.2 Types of Events Recorded

The CA shall record in audit logs all relevant events relating to the security of the CA system. All relevant logs whether electronic or manual should contain the date and time of the event, and the identity of the individual or service that caused the event.

5.4.3 Frequency of Processing Log

The Information Security team shall review audit logs at least once a year for offline CAs and once every three months for issuing CAs.

Such reviews involve reviewing dashboards summarizing log entries. Dashboards must include statistics on regular certificate issuance and details of all warning of errors that occurred during the review period.

All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

5.4.4 Retention Period for Audit Logs

Audit logs shall be retained online for at least three months.

Audit logs shall be archived as described in Section 5.5.

5.4.5 Protection of Audit Logs

Access to all security audit logs shall conform to the principle of least privilege. Only authorized individuals or systems shall have access to security audit logs. If authorized entities have deletion privileges, procedures must be in place to protect archived data from deletion or destruction prior to the expiry of the retention period for audit logs specified in Section 5.4.3.

No individual shall have modification privileges on audit logs. Erroneous log entries must be corrected using a supplementary log entry.

5.4.6 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly for issuing CAs and every time operations take place on an offline CA.

5.4.7 Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the CA system. Automated audit processes shall be initialized at system or application startup and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files).

Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations shall be suspended until the problem has been remedied.

5.4.8 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited.

5.4.9 Vulnerability Assessments

The PKI shall be included in vulnerability assessments that are performed regularly on the Tesla infrastructure.

5.5 Records Archive

5.5.1 Types of Events Archived

Certificate manager archive records shall be sufficient detail to establish the validity of a signature and the proper operation of the PKI. This shall include, at a minimum:

- Certificates, public verification keys, CRLs, and any other information generated by the offline and issuing CAs.
- Vendor contracts that relate to the operation of the CAs.
- Any other contracts or agreements associated with the Tesla CAs.
- Audit results.

5.5.2 Retention Period for Archive

Contracts archived pursuant to this Section shall be retained for the duration of the contracts plus ten (10) years.

Audit results archived pursuant to this Section shall be retained for ten (10) years.

Digital Signature certificates, public verification keys, CRLs, and any other information generated by the offline and issuing CA shall be kept without any loss of data for a period of

- At least ten years for offline CAs.
- At least five years for online CAs.

Applications necessary to read these archives must be maintained for at least the applicable retention period above.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

Applications needed to process the archive data shall also be maintained for the archival retention period.

This CP/CPS does not restrict longer retention of archived data.

5.5.3 Protection of Archive

No unauthorized CA equipment operator shall be able to modify or delete the archive, but archived records may be moved to another medium. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. No transfer of medium shall invalidate certificate manager applied signatures. The certificate manager shall maintain a list of people authorized to modify or delete the archive and make this list available during CP compliance audits. Release of sensitive archive data shall be consistent with the stipulations in Section 9.4 of this Policy.

5.5.4 Archive Backup Procedures

All archived PKI records shall include in the automated backups of the systems used to store those records.

5.5.5 Requirements for Timestamping of Records

Storage of records shall be done in systems that support version control and preserve the date of storage of the records.

5.5.6 Archive Collection System (internal or external)

No stipulation.

5.5.7 Procedures to Obtain & Verify Archive Information

All requests will be handled consistent with Section 9.4 of this document.

5.6 Key Changeover

When the certificate of a CA is about to expire, a new CA certificate must be generated and is handled as a new certificate application as described in Section 4.1.

The CA should ensure that no certificate can be issued for a Subscriber with an expiration time past the expiration time of its issuing CA.

5.7 Compromise & Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The OA shall be notified if any CAs operating under this policy experience:

- Suspected or detected compromise of the CA systems.
- Physical or electronic penetration of CA systems.
- Successful denial of service attacks on CA components.
- Any incident preventing the root CA from issuing a CRL within one week of the expiration of the previous base CRL.
- Any incident preventing an issuing CA from issuing a base CRL within two hours of the expiration of the previous CRL.

The OA shall re-establish operational capabilities as quickly as possible in accordance with procedures set forth in the PKI Disaster Recovery Guide.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this policy shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- If the CA signature keys are not destroyed, CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7 and then implementing PKI disaster recovery procedures.
- If the CA signature keys are destroyed, CA operation shall be re-established as quickly as possible, giving

priority to the generation of a new CA key pair.

The OA shall be notified as soon as possible.

5.7.3 CA Private Key Compromise Procedures

If a CA private key is compromised or there are sufficient grounds to believe that the key may have been compromised, the parent CA in the chain, if one exists, shall revoke the potentially compromised CA certificate.

The revocation data shall be published immediately. The CA's key shall be re-established according to the stipulations in Section 5.7.4.

If the CA is a Root CA, the trusted self-signed certificate must be removed from each Relying Party application, and a new one distributed via secure out-of-band mechanisms.

The Tesla OA shall investigate and report to the PAA what caused the compromise or loss, and what measures have been taken to reduce the probability of recurrence.

5.7.4 Business Continuity Capabilities After a Disaster

If the CA equipment is inoperative because of damage, the issuing CAs shall re-establish CA operations as quickly as practical. Priority shall be given to restoring the ability to revoke certificates. If revocation abilities cannot be established within two hours, a report to the OA must be made. Upon receipt of report, the OA will determine whether to declare that the CA's private key has been compromised.

If the CA private key cannot be recovered, the CA shall request revocation of its certificates.

Subsequently, the CA must be completely rebuilt by re-establishing CA hardware, generating new key pairs, being re-certified, and re-issuing all certificates, including cross-certificates and Subscriber certificates.

5.8 CA & RA TERMINATION

Tesla may terminate CA operations at any time following one month notice to the Application Owners of record and Tesla Sponsors (where applicable). Upon CA termination:

- All CA certificates shall be revoked.
- The CPS, CP(s), and CRL(s) shall be available at the specified URIs for six months following the termination of CA operation.
- All archived records shall remain with current custodian for the periods described in Section 5.5.2.
- The CA private key shall be destroyed.

---

6 Technical Security Controls

6.1 Key Pair Generation & Intallation

6.1.1 Key Pair Generation

Generation of CA key pairs shall take place while all parties responsible for verification are present as required in Section 5.2.2.

Generation of CA key pairs shall be done inside a Hardware Security Module (HSM).

All Hardware Security Modules used for CA keys shall be certified to support an operational mode compliant to a Federal Information Processing Standards (FIPS) 140-2 Level 3 or above, or a Common Criteria Evaluation Assurance Level (EAL) 4+.

6.1.2 Private Key Delivery to Subscriber

If a CA or RA generates a private key for a Subscriber, the private key must be delivered to the entity positively identified as the Subject Name in the Certificate. The delivery must occur using a secure method agreed upon by both the Subscriber and the CA, and the Subscriber shall acknowledge receipt of private key.

CAs shall generate their own key pairs in hardware.

6.1.3 Public Key Delivery to Certificate Issuer

Subordinate CA key pairs are subject to the same HSM requirements described in Section 6.1.1, but their public key is then signed by a superior CA.

The signing and transportation of the certificate signing request (CSR) of a CA subordinate to the root CA is done via manual transport since the root CA is always disconnected from any network.

All certificate requests for CAs and Subscribers shall be formatted as PKCS#10.

6.1.4 CA Public Key Delivery to Relying Parties

Public keys for CAs and Subscribers shall be stored in the repositories specified in Sections 2.1 and 2.2 of this Policy.

6.1.5 Key Sizes

This Policy requires the use of keys that comply with ISO 15118-2. NIST-P256 (also called secp256r1) is the only type allowed for ISO 15118-2.

6.1.6 Public Key Parameters Generation and Quality Checking

For both Subscribers and issuing CAs, the key parameters must be verified by the issuing CA to comply with the requirements of Section 6.1.5.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

Certificates issued by Tesla V2G PKI shall be used in accordance with the requirements of ISO 15118-2 and follow the key usage requirements described in the profiles in ISO 15118-2 Annex H.

6.1.8 Signature Algorithm

The certificates issued by Tesla V2G PKI shall use ECDSA-SHA256 signatures as per ISO 15118-2 requirements.

6.2 Private Key Protection & Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards & Controls

Section 6.1.1 describes the requirements for cryptographic modules.

Section 5.1 describes the physical controls that shall be used for protecting cryptographic modules.

Additionally, the Root CA hardware security module and all computers communicating with it must be entirely air gapped. This means that a local network between a dedicated administration computer and the PKI application is allowed, but that network must never be connected to any other network for the entire life of the PKI.

6.2.2 Private Key Multi-Person Control

No single trusted person shall have access to the CA private key material of the offline Root CA.

All CA private key material shall be protected by Hardware Security Modules (HSM).

All access to the private key material of offline CAs shall require a smartcard.

Smartcards activation shall be protected by a PIN code of at least six digits entered directly on a smartcard reader keypad.

No single trusted role shall have access to both smartcards and PIN codes, and no single individual shall be authorized to fulfill a role with smartcard access and a role with PIN code access.

Operations that require access to private key material include:

- Starting certificate services on the CA
- Activation of the CA private key
- Renew certificates
- Signing CRLs
- Signing subordinate CA certificates
- Backing up private key material
- Revoking subordinate CA certificates

At least two smartcards shall be required to authorize the following actions:

- Loading the Master Backup Key to an existing HSM
- Loading the Master Backup Key to a new HSM

The private key material of online issuing CAs shall be protected by a hardware security module.

Because the private key material must be continuously available for online CA operations, online issuing CAs do not require multi-person controls of the private key material for the purpose of CA activation at CA startup.

When not in use, all smartcards and PIN codes used for HSMs must be stored in locked safes.

Given the requirement for role separation regarding smartcards and PIN codes, two separate safes shall be used to store smartcards and PIN codes, with no individual having access to both safes.

6.2.3 Private Key Escrow

Private key shall not be escrowed.

6.2.4 Private Key Backup

CA private keys are protected by the HSM. The CA private keys are backed up by using methods specific to the HSM that ensure private keys backups are encrypted using a Master Backup Key.

The Master Backup Key shall be stored on smartcards protected by PIN codes. At least two smartcards must be required to loading the Master Backup Key into an HSM. As described above, PIN codes and smartcard access shall require role separation.

Online CA databases encrypted key backups and audit logs shall be backed up daily. Offline CA databases shall be backed up each time that the CA is accessed for CRL publication or other CA operations.

6.2.5 Private Key Archival

Private keys shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys must not be transferred, outside of backup operations described in Section 6.2.4 and disaster recovery operations as described in Section 5.7.

6.2.7 Private Key Storage on Cryptographic Module

See Section 6.2.1.

6.2.8 Method of Activating Private Keys

OA Operators with access to the CA must authenticate with TLS certificates protected by two-factor authentication (e.g., smart card plus PIN).

Successful authentication is required by all entities logging on to PKI components.

Activation of the private key material on HSMs operating online CAs can be automated provided that physical and logical access control to those devices follow the requirements of Section 5.

Activation of the private key material on offline CAs requires that a quorum of trusted individuals is present to provide credentials. See Section 6.2.2.

6.2.9 Methods of Deactivating Private Keys

Private keys remain active for the period of login. The login period is ended either by the subject logging out from the PKI application or automatically as determined by a preset timer.

Manually activated Cryptomodules must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, e.g. via a manual logout procedure, or by a passive timeout.

HSMs for offline CAs must be deactivated and reset after use.

6.2.10 Method of Destroying Private Keys

CA private keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. HSM-specific methods shall be used to destroy private keys. Physical

destruction of hardware is not required.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

Public keys are archived in the CA database.

CA Public Key data is backed up at the same time as CA private key data, as stipulated in Section 6.2.4.

6.3.2 Certificate Operational Periods/Key Usage Periods

Maximum certificate validity periods for the PKI are defined as follows: CAs shall not issue certificates with

Certificate	Maximum Validity Period (years)
Root CA	50
Sub-CA	40
End Entity	20

validity periods that extend beyond the expiration date of their own certificate.

6.4 Activation Data

6.4.1 Activation Data Generation & Installation

Activation of CA keys shall be subject to multi-person control as described in Section 6.2.2.

6.4.2 Activation Data Protection

If activation data is used it shall be protected from unauthorized use by a combination of cryptographic and physical access controls mechanisms and from accidental disclosure when activation data is entered.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

All "high security" configuration recommendations from operating system vendors, application vendors, PKI Operations team shall be followed, where practical, in the design of the CA unless the recommendations conflict with the CP/CPS.

All applicable vendor security patches shall be applied after testing and verification that they do not disrupt operations of the CA.

The Root CA shall only apply patches if they fix broken functionality or add new functionality required by the PKI.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

No production data shall be used in development systems. Robust change control processes shall be in place to control modifications of production systems.

The following specific requirements shall be met as part of the system development process:

CAs shall use software, whether off-the-shelf or custom-built, that has been designed and developed under a formal, documented development methodology.

- Hardware and software procured shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Hardware and software that is developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented.
- The PKI platform (server hardware, operating system software, and PKI application software) shall be exclusively used for PKI functions.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment and be installed by trusted personnel.

6.6.2 Security Management Controls

Configuration management of the CAs shall require validation of all software and configuration changes.

6.6.3 Life Cycle Security Ratings

The OA shall ensure that it receives notifications of software and firmware updates, as well as notifications of bugs and vulnerabilities from all vendors used for the PKI and shall monitor public sources for CVEs affecting any part of the PKI.

The OA shall determine the timeline to update software and/or hardware based on the above input and the severity of any reported vulnerability.

6.7 Network Security Controls

See Section 6.2.1 for network requirements for offline CAs.

Online CAs can be connected to a network. The network segments that host online CAs must implement security controls. At a minimum, these controls include:

- Only required services and applications shall be installed on the CA computer.
- PKI server network firewall rules shall be used to limit network access to required hosts and ports.
- Access to the web management interface of the PKI servers must be only possible from a "jump box" only accessible by PKI administrators.
- SSH to PKI servers must be disabled by default and only enabled on a temporary basis by PKI administrators if required for maintenance.
- When enabled, SSH must only be allowed a "jump box" only accessible by PKI administrators.

6.8 Time Stamping

A trusted time source should be used to support the accurate time stamping of data and transactions.

---

7 Certificate, CRL, and OCSP Profiles Format

7.1 Certificate Profile

CAs shall issue X.509 version 3 certificates that conform to the PKIX Certificate and CRL Profile, as stipulated in IETF PKIX, RFC 5280. All end-entity PKI software shall support all base (non-extension) fields of X.509 certificates, as shown in the table below: Additionally, all end-entity PKI software shall support all

Field Name	Description
Issuer	Name of CA that issued certificate
Validity	Activation and expiry date of certificate
Subject	Subscriber's Distinguished Name
Subject Public Key Information	Public key of entity named in certificate, along with algorithm ID key to identify the algorithm used to generate public / private key pair.
Version	Version of X.509 certificate
Serial Number	Unique serial number assigned to certificate
CA Signature Algorithm	Algorithm used by the CA to sign certificate
Signature Value	Value of the CA signature

Additionally, all end-entity PKI software shall support all X.509 certificate version 3 extensions defined in this Policy.

7.1.1 Version Numbers and certificate profiles

CA shall issue X.509 version 3 certificates. Version numbers are governed by RFC 5280, Section 4.1.2.1.

7.1.1.1 Tesla V2G PKI Root certificate profile

Field	Value	Comment
Key type	secp256r1	
Subject (example)	O=Tesla, CN=V2G Root G1, DC=V2G	Country and OU are allowed by the standard, we are not using those to keep the certificate as short as possible. Each subsequent revision for the root will update "Gn" where n starts at 2: for instance, "G2", "G5" ... "G32"
Validity	40 Years	
AuthorityKeyIdentifier	Included	
SubjectKeyIdentifier	Included	
Key usage	Critical keyCertSign, cRLSign	
BasicConstraints	Critical	
CA	True	
CertificatePolicies	Not used	Optional, not critical
CRLDistributionPoints	Not used	Optional, not critical
AIA (OCSP)	Not used	Optional, not critical
Signature	ecdsa-with-SHA256	

7.1.1.2 CPO SubCA-1 Certificate profile

Field	Value	Comment
Key type	secp256r1	

Subject (example)	DC=CPO, O=Tesla, CN=CPO Sub1 G1.1	At renewal, the "Gm.n" suffix will be updated, with "m" corresponding to the Root CA generation and "n" corresponding to the SubCA generation: "V2G Root G2" → "CPO Sub1 G2.1"
Validity	4 years	4 years is as per ISO 15118-2 requirements.
AuthorityKeyIdentifier	Included	
SubjectKeyIdentifier	Included	
Key usage	Critical keyCertSign, cRLSign	
BasicConstraints	Critical	
CA	True	
PathLength	1	
CertificatePolicies	Not used	
AIA	Not used	
Signature	ecdsa-with-SHA256	

7.1.1.3 CPO SubCA-2 Certificate profile

Field	Value	Comment
Key type	secp256r1	
Subject (example)	O=Tesla, CN=NA CPO Sub2 G1.1.1	At renewal, "Gm.n.o" suffix will be updated, with "m" corresponding to the Root CA generation, "n" the SubCA 1 generation, and "o" the SubCA2 generation "V2G Root G2" → "CPO Sub1 G2.1" → "NA CPO Sub2 G2.1.2"
Validity	2 Years	As per ISO 15118-2 requirements
AuthorityKeyIdentifier	Included	
SubjectKeyIdentifier	Included	

Key usage	Critical, keyCertSign, cRLSign	
BasicConstraints	Critical	
CA	True	
PathLength	0	
CertificatePolicies	Not used	
AIA	Not used	
Signature	ecdsa-with-SHA256	

7.1.1.4 CPO SECC End Entity certificate profile

Field	Value	Comment
Key type	secp256r1	
Subject (example)	O=Tesla, OU=Superchargers, CN=<CPID>, DC=CPO	CPID is the charging point ID "CPO" is required OU is optional
Validity	Up to 1 year	
Key Usage	critical digitalSignature	

7.1.1.5 Tesla MO SubCA-1 profile

Field	Value	Comment
Key type	secp256r1	
Subject (example)	DC=MO, O=Tesla, CN=MO Sub1 G1.1	At renewal, the "Gm.n" suffix will be updated, with "m" corresponding to the Root CA generation and "n" corresponding to the SubCA generation: "V2G Root G2" → "MO Sub1 G2.1"
Validity	10 Years	

AuthorityKeyIdentifier	Included	
SubjectKeyIdentifier	Included	
Key usage	Critical, keyCertSign, cRLSign	
BasicConstraints	Critical	
CA	True	
PathLength	1	
CRLDistributionPoints	Not used	
AIA	Not used	
Signature	ecdsa-with-SHA256	

7.1.1.6 Tesla MO SubCA-2 profile

Field	Value	Comment
Key type	secp256r1	
Subject (example)	O=Tesla, CN=NA MO Sub2 G1.1.1 (for North America) Optional: DC=MO	At renewal, "Gm.n.o" suffix will be updated, with "m" corresponding to the Root CA generation, "n" the SubCA 1 generation, and "o" the SubCA2 generation "V2G Root G2" → "MO Sub1 G2.1" → "NA MO Sub2 G2.1.2"
Validity	5 Years	
AuthorityKeyIdentifier	Included	
SubjectKeyIdentifier	Included	
Key usage	Critical keyCertSign, cRLSign, digitalSignature, nonRepudiation	
BasicConstraints	Critical	
CA	True	

PathLength	0	
CRLDistributionPoints	Not used	
AIA	Not used	
Signature	ecdsa-with-SHA256	

7.1.1.7 Tesla MO Contract Certificate profile

Field	Value	Comment
Key type	Secp256r1	
Subject (example)	O=Tesla, OU=<optional>, CN=EMAID	EMAID follows 15118-2 recommendations. OU: this is optional, can be used to provide human-readable information related to the MO, such as “Supercharging”, or “North America Supercharging”.
Validity	Up to 2 years	This can be adjusted from 1 day to 2 years depending on contract.
Authority Key Identifier	Included	
Subject Key Identifier	Included	
Basic Constraints	Critical	
CA	**False**	
Key Usage	Critical digitalSignature, nonrepudiation, keyEncipherment, keyAgreement	

7.1.2 Certificate Extensions

Only the X.509 version 3 certificate extensions described in the profiles above may be included in the issued certificates.

7.1.3 Algorithm Object Identifiers

Refer to the certificate profiles in Section 7.1.1 for algorithm object identifiers.

7.1.4 Name Forms

Section 3.1 of this Policy provides information on the stipulations for DNs in the Subject and Issuer fields of

a Certificate.

7.1.5 Name Constraints

Not supported.

7.1.6 Certificate Policy Object Identifier

A certificate policy object identifier may be included in some certificate profiles as described above.

The Certificate Policy OIDs are described in Section 1.2 of this Policy.

7.1.7 Usage of Policy Constraints Extension

Not supported.

7.1.8 Policy Qualifiers Syntax & Semantics

Not supported.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Not supported.

7.2 CRL Profile

7.2.1 Version Numbers

This CA shall issue X.509 version 2 CRLs in compliance with PKIX certificate and CRL profile, as stipulated in IETF PKIX, RFC 5280.

7.2.2 CRL Entry Extensions

All entity PKI software shall correctly process all CRL extensions required in the PKIX Certificate and CRL Profile.

7.3 OCSP Profile

7.3.1 Version Number(s)

If used, the PKI shall use OCSP version 1 or later.

7.3.2 OCSP Extensions

Appropriate extensions from the RFC 6960, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP" and RFC 5019, "The Lightweight Online Certificate Status Protocol (OCSP) Profile" may be used in OCSP requests and responses. Due to support for RFC 5019, signed requests are not supported by the Online responder.

Nonces may be included in OCSP requests but are not required.

8 Compliance Audit & Other Assessments

8.1 Frequency of Audit or Assessments

The maximum interval between compliance audits is one year.

8.2 Identity & Qualifications of Assessor

All compliance audits should be performed by an Auditor with experience in PKI process and infrastructure auditing.

8.3 Assessor's Relationship to Assessed Entity

The assessor must be independent from the PKI. They must not be a PKI participant or report to the same director as any of the PKI participants.

8.4 Topics Covered By Assessment

Auditors shall certify whether this Certification Practice Statement and Certificate Policies are appropriate to meet their stated purpose and whether PKI operations meet the terms and conditions specified in said documents.

Auditors shall provide detailed documentation on all deficiencies and include information on available options to achieve compliance.

8.5 Actions Taken as a Result of Deficiency

Tesla shall modify PKI supporting documentation or operational practices as appropriate to resolve any identified deficiencies.

8.6 Communication of Results

Results of audits and remedial actions will be provided to the PAA, and any other parties with an explicit contractual right to see such results.

Certification of compliance, including the effective dates of any such certification, may be published to the general public.

---

9 Other Business & Legal Matters

9.1 Fees

9.1.1 Certificate Issuance/Renewal Fees

May be governed by a separate commercial agreement.

9.1.2 Certificate Access Fees

May be governed by a separate commercial agreement.

9.1.3 Revocation or Status Information Access Fee

May be governed by a separate commercial agreement.

9.1.4 Fees for other Services

May be governed by a separate commercial agreement.

9.1.5 Refund Policy

May be governed by a separate commercial agreement.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation

9.2.3 Insurance/warranty Coverage for End Entities

No stipulation.

9.3 Confidentiality of Business Information

The CA and RA SHALL protect the Confidentiality of sensitive information stored or processed on CA systems that could lead to abuse or fraud.

The CA and RA SHALL protect customer data that could allow an attacker to impersonate a customer.

9.3.1 Scope of Confidential Information

No stipulation

9.3.2 Information not within the scope of Confidential Information

No stipulation

9.3.3 Responsibility to Protect Confidential Information

No stipulation

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The V2G PKI is operated in compliance with the Tesla Customer Privacy Notice described at https://www.tesla.com/legal/privacy.

9.4.2 Information Treated as Private

The following types of information are considered private:

- CA, RA or Subscriber private keys.
- Audit logs.
- User PINs and passwords.

Additionally, the PKI must handle all personal data in compliance with local law and regulations and the Tesla privacy plan.

9.4.3 Information not Deemed Private

Information included in certificates and CRLs issued by the PKI are not subject to protection outlined in Section 9.4.2

9.4.4 Responsibility to Protect Private Information

Private and sensitive information is stored securely and released only in accordance with the provisions in 9.4.6 and 9.4.7.

9.4.5 Notice and Consent to use Private Information

Notice and Consent to use private information is governed by the terms described at https://www.tesla.com/privacy.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Any disclosure shall be handled in accordance with Tesla Operating Policies, and all applicable internal and local rules and regulations.

9.4.7 Other Information Disclosure Circumstances

Any disclosure shall be handled in accordance with Tesla Operating Policies, and all applicable local rules and regulations.

9.5 Intellectual Property Rights

Tesla retains all intellectual property rights to all certificates issued by Tesla and all CRLs created by Tesla Issuing CAs. Tesla grants permission to reproduce and distribute certificates on a royalty-free basis on the condition that they are reproduced in their entirety and that their use is subject to the Relying Party Obligations described throughout the CP referenced in the certificate.

As between Tesla, Relying Parties, Application Owners, and the CA, all patentable inventions including any process and method used in the performance or enablement of the CA function are the property of Tesla.

The intellectual property described here is protected by civil and criminal state and federal law in the United States, and by comparable laws in other countries.

9.6 Representations & Warranties

Tesla and its CAs are not agents, fiduciaries, trustees, or representatives of Certificate Holders or Relying Parties. The relationship between Tesla V2G PKI CAs and Certificate Holders and Relying Parties is not that of agent and principal. Neither Certificate Holders nor Relying Parties have any authority to bind a Tesla V2G PKI CA, by contract or otherwise, to any obligation or to make representations on their behalf. Tesla V2G PKI CAs shall make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

9.6.1 CA Representations and Warranties

The Certification Authority (CA) represents and warrants that it will perform all duties described in this document and all supported Certificate Policies with reasonable care and due diligence.

9.6.2 RA Representations and Warranties

An RA who performs registration functions as described in this policy represents and warrants that it will comply with the stipulations of this policy and comply with a CP/CPS approved by an appropriate authority. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

9.6.3 Subscriber Representations and Warranties

No stipulation.

9.6.4 Relying Parties Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

Not applicable.

9.8 Limitations of Liability

Tesla accepts no liability to any party in relation to the operation of the Tesla V2G PKI unless expressly provided for in another contractual relationship.

9.9 Indemnities

Persons not expressly identified in Section 1.3.6 of this document as Authorized Relying Parties are prohibited from relying on Tesla V2G PKI CA Certificates. Any other person choosing to rely on any Tesla certificate is an Unauthorized Relying Party. By relying on any Tesla certificate, each Unauthorized Relying Party agrees to indemnify, defend, and hold harmless Tesla and each of Tesla's affiliates and their respective employees, officers, directors, and agents for any and all losses incurred as a result of such reliance. The forgoing obligation includes an obligation to promptly reimburse Tesla for all losses including costs, expenses, fees, including attorney fees and expert fees, incurred by Tesla relating to or arising from such reliance or from any investigation or from any actual or potential litigation related to such reliance. For purposes of this Section 9.9 Tesla's losses are deemed to include losses incurred by a third party as to which Tesla has any obligation

of indemnity or reimbursement.

9.10 Term & Termination

9.10.1 Term

This CP shall become effective when approved by the PAA. This CP/CPS has no specified term.

9.10.2 Termination

This policy remains in effect until it is superseded by a newer version. Termination of this Policy is at the discretion of the Tesla PA. The Tesla PA may terminate this Policy for any reason and without notice.

9.10.3 Effect of Termination and Survival

Upon termination of the CP, PKI participants are still bound by its term for the remainder of the validity periods of its certificates.

9.11 Individual Notices & Communications With Participants

Tesla PAA for this policy shall publish information (including this policy) on a public web page at https://developer.tesla.com/docs/charging/public-key-infrastructure . Tesla PAA will maintain a list of CAs asserting this policy. Proposed changes to the policy and policy updates shall be sent to those CAs. The certificate manager shall notify Tesla Subscribers of any changes to the CP/CPS.

9.12 Amendments

9.12.1 Procedure for Amendment

All Participants understand and agree that this CP/CPS may require periodic modifications, and that the Tesla PAA has the authority to modify this CP/CPS. Any suggested modifications should be communicated to the Contact Person listed in Section 1.5.2 of this CP/CPS.

9.12.2 Notification Mechanism and Period

See Sections 2.2 and 2.3.

9.12.3 Circumstances Under Which OID Must be changed

Object identifiers (OIDs) must be changed/added whenever this Policy introduces a new Assurance level.

9.13 Dispute Resolution Provisions

Not applicable.

9.14 Governing Law

This document shall be interpreted using the internal laws of the State of California of the United States of America without regard to its choice of laws rules or the physical location of the Certification Authority.

9.15 Compliance With Applicable Law

This PKI, and its supporting documentation, is designed to comply with applicable laws.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.2.1 Severability

If any provision of this CP is held invalid by an arbitrator or court having jurisdiction, such provision will be severed, and the remainder of the CP will remain in full force and effect. Nothing in this Section affects or limits the process for amending this CP in Section 9.12.

9.16.3 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.4 Force Majeure

No stipulation.

9.17 Other Provisions

9.17.1 Fiduciary Relationships

No stipulation.

9.17.2 Administrative Processes

No stipulation.

---

10 Bibliographies

CA / Browser Forum, Guidelines for the Issuance and Management of Extended Validation Certificates, version 1.0, June 7, 2007.

DoD Public Key Infrastructure Program Management Office, *United States Department of Defense X.509 Certificate Policy*, version 10, March 2, 2009.

Federal Bridge Certification Authority, *X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA)*, Version 2.12 February 11, 2009

Federal Information Processing Standards (FIPS) Publications,140-2 *Security Requirements for Cryptographic Modules*, 25 May 2001.

Federal Public Key Infrastructure Policy Authority, *X.509 Certificate Policy for the US Federal PKI Common*

Policy Framework, version 3647 - 1.7, April 15, 2009.

Internet Engineering Task Force (IETF), *Public Key Infrastructure X.509 (IETF PKIX), RFC 5280, Certificate and Certificate Revocation List (CRL) Profile*

Internet Engineering Task Force (IETF), *Public Key Infrastructure X.509 (IETF PKIX), RFC 3647, Certificate Policy and Certification Practice Statement frameworks*

Internet Engineering Task Force (IETF), RFC 5019, *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*

Internet Engineering Task Force (IETF), *RFC 1777, Lightweight Directory Access Protocol*

Internet Engineering Task Force (IETF), *RFC2253, Lightweight Directory Access Protocol (v3): UTF-8 Str*

Komar, Brian, *Windows Server® 2008 PKI and Certificate Security*, Microsoft Press, 2008.

RSA Laboratories, *PKCS #1 v2.1: RSA Cryptography Standard*, June 14, 2002.

11 Acronyms & Abbreviations

AD	Active Directory
AIA	Authority Information Access
CA	Certification Authority
CC	Common Criteria
CDP	Certificate Revocation List (CRL) Distribution Point
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DACL	Discretionary Access Control Lis
DC	Domain Component (in LDAP Distinguished Names)
DN	Distinguished Name
EAL	Evaluation Assurance Level
EU	European Union

EV	Extended Validation
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
GPO	Group Policy Object
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	SSL for HTTP
IANA	Internet Assigned Number Authority
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunications Union
KRA	Key Recovery Agent
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MBK	Master Backup Key
MD	Message Digest
NIST	National Institute of Standards and Technology
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PAA	Policy Approval Authority
PED	PIN Entry Device
PIN	Personal Identification Number

PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RPK	Remote PED Key
RPV	Remote PED Vector
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA	Secure Hash Algorithm
SID	Security ID
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
UPN	User Principal Name
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

12 Glossaries

Activation Data: Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g. PIN, passphrase, or manually held key share).

Active Directory: The Microsoft implementation of a directory service. A directory is a place to find information about users, computers, groups, services, and more. It is also used for authentication and authorization for Microsoft-based clients or products.

Algorithm: The mathematical function that is used to encrypt or decrypt data. Both parties wishing to exchange encrypted data must know and use the same algorithm in order to encrypt or decrypt data. See Key.

Applicant: An entity that submits a request for certificate, the entity identified as certificate Subscriber before a certificate is issued. See Subscriber.

Application Owner: An individual who is responsible for an application or service and can make requests to a CA or RA for certificate enrollment, revocation, or renewal on behalf of the application or service. See

Custodian.

Arc: A sub-tree (branch) of an object identifier (OID) tree. See OID.

Archive: Long-term, physically separate storage for data.

Assurance Level: An assertion of the level of trust a Certificate User (Relying Party) can reliably place in certificate. The level of assurance is a function of the rigor with which entities identified as Subjects in Certificates are authenticated prior to certificate issuance, the measures in place to protect the entity's private key, and the policies and controls in place with respect to the management of the CA.

Asymmetric Encryption: A one-way encryption process that uses one key of a public key pair to encrypt a message and the other key to decrypt it. Because asymmetric encryption is computationally expensive, it is often used to encrypt the shared secret key used for symmetric encryption to provide assurance of the confidentiality of the shared secret key. See Symmetric Encryption.

Binding: The linking or association of two or more pieces of information.

CA Certificate: A certificate for one CA's Public-key issued by another CA.

Certificate: A digital file that conforms to the ITU-T Recommendation X.509 and that 1) identifies the Subscriber of the certificate, 2) identifies the authority that issued the certificate, 3) contains the Subscriber's public key, 4) provides a validity period for the certificate, 5) is digitally signed by the CA that issues the certificate to provide assurance of the integrity of data contained within the certificate and the identity of the CA that issued the certificate.

Certification Authority (CA): An authority trusted by one or more entities and end entities to issue and manage X.509 certificates and CRLs.

Certificate Holder: The entity whose identity has been bound to a Tesla CA certificate and to whom the Tesla CA certificate was issued. Synonymous with the term "Subscriber".

Certificate Policy (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. In general, A CP describes what level of assurance may be placed in certificates that are issued under the Policy. More specifically, a CP is an administrative policy that addresses all aspects associated with the generation, production, distribution, accounting, compromise, recovery and administration of certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certificate User: A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. Synonymous with the term "Relying Party" Certification Path: An ordered sequence of certificates which, together with the Public-key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS): A detailed and technical statement of the practices and procedures which a Certification Authority (CA) employs in managing certificates, related processes, and related infrastructure. Although a CPS is similar in structure to a CP, it differs from a CP in that it provides a detailed and comprehensive set of technical requirements and procedures in support of the stipulations of the CP. Whereas a CP describes what assurance can be placed in Certificates issued under it, the CPS describes how that assurance is achieved with respect to the operation of the supporting infrastructure. Often, the CP

and CPS are combined into a single document.

Certificate Revocation List (CRL): A list issued and maintained by a Certification Authority (CA) that contains information on the certificates the CA has revoked before their expiry date.

Certificate Signing Request (CSR): Also known as a CSR or Certification Request, a message request sent to a Certification Authority (CA) by an applicant or other authorized entity on behalf of applicant for a certificate. The CSR includes information identifying the applicant as the Subject of the certificate, the public key of Public/Private key pair generated by the applicant, and other information. The private key is not included as part of the CSR, but is used to sign the message to the CA. The CA may require additional authentication before signing the CSR with its (the CA's) Private key. Once the CA signs the CSR, the CSR becomes a valid certificate.

Ciphertext: The seemingly random transformation of data by means of an encryption process to prevent disclosure to unauthorized entities.

Compromise: The intentional or unintentional disclosure of information to unauthorized individuals or processes. Also, the intentional or unintentional violation of security policies or controls that could potentially result in the unauthorized disclosure, modification, loss, or destruction of information.

Confidentiality: Assurance that information is available only to authorized entities.

Cross-Certificate: A certificate issued by one Certification Authority in a PKI domain to Certification Authority in another PKI domain to establish a trust relationship. In effect, cross-certification allows organizations to trust all, or a subset of certificates issued by partner organizations. End-entities can rely on certificates from other organizations as if their own organization had issued them, subject to limitations that can be placed on cross-certified organization certificates. For example, an organization can choose to trust only certificates issued under a Medium Assurance level at the partner organization.

Custodian: An individual who is responsible for a device, application, and service and can make requests to a CA or RA for certificate enrollment, revocation, or renewal on behalf of the device, application, or service. See Application Owner.

Cryptographic Module: According to FIPS 140-2, the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Data Integrity: The assurance that data has not been modified or altered in any way from creation to reception. Digital signatures are used to provide assurance of data integrity. CAs and other entities use digital signatures to provide assurance that the data has not been altered or modified. See Message Digest.

Digital Signature: An electronic analogue of paper signatures. Digital signatures cannot be forged. They provide assurance of the identity of the entity that signs the data, and that the data has not been modified from the moment the signature is applied to reception. Digital signatures make use of public key encryption and message digests. When a block of data is signed with a digital signature, a message digest is computed for the data and the message digest encrypted with the sender's private key. The recipient of the data decrypts the received message digest with the sender's public key, independently computes a message digest for the received data, and compares the two message digests. If the two message digests are identical, the recipient has assurance that the data has not been altered. Assurance of the identity of the sender is function of the level of trust the recipient has that only the sender of the message is in possession of the private key used to sign the data of the key pair. If the level of assurance is high or very high, then non-repudiation can also be asserted with digital signatures.

Enrollment Agent: A trusted individual or service that is authorized to enroll certificates on behalf of a Subscriber. Typically, enrollment agents enroll smart card certificates on behalf of Subscribers.

Extended Validation (EV) Certificate: A certificate that asserts a high degree of assurance of the identity of a Web server. In browsers that support EV certificates, the address bar turns green when a user connects to a Web site that uses an EV certificate to identify itself and to provide encryption of data by using SSL. The authentication requirements to apply for an EV certificate are more rigorous than the requirements to apply for a typical SSL certificate.

FIPS PUB 140-2: Also known as FIPS 140-2, the designation for the Federal Information Processing Standards that provides security requirements for cryptographic modules. FIPS 140-2 provides four levels of security, numbered one through four. The higher levels specify stringent and robust requirements for protection against physical threats, such as tampering with cryptographic modules and resistance to environmental threats.

Hardware Security Module (HSM): Special purpose cryptographic hardware that is used to protect private keys that have a high value.

Host Trust Link: A binding protocol to maintain the connection's association with a given VM regardless of where that physical VM instantiation resides.

Issuing CA: The entity responsible for managing all aspects (issuance, renewal, revocation, etc.) of certificates for end-entity Subscribers.

Key: A value used as input into an encryption algorithm along with the plaintext or ciphertext in order to encrypt or decrypt a message, respectively. See Algorithm.

Key Escrow: The secure holding, in trust, of a Subscriber's private key by an agent for the benefit of the Subscriber. Key escrow provides a means to store private keys securely and for an agent to deliver the private key to the Subscriber in the event the Subscriber's private key is lost or destroyed.

Key Pair: Also known as Asymmetric key pair or public key pair. Two keys (a public and a private key) that are mathematically related in such a way that it is not feasible to derive one key from knowledge of the other key or from a combination of the knowledge of the key and the resultant ciphertext. For example, a message encrypted with a public key can only be decrypted by using the private key of the key pair. It is not feasible to derive the private key from knowledge of the ciphertext and the public key.

Key Recovery Agent: An agent who is authorized to recover escrowed private keys for Certificate Subscribers. See Key Escrow.

Local Registration Authority (LRA): A Registration Authority that has responsibility for a local community. See Registration Authority.

Master Backup Key: The Master Backup Key (MBK) is used within an Utimaco HSM to decrypt key pairs used by HSM clients. The same MBK is implemented at each HSM to allow keys to be used on any HSM within the specific environment.

Message Digest: Also known as a hash value or digest, the result of a cryptographic hash function which uses an algorithm that provides a deterministic result (eg, SHA-1). A cryptographic hash function operates on a block of data and returns a hash value in the form of a bit string. The cryptographic hash function will always return the same hash value for the block of data as long as no changes to the data occur. However,

it is computationally infeasible to derive the block of data from knowledge of the hash value. Furthermore, it is highly improbable that two different blocks of data will result in the same hash value. Because of these properties, message digests are often used as part of the digital signing process to provide assurance of the integrity of the data. See Data Integrity.

Non-repudiation: An assurance of sufficient strength that an actor cannot later deny having performed a particular action.

OID: Object identifier. A specially formatted globally unique dotted numeric string that identifies an organization and the services or entities it controls. Organizations such as Tesla acquire an OID arc from a naming authority, such as IANA. The OID arc for Tesla is 1.3.6.1.4.1.49279. Tesla subsequently controls any subarcs under the arc it owns. In the context of a PKI implementation, Tesla uniquely identifies assurance levels by using OIDs created under the Tesla OID arc by adding dotted numeric strings to the right of the arc, for example, {1.3.6.1.4.1.49279.2.1.2. OIDS are used to identity other elements in PKI, for example, encryption algorithms. OIDs create almost no computational burden and can be very long, as a consequence.

Outsourcer: Commercial entity that has been retained to perform operational duties. Outsourcer shall be contractually bound by non-disclosure agreements and service level agreements creating equivalent confidentiality and responsibility to that of direct Tesla employees.

Personal Data: Personal Data is defined in Tesla Policy 90 as "Information about living individuals which is held in automatically processable form (for example, on a computer) or in a structured manual filing system."

PIN Entry Device: Device used to input PINs for Utimaco HSM management smart cards.

PKCS: Public Key Cryptography Standards. Published by RSA, a series of standards that describe methods, syntax, storage, communication and aspects of public keys. For example, PKCS #1 defines methods for encrypting and signing data by using RSA's public key cryptography system; PKCS #11 defines methods for communicating with hardware based cryptographic devices such as smartcards.

Plaintext: Unencrypted text.

Private Key: A private key is the key that is under the control of the Subscriber identified in Subject of a Certificate. In a PKI, the private key has two primary functions: to decrypt messages that are encrypted with the corresponding Public Key, and to encrypt the Message Digest to provide assurance of data integrity (Digital Signature).

Public Key: A Public Key is the key bound to a certificate that is available to Relying Parties (Certificate User) and identifies the Subject in the certificate as the holder of the corresponding private key. In a PKI, the Public Key has two primary functions: to encrypt messages that are sent to the holder of the private key and to decrypt the Message Digest to provide assurance of data integrity (Digital Signature).

Quorum: Minimum number of entities belonging to set of entities that must be present to authorize a particular operation, process, or action.

Registration Authority (RA): An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates.

Relying Party: A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. Synonymous with the term "Certificate User".

Risk: A measure of the likelihood and impact of harm if a threat is realized or vulnerability exploited. Risk is

often expressed as the sum of the threat plus the vulnerability plus the impact (value of the affected asset).

Root CA: The highest authority in a hierarchy of CAs and the start of the trust path for CA hierarchy. In environments that require high degrees of trust and assurance, Root CAs are limited to issuing, renewing and revoking certificates of subordinate CAs and to publishing CRLs. Also, because the compromise of a Root CA could have profound consequences, Root CAs is often kept in high security facilities and are turned off when not in use.

Smart card: Approximately the size of credit card, a smart card is a hardware device that contains a small microprocessor with sufficient capacity to store and transfer information. Smartcards can contain cryptographic modules that can generate and store key pairs and certificates. Smart cards have robust security features. It is not possible to export private keys from them. Also, some smart cards have the ability ~~to zeroize key material under certain conditions, such as too many attempts to activate the private with an~~ incorrect PIN. Because of the robust security of smart cards, they are often used in situations where levels of assurance are required.

Subordinate CA: A Certification Authority that is issued a CA certificate authorizing it in a PKI hierarchy from a Superior CA.

Subscriber: The entity whose identity has been bound to a Tesla CA certificate and to whom the Tesla CA certificate was issued. Synonymous with the term "Certificate Holder".

Superior CA: A Certification Authority that issues certificates to subordinate CAs.

Symmetric Encryption: Also known as shared secret encryption, uses a single key for data encryption and decryption. With symmetric encryption both the sender and recipient possess the same key that enables then to encrypt and decrypt data. A disadvantage of symmetric key encryption is its vulnerability to compromise during the key exchange between parties that wish to exchange encrypted messages. An advantage of symmetric encryption is that it is not computationally expensive to encrypt or decrypt messages using this method. Because of these properties, symmetric encryption is often used in combination with the more computationally expensive asymmetric encryption. Asymmetric encryption is used to encrypt the shared secret to assure confidentiality of shared secret key during transmission of the shared secret key. See Asymmetric Encryption.

Tesla Product: Any physical item or service, or part thereof that is sold to end customers

Tesla Manufacturing equipment: any physical item or service that is used for the manufacturing of Tesla Products

Threat: The probability or likelihood that an event or agent will cause harm to an information system resulting in the loss or unauthorized destruction, modification, or disclosure of data.

Vulnerability: A weakness in a system, process, or policy that can be exploited to cause harm to information systems, resulting in the loss or unauthorized destruction, modification, or disclosure of data.

13 Acknowledgements

The authors of the document would like to acknowledge the contributions of Brian Komar to this certificate policy.

14 APPROVAL SIGNATURES

14.1 Reviewer's Signature

The signature below affirms that you have reviewed this document to ensure its accuracy:

Name and Title	Signature	Date

14.2 Approver's Signature

Your signature affirms that this procedure is accurate and complete and has been reviewed by the appropriate persons and reflects the area's current processes.

Name and Title	Signature	Date

14.3 Quality Integrator's Signature

Your signature affirms that this procedure complies with applicable corporate and local requirements.

Name and Title	Signature	Date