PKI Certificate Policy

Version HEAD 04a776875, 2022-12-19 10:12:22 -0800: Approved

Table of Contents

Notice and Disclaimer . . . 1
1. Introduction . . . 2
1.1. Overview . . . 2
1.2. References . . . 3
1.3. Document Name and Identification . . . 4
1.4. PKI Participants . . . 4
1.4.1. Requirements for candidate PAA/PAI . . . 5
1.4.2. Certification Authorities (CAs) . . . 6
1.4.3. Registration Authority (RA) . . . 6
1.4.4. Requestors . . . 6
1.4.5. Relying Parties . . . 7
1.4.6. Other Participants . . . 7
1.4.6.1. Management Authority (MA) . . . 7
1.4.6.2. Certificate Requesting Account (CRA) . . . 8
1.4.6.3. Other Request Methods . . . 8
1.5. Certificate Usage . . . 8
1.5.1. Appropriate Certificate Uses . . . 8
1.6. Prohibited Certificate Uses . . . 8
1.7. Policy Administration . . . 8
1.7.1. Organization Administering the Document . . . 8
1.7.2. Contact Person . . . 9
1.7.3. Person Determining CPS Suitability for the Policy . . . 9
1.7.4. CPS Approval Procedures . . . 9
1.8. Definitions and Acronyms . . . 9
1.8.1. Definitions . . . 9
1.8.2. Acronyms . . . 14
2. Publication and Repository Responsibilities . . . 16
2.1. Repositories . . . 16
2.2. Publication of Certification Information . . . 16
2.3. Time or Frequency of Publication . . . 16
2.4. Access Controls on Repositories . . . 16
3. Identification and Authentication . . . 17
3.1. Naming . . . 17
3.1.1. Types of Names . . . 17
3.1.2. Need for Names to Be Meaningful . . . 17
3.1.3. Anonymity or Pseudonymity of Requestors . . . 17
3.1.4. Rules for Interpreting Various Name Forms . . . 17
3.1.5. Uniqueness of Names . . . 17

3.1.6. Recognition, Authentication, and Role of Trademarks . . . 17
3.2. Initial Identity Validation . . . 18
3.2.1. Method to Prove Possession of Private Key . . . 18
3.2.2. Authentication of Organization Identity . . . 18
3.2.3. Authentication of Individual Identity . . . 18
3.2.4. Non-verified Requestor Information . . . 19
3.2.5. Validation of Authority . . . 19
3.2.6. Criteria for Inter-operation . . . 19
3.3. Identification and Authentication for Re-key Requests . . . 19
3.3.1. Identification and Authentication for Routine Re-key . . . 19
3.3.2. Identification and Authentication for Re-key After Revocation . . . 19
3.4. Identification and Authentication for Revocation Request . . . 19
4. Certificate Lifecycle Operational Requirements . . . 20
4.1. Certificate Application . . . 20
4.1.1. Certificate Application Submitters . . . 20
4.1.2. Enrollment Process and Responsibilities . . . 20
4.2. Certificate Application Processing . . . 20
4.2.1. Performing Identification and Authentication Functions . . . 20
4.2.2. Approval of Certificate Applications . . . 20
4.2.3. Time to Process Certificate Applications . . . 21
4.3. Certificate Issuance . . . 21
4.3.1. CA Actions During Certificate Issuance . . . 21
4.3.2. Notification to Requestor by the CA of Issuance of Certificates . . . 21
4.4. Certificate Acceptance . . . 21
4.4.1. Conduct Constituting Certificate Acceptance . . . 21
4.4.2. Publication of the Certificate by the CA . . . 22
4.4.3. Notification of Certificate Issuance by the CA to Other Entities . . . 22
4.5. Key Pair and Certificate Usage . . . 22
4.5.1. Requestor Private Key and Certificate Usage . . . 22
4.5.2. Relying Party Public Key and Certificate Usage . . . 22
4.6. Certificate Renewal . . . 23
4.7. Certificate Re-key . . . 23
4.8. Certificate Modification . . . 23
4.9. Certificate Revocation and Suspension . . . 23
4.10. Certificate Status Services . . . 23
4.10.1. Operational Characteristics . . . 23
4.10.2. Service Availability . . . 23
4.10.3. Optional Features . . . 23
4.11. Key Escrow and Recovery . . . 24
4.11.1. Key Escrow and Recovery Policy and Practices . . . 24
4.11.2. Session Key Encapsulation and Recovery Policy and Practices . . . 24

5. Facility, Management, and Operational Controls . . . 25
5.1. Physical Controls . . . 25
5.1.1. Site Location and Construction . . . 25
5.1.2. Physical Access . . . 25
5.1.2.1. RA Equipment Physical Access . . . 27
5.1.3. Power and Air Conditioning . . . 27
5.1.4. Water Exposures . . . 27
5.1.5. Fire Prevention and Protection . . . 27
5.1.6. Media Storage . . . 27
5.1.7. Waste Disposal . . . 27
5.1.8. Off-site Backup . . . 28
5.2. Procedural Controls . . . 28
5.2.1. Trusted Roles . . . 28
5.2.2. Number of Persons Required per Task . . . 28
5.2.3. Identification and Authentication for Each Role . . . 29
5.2.4. Roles Requiring Separation of Duties . . . 29
5.3. Personnel Controls . . . 30
5.3.1. Qualifications, Experience, and Clearance Requirements . . . 30
5.3.2. Background Check Procedures . . . 30
5.3.3. Training Requirements . . . 31
5.3.4. Retraining Frequency and Requirements . . . 31
5.3.5. Job Rotation Frequency and Sequence . . . 31
5.3.6. Sanctions for Unauthorized Actions . . . 31
5.3.7. Independent Contractor Requirements . . . 31
5.3.8. Documentation Supplied to Personnel . . . 32
5.4. Audit Logging Procedures . . . 32
5.4.1. Types of Events Recorded . . . 32
5.4.2. Frequency of Processing Log . . . 34
5.4.3. Retention Period for Audit Log . . . 34
5.4.4. Protection of Audit Log . . . 34
5.4.5. Audit Log Backup Procedures . . . 34
5.4.6. Audit Collection System (Internal vs. External) . . . 34
5.4.7. Notification to Event-Causing Subject . . . 35
5.4.8. Vulnerability Assessments . . . 35
5.5. Records Archival . . . 35
5.5.1. Types of Events Archived . . . 35
5.5.2. Retention Period for Archive . . . 36
5.5.3. Protection of Archive . . . 36
5.5.4. Archive Backup Procedures . . . 36
5.5.5. Requirements for Time-Stamping of Records . . . 36
5.5.6. Archive Collection Systems (Internal or External) . . . 36

5.5.7. Procedures to Obtain and Verify Archive Information . . . 36
5.6. Key Changeover . . . 36
5.7. Compromise and Disaster Recovery . . . 37
5.7.1. Incident and Compromise Handling Procedures . . . 37
5.7.2. Computing Resources, Software, and/or Data Are Corrupted . . . 37
5.7.3. Entity (CA) Private Key Compromise Procedures . . . 37
5.7.4. Business Continuity Capabilities After a Disaster . . . 38
5.8. CA and RA Termination . . . 39
6. Technical Security Controls . . . 40
6.1. Key Pair Generation and Installation . . . 40
6.1.1. Key Pair Generation . . . 40
6.1.1.1. CA Key Pair Generation . . . 40
6.1.1.2. Requestor Key Pair Generation . . . 40
6.1.2. Private Key Delivery to Requestor . . . 41
6.1.3. Public Key Delivery to Certificate Issuer . . . 41
6.1.4. CA Public Key Delivery to Relying Parties . . . 41
6.1.5. Key Sizes . . . 41
6.1.6. Public Key Parameters Generation and Quality Checking . . . 42
6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field) . . . 42
6.2. Private Key Protection and Cryptographic Module Engineering Controls . . . 42
6.2.1. Cryptographic Module Standards and Controls . . . 42
6.2.2. Private Key (n out of m) Multi-Person Control . . . 42
6.2.3. Private Key Escrow . . . 43
6.2.4. Private Key Backup . . . 43
6.2.5. Private Key Archival . . . 43
6.2.6. Private Key Transfer into or from a Cryptographic Module . . . 44
6.2.7. Private Key Storage on Cryptographic Module . . . 44
6.2.8. Method of Activating Private Keys . . . 44
6.2.8.1. CA Administrator Activation . . . 45
6.2.8.2. Offline CA Private Keys . . . 45
6.2.8.3. Online CA Private Keys . . . 45
6.2.8.4. Requestor Private Keys . . . 45
6.2.9. Method of Deactivating Private Keys . . . 45
6.2.10. Method of Destroying Private Keys . . . 46
6.2.11. Cryptographic Module Rating . . . 46
6.3. Other Aspects of Key Pair Management . . . 46
6.3.1. Public Key Archival . . . 46
6.3.2. Certificate Operational Periods and Key Pair Usage Periods . . . 46
6.4. Activation Data . . . 46
6.4.1. Activation Data Generation and Installation . . . 46
6.4.2. Activation Data Protection . . . 47

6.4.3. Aspects of Activation Data . . . 47
6.4.3.1. Activation Data Transmission . . . 47
6.4.3.2. Activation Data Destruction . . . 48
6.5. Computer Security Controls . . . 48
6.5.1. Specific Computer Security Technical Requirements . . . 48
6.5.2. Computer Security Rating . . . 49
6.6. Lifecycle Technical Controls . . . 49
6.6.1. System Development Controls . . . 50
6.6.2. Security Management Controls . . . 50
6.6.3. Lifecycle Security Controls . . . 50
6.7. Network Security Controls . . . 51
6.8. Time-Stamping . . . 51
7. Certificate, CRL and OCSP Profiles . . . 52
7.1. Certificate Profile . . . 52
7.1.1. Version Number(s) . . . 52
7.1.2. Certificate Extensions . . . 53
7.1.2.1. Subject Key Identifier Extension . . . 53
7.1.2.2. Basic Constraints Extension . . . 53
7.1.3. Algorithm Object Identifiers (OIDs) . . . 53
7.1.4. PAA Certificate . . . 53
7.1.5. PAI Certificate . . . 53
7.1.6. Device Attestation Certificate (DAC) . . . 53
7.1.7. Name Forms . . . 54
7.1.8. Name Constraints . . . 54
7.1.9. Certificate Policy Object Identifier . . . 54
7.1.10. Usage of Policy Constraints Extension . . . 54
7.1.11. Policy Qualifiers Syntax and Semantics . . . 54
7.1.12. Processing Semantics for the Critical *Certificate Policies* Extension . . . 54
7.2. CRL Profile . . . 54
8. Compliance Audit and Other Assessments . . . 55
8.1. Frequency or Circumstances of Assessment . . . 55
8.2. Identity/Qualifications of Assessor . . . 55
8.3. Assessor’s Relationship to Assessed Entity . . . 55
8.4. Topics Covered by Assessment . . . 55
8.5. Actions Taken because of Deficiency . . . 56
8.6. Communication of Results . . . 56
9. Other Business and Legal Matters . . . 57
9.1. Fees . . . 57
9.1.1. Certificate Issuance or Renewal Fees . . . 57
9.1.2. Certificate Access Fees . . . 57
9.1.3. Revocation or Status Information Access Fees . . . 57

9.1.4. Fees for Other Services . . . 57
9.1.5. Refund Policy . . . 57
9.2. Financial Responsibility . . . 57
9.2.1. Insurance Coverage . . . 57
9.2.2. Other Assets . . . 57
9.2.3. Insurance or Warranty Coverage for End-Entities . . . 57
9.3. Confidentiality of Business Information . . . 57
9.3.1. Scope of Confidential Information . . . 58
9.3.2. Information Not Within the Scope of Confidential Information . . . 58
9.3.3. Responsibility to Protect Confidential Information . . . 58
9.4. Privacy of Personal Information . . . 58
9.4.1. Privacy Policy . . . 58
9.4.2. Information Treated as Private . . . 58
9.4.3. Information Not Deemed Private . . . 58
9.4.4. Responsibility to Protect Private Information . . . 58
9.4.5. Notice and Consent to Use Private Information . . . 58
9.4.6. Disclosure Pursuant to Judicial or Administrative Process . . . 59
9.4.7. Other Information Disclosure Circumstances . . . 59
9.5. Intellectual Property Rights . . . 59
9.6. Representations and Warranties . . . 59
9.6.1. CA Representations and Warranties . . . 59
9.6.2. RA Representations and Warranties . . . 60
9.6.3. Requestor Representations and Warranties . . . 60
9.6.4. Relying Party Representations and Warranties . . . 60
9.6.5. Representations and Warranties of Other Participants . . . 61
9.7. Disclaimers of Warranties . . . 61
9.8. Limitations of Liability . . . 61
9.9. Indemnities . . . 61
9.10. Term and Termination . . . 61
9.10.1. Term . . . 61
9.10.2. Termination . . . 61
9.10.3. Effect of Termination and Survival . . . 62
9.11. Individual Notices and Communications with PKI Participants . . . 62
9.12. Amendments . . . 62
9.12.1. Procedure for Amendment . . . 62
9.12.2. Notification Mechanism and Period . . . 62
9.12.3. Circumstances Under Which OID SHALL be Changed . . . 62
9.13. Dispute Resolution Provisions . . . 62
9.14. Governing Law . . . 62
9.15. Compliance with Applicable Law . . . 63
9.16. Miscellaneous Provisions . . . 63

9.16.1. Entire Agreement . . . 63
9.16.2. Assignment . . . 63
9.16.3. Severability . . . 63
9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights) . . . 63
9.16.5. Force Majeure . . . 63
9.17. Other Provisions . . . 63

Notice and Disclaimer

Copyright © Connectivity Standards Alliance (2021-2022). All rights reserved. The information within this document is the property of the Connectivity Standards Alliance and its use and disclosure are restricted.

Elements of this document may be subject to third party intellectual property rights, including without limitation, patent, copyright or trademark rights (such a third party may or may not be a member of the Connectivity Standards Alliance). The Connectivity Standards Alliance is not responsible and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

Commented sections of this document are to be considered not in effect.

This document and the information herein is furnished on an "AS IS" basis and Connectivity Standards Alliance DISCLAIMS ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO (A) ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OF THIRD PARTIES (INCLUDING WITHOUT LIMITATION ANY INTELLECTUAL PROPERTY RIGHTS INCLUDING PATENT, COPYRIGHT OR TRADEMARK RIGHTS) OR (B) ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NONINFRINGEMENT. IN NO EVENT WILL THE CONNECTIVITY STANDARDS ALLIANCE BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF INTEROPERABILITY, IMPROPER INTEROPERABILITY, LOSS OF FUNCTIONALITY, LOSS OF USE OF DATA, INTERRUPTION OF BUSINESS, OR FOR ANY OTHER DIRECT, INDIRECT, SPECIAL OR EXEMPLARY, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, IN CONTRACT OR IN TORT, IN CONNECTION WITH THIS DOCUMENT OR THE INFORMATION CONTAINED HEREIN, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. All company, brand and product names in this document may be trademarks that are the sole property of their respective owners. Any use or reliance on the information in this document is at the risk of the user.

This Notice and Disclaimer statement must be included on all copies of this document that are made.

The Connectivity Standards Alliance reserves the right to revise this document at any time for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, security advances, or changes in design, manufacturing techniques, or operating procedures described, or referred to, herein.

This work, "Matter PKI Certificate Policy", is a derivative of the "CableLabs PKI Certificate Policy" by Cable Television Laboratories, Inc., used under CC BY 4.0. "PKI Certificate Policy" is licensed under CC BY 4.0. To view a copy of the CC BY 4.0 license, visit http://creativecommons.org/licenses/by/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Chapter 1. Introduction

1.1. Overview

This document defines the policies by which the Matter Public Key Infrastructure (Matter PKI) will be governed by the Matter PKI Policy Authority (PKI-PA). The PKI-PA (the Connectivity Standards Alliance (CSA)) has the final authority over the Matter PKI Certificate Policy (CP). Any policy items not covered by the Matter PKI CP are left to the consideration of the PKI-PA. The PKI-PA procedure in such an unforeseen case should involve TCOC and BoD approval. PKI-PA, at its discretion, may involve also security experts.

This CP comprises the policy framework for the Matter PKI and is consistent with the Internet X.509 PKI Certificate Policy and Certification Practices Framework [RFC 3647][1] . It governs the operations of the PKI components by all individuals and entities within the infrastructure (collectively, PKI Participants). It provides the requirements that PKI Participants SHALL meet when issuing and managing Certificate Authorities (CAs), Certificates, and private keys. In addition, it informs potential Relying Parties about what they need to know prior to relying on issued Certificates.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX), Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC 3647] [1] . To preserve the outline specified by [RFC 3647][1] , section headings that do not apply have the statement “No stipulation.”

This CP also defines the terms and conditions under which the CAs SHALL operate to issue Certificates. Where “operate” includes Certificate management (i.e., approval, and issuance) of issued Certificates, and "issue" in this context refers to the process of digitally signing, with the private key associated with its authority Certificate, a structured digital object conforming to the X.509, version 3 Certificate format.

In addition, this CP acts as an umbrella document establishing baseline requirements and applies consistently throughout the entire Matter PKI, thereby providing a uniform level of trust throughout the applicable community. It describes the overall business, legal, and technical infrastructure of the Matter PKI. More specifically, it describes the:

- Appropriate applications for, and the assurance levels associated with, the PKI Certificates;
- Obligations of a Certificate Authority (CA);
- Requirements for Compliance Audit (Audit) and related security and practices reviews;
- Methods to confirm the identity of Certificate Applicants;
- Operational procedures for Certificate lifecycle services: Certificate Applications, issuance, acceptance, and renewal;
- Operational security procedures for Audit logging, records retention, and disaster recovery;
- Physical, personnel, key management, and logical security;
- Certificate profile; and
- Ancillary agreements, such as the Requestor Agreement Document (RAD).

Throughout this CP, the words that are used to define the significance of requirements are:

Table 1. Normative Reference

"SHALL"	This word, or the word “require”, means that the definition is an absolute requirement of this CP.
"SHALL NOT"	This phrase means that the definition is an absolute prohibition of this CP.
"SHOULD"	This word means that there may exist valid reasons circumstances to ignore this item, but the full implications SHOULD be understood, and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons circumstances when the listed behavior is acceptable or even useful, but the full implications SHOULD be understood, and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word, or the word “optional”, means that an item is truly discretionary.

1.2. References

This CP uses the following references:

Table 2. References Table

Ref #	Doc Number	Reference Title
[1]	RFC 3647	Internet X.509 PKI Certificate Policy and Certification Practices Framework, IETF (Chokhani, Ford, Sabett, Merrill, and Wu), November 2003. http://www.ietf.org/rfc/rfc3647.txt
[2]	X.501	ITU-T Recommendation X.501 (10/2019): Information Technology - Open Systems Interconnection - The Directory: Models. X.501: Information technology - Open Systems Interconnection - The Directory: Models (itu.int)

Ref #	Doc Number	Reference Title
[3]	RFC 5280	Internet X.509 PKI Certificate and Certification Revocation List (CRL) Profile, IETF (Cooper, Santesson, Farrell, Boeyen, Housley, and Polk), May 2008. http://www.ietf.org/rfc/rfc5280.txt
[4]	FIPS 140-3*	Security Requirements for Cryptographic Modules, FIPS 140-3, March 22, 2019. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
[5]	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF (Myers, Ankney, Malpani, Galperin, Adams), June 2013. http://www.ietf.org/rfc/rfc6960.txt
[6]	Matter Specification	Connectivity Standards Alliance Matter Specification, May 2022.

*During the transition period until September 21, 2026, every reference of FIPS 140-3 in this document SHALL refer to as either the use of FIPS 140-3 or FIPS 140-2. After September 21, 2026, FIPS 140-2 will no longer be accepted.

1.3. Document Name and Identification

This document is the Matter PKI CP. The Connectivity Standards Alliance acting as a PKI Policy Authority (PKI-PA), in the future, MAY assign a policy object identifier value extension for the class of Certificate specified within this CP.

Note: The Matter Specification [6] is the authoritative reference for Certificate profiles and Certificate usage.

1.4. PKI Participants

The Matter PKI shown in Figure 1 is comprised of a two-tier infrastructure with multiple Root CAs at tier 1 called Product Attestation Authority (PAA) CAs, forming a federated apex of the hierarchy. The PAA CAs issues the tier 2 Subordinate CA (Sub-CA) Certificates called Product Attestation Intermediate (PAI) CAs. Each PAI CA issues Certificates called Device Attestation Certificate (DAC) to authorized entities (i.e., Manufacturers (MFR)). MFRs embed the DAC into Matter compliant devices and commissionable components. Each PAI CA is restricted to only issue DACs for a single vendor (i.e. MFR) which is indicated by the Vendor Identifier (VID) within the PAI Certificate. The PAI CA

can be further restricted to only issue DACs for a single product of a vendor if a Product Identifier (PID) is included in the PAI Certificate.

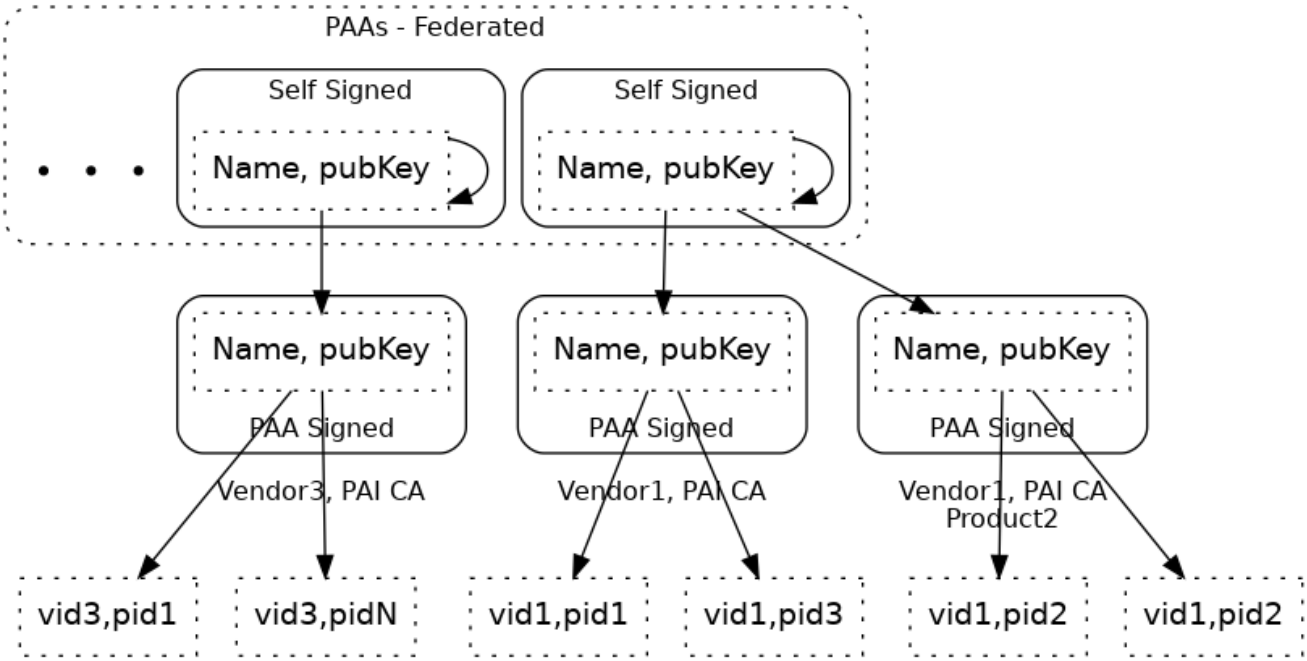

Figure 1. Device Attestation PKI Hierarchy

1.4.1. Requirements for candidate PAA/PAI

A PAA (VID-scoped PAA or broader) candidate SHALL fulfil the following criteria (which the PKI-PA will validate):

- the PAA candidate is a CSA Participant or Promoter member in good standing and Matter Working Group (WG) member;
- the submitted CPS fulfills the requirements of Matter PKI CP for PAA;
- the submitted RAD fulfills the requirements of Matter PKI CP for PAA;
  NOTE: When the same entity that operates a PAA also operates a PAI to issue DACs within the same organization (e.g. for VID-scoped PAAs), the PAI/DAC policies MAY be covered within the CPS rather than in a RAD. In that case a RAD MAY be omitted since the requestor and the CA are the same entity altogether.
- for the VID-scoped PAA: the owner of the VID authorizes the PAA candidate request and the VID is encoded in the appropriate PAA field(s); and
- follow any additional requirements of Matter PKI CP on Identification and Authentication and Certificate Application.

A PAI candidate to be created under another party's PAA (i.e. non-VID-scoped PAA) SHALL fulfil the following criteria (which the PKI-PA will validate):

- the PAI candidate is a CSA Participant or Promoter member in good standing and Matter WG member;
- the submitted CPS fulfills the requirements of Matter PKI CP for PAI;
- the submitted RAD fulfills the requirements of Matter PKI CP for PAI;

- the Requestor i.e. the owner of the PAI VID authorizes the PAI candidate request and the VID is encoded in the appropriate PAI field(s); and
- follow any additional requirements of Matter PKI CP on Identification and Authentication and Certificate Application

A PAI established and operated by a VID-scoped PAA:

- SHALL submit CPS to CSA for the record, but does NOT require approval prior to PAI creation.

1.4.2. Certification Authorities (CAs)

The CAs in the Matter PKI fall into two categories: (1) the PAAs, which issue the PAI Certificates; and (2) the PAIs, which issue DAC Certificates for devices and other commissionable software components (DACs). The CAs are authorized to issue, manage, and renew Certificates and are responsible for:

- Developing and maintaining its Certification Practice Statements (CPSs);
- Issuing compliant Certificates;
- Securing delivery of Certificates to its Requestors;
- Generating, protecting, operating, and destroying CA private keys;
- Managing all aspects of the CA services, operations, and infrastructure related to Certificates issued under this CP and ensuring that they are performed in accordance with the requirements, representations, and warranties of this CP; and
- Acting as a trusted party to facilitate the confirmation of the binding between a public key and the identity, and/or other attributes and values, of the “Subject” of the Certificate.

1.4.3. Registration Authority (RA)

The RA is the entity that collects and verifies each Requestor’s identity and the information that is to be entered in the public key Certificate. The RA interacts with the CA to enter and approve the Requestor Certificate request information.

1.4.4. Requestors

In the Matter PKI, the Requestor is the entity named in the RAD. An authorized representative of the Requestor, as a Certificate Applicant, completes the Certificate issuance process established by the CA. In response, the CA confirms the identity of the Certificate Applicant and either approves or denies the Certificate Application. If approved, the Requestor MAY request Certificates:

- via a web-based Certificate Requesting Account (CRA) or directly from the PAI, for use in Matter compliant devices or other commissionable software components; or
- their PAI to generate device Certificates for use in their Matter compliant devices or other commissionable software components.

CAs may require that Requestors adopt the appropriate requirements and any additional Certificate management practices to govern the Requestor’s practice for requesting Certificates and handling

the corresponding private keys. The Requestor agrees to be bound by its obligations through execution of the CA's RAD.

CAs, technically, are also Requestors of Certificates within a PKI, either as a PAA issuing a self-signed Certificate to itself, or as a PAI issuing a Certificate by a PAA. References to "Requestors" in the CP, however, apply only to the device Certificates and PAIs.

For a member requesting DAC Certificates at a PAI which is not run by that vendor, the PAI SHALL validate:

- that the Requestor is a CSA member; this check should be done by the company running the PAI at least once a year.

1.4.5. Relying Parties

The Relying Party MAY be any entity that validates the binding of a public key to the Requestor's name in a Matter PKI Certificate. The Relying Party is responsible for deciding whether or how to check the validity of the Certificate by checking the appropriate Certificate status information. The Relying Party can use the Certificate to verify the integrity of a digitally signed message, to identify the initiator of a communication, or to establish confidential communications with the holder of the Certificate, in all cases the Matter Specification [6] is the authoritative reference for Certificate usage.

1.4.6. Other Participants

1.4.6.1. Management Authority (MA)

The Connectivity Standards Alliance, as the PKI-PA, MAY offload some of its duties to an MA to manage the design, the development, and the implementation of the PKI architecture on behalf of the PKI-PA. The MA's role is to provide trust management services to support the ecosystem in meeting its security goals using the Matter PKI.

The MA'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 Certificate Policies and standards. Activities of the MA include the:

- Process for CAs to submit CPSs;
- Rules/process for PKI-PA to approve CPSs;
- Process for recognizing Requestors, their authorized representatives, and their agreements for CRAs;
- Process for Audits;
- Registration of PAIs; and
- Registration of Requestors.

The PKI-PA can perform the MA duties itself or designate a trusted third party to act as the MA on its behalf to provide operational support and maintain the Matter PKI in accordance with the CP.

1.4.6.2. Certificate Requesting Account (CRA)

The CRA is an account interface for services hosted by a entity complying with the Certificate Authority Auditing Framework (CAAF) that is used to issue Certificates in bulk and in batch mode to Requestors. In the CRA architecture, the Requestor uses a standard web browser, a command line interface or an easily portable client to connect to the hosted Requestor PAI's interface. Via this interface, the Requestor will request appropriate device Certificates and obtain the resulting signed Certificates.

1.4.6.3. Other Request Methods

Some vendors MAY need just-in-time issuance of DACs, in which case a CRA might not be used.

1.5. Certificate Usage

This CP applies to all Matter PKI Participants, including Requestors and Relying Parties. This CP sets forth policies governing the use of Matter PKI Certificates. Each Certificate is generally appropriate for use with the applications set forth in this CP.

1.5.1. Appropriate Certificate Uses

CAs SHALL adhere to the CSA Matter Specification for which they are issuing the Certificates.

1.6. Prohibited Certificate Uses

Matter PKI Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances, or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or military use or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

1.7. Policy Administration

1.7.1. Organization Administering the Document

The Connectivity Standards Alliance is the PKI-PA. It owns the CP and represents the interest of its members in developing the policies that govern the Matter PKI. The PKI-PA is responsible for all aspects of this CP, including:

- Maintaining this CP;
- Governing and operating the PKI according to this CP;
- Approving the CPS for CAs that issue Certificates under this CP; and
- Approving the Audit for CAs operating under this CP.

1.7.2. Contact Person

Inquiries regarding this CP can be directed to the PKI-PA at:

Matter PKI Policy Authority

Connectivity Standards Alliance

Email: certification@csa-iot.org

www.csa-iot.org

1.7.3. Person Determining CPS Suitability for the Policy

The PKI-PA SHALL approve the CPS for each CA that issues Certificates under this CP.

1.7.4. CPS Approval Procedures

CAs operating under this CP SHALL meet all facets of the policy. The PKI-PA SHALL determine if a CPS complies with this CP. The CA SHALL complete a CPS on how it will meet all the CA requirements of this CP and receive approval from the PKI-PA before commencing operations. In some cases, the PKI-PA MAY require the additional approval of the Connectivity Standards Alliance members.

1.8. Definitions and Acronyms

1.8.1. Definitions

This CP uses the following terms and definitions:

Table 3. Definitions

Term	Description
Certificate	A digital representation of information which at least: • Identifies its issuing CA; • Names or identifies the Requestor of the Certificate; • Contains the Requestor's public key; • Identifies its operational period; and • Is digitally signed by the issuing CA.
Certificate Applicant	An individual representing the Requestor that requests the issuance of a Certificate by a CA.

Term	Description
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to the CA for the issuance of a CRA. The request, also called a naming application (which is part of the RAD), contains the naming information that will be included in the device Certificates.
Certificate Authority Auditing Framework (CAAF)	A framework for auditing Certificate Authority implementations
Certificate Chain	An ordered list of Certificates containing a Requestor Certificate and one or more CA Certificates, which terminates in a Root Certificate.
Certificate Policy (CP)	A document addressing all aspects associated with the generation, production, distribution, accounting, Compromise, recovery, and administration of Certificates.
Certificate Requesting Account (CRA)	The online portal to assist Certificate Applicants in requesting Certificates, if provided by the CA.
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued.
Certificate Status Server (CSS)	An authority that provides status information about Certificates on behalf of a CA.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the Matter PKI.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing Certificates and providing access to them, in accordance with the CP governing the CA.
Compliance Audit (Audit)	A periodic audit that a CA system undergoes to determine its conformance with Matter PKI requirements that apply to it.
Compliance Auditor (Auditor)	The person, or company, performing the Compliance Audit.
Compromise	A violation of a Security Policy, in which an unauthorized disclosure of, or loss of control over, sensitive information has occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information that is not public knowledge.

Term	Description
Delegated Service Provider (DSP)	A provider of PKI services such as HSM and/or CA infrastructure to which a CA has delegated some of its operations.
Device Attestation Certificate (DAC)	Device specific Certificate used to attest the Vendor ID and Product ID of the device or commissionable software component.
Disaster Recovery Plan (DRP)	A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
Distinguished Name (DN)	Identification fields in a Certificate that are input by the CA when issuing Certificates. The information is obtained from the Requestor's naming application.
Hardware Security Module (HSM)	A physical computing device that safeguards and manages digital keys and performs cryptographic functions.
Intellectual Property Rights	Rights under one or more of the following: copyright, patent, trade secret, trademark, trade names, or any other intellectual property rights.
Key Generation Ceremony	A procedure whereby a CA's key pair is generated, its private key is backed up, and/or its public key is certified.
MAC Address	A media access control (MAC) address is an address that uniquely identifies each of a network interface.
Management Authority (MA)	An entity whose role is to provide trust management services to support the ecosystem in meeting its security goals using the Matter PKI.
Product Attestation Authority (PAA)	A Certificate Authority used to issue certificates for PAIs.
Product Attestation Intermediate (PAI)	An intermediate Certificate Authority used to directly issue Device Attestations Certificates (DAC).
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a CSR.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines private key file format.

Term	Description
PKCS #8	Public-Key Cryptography Standard #8, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
PKI Participant	An individual or organization that is one or more of the following within the Matter PKI: the Connectivity Standards Alliance, a CA, a Requestor, or a Relying Party.
Signing System	A Signing System is a system that has direct access to a CA's plaintext private keys, including software that interfaces with the hardware to perform the signing operations.
Policy Authority (also PKI-PA)	The entity that establishes Certificate Policies. Also known as the PKI Policy Authority (PKI-PA).
Processing Center	A secure facility created by an appropriate organization that houses, among other things, the cryptographic modules used for the issuance of Certificates.
Product Identifier (PID)	A 16-bit number that uniquely identifies a product of a vendor.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for administering Certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key Certificates.
Registration Authority (RA)	The entity that collects and verifies each Requestor's identity and the information that is to be entered the public key Certificate.
Relying Party	An entity that receives a Certificate with a digital signature verifiable with the public key listed in the Certificate and is able to assess the trust in the authentication information provided by the Certificate depending on the CP governing the PKI and the Certificate verification.
Requestor	The entity who requests a Certificate (e.g., a manufacturer). The Requestor can use, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Requestor Agreement Document (RAD)	An agreement used by the CA setting forth the terms and conditions under which an organization acts as a Requestor. The RAD contains the Certificate Application.

Term	Description
Secret Share	A portion of the activation data needed to operate the private key, held by individuals called “Shareholders.” A threshold number of Secret Shares (n) out of the total number of Secret Shares (m) SHALL be required to operate the private key.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key to enforce multi-person control over CA private key operations.
Security Policy	The highest-level document describing the Connectivity Standards Alliance’s security policies.
Shareholders	Holders of Secret Shares needed to operate a CA private key.
Subject	The holder of a private key corresponding to a public key. The term 'Subject' can, in the case of a Matter PKI Certificate, refer to a device. For example, for Matter end-entity device attestation certificates, this would be the device presenting the certificate.
Superior Entity	An entity above a certain entity within the Matter PKI.
Trusted Person	An employee, contractor, or consultant of an entity within the Matter PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.
Trusted Position	The positions within the Matter PKI entity that SHALL be held by a Trusted Person.
Trustworthy Systems	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable Security Policy.
Validity Period	The period starting with the date and time a Certificate is issued and ending with the date and time on which the Certificate expires.

Term	Description
Vendor Identifier (VID)	A 16-bit number that uniquely identifies a particular product manufacturer, vendor, or group thereof.

1.8.2. Acronyms

This CP uses the following abbreviations and acronyms:

Table 4. Acronyms

Term	Description
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRA	Certificate Requesting Account
CSR	Certificate Signing Request
CSS	Certificate Status Server
DCL	Distributed Compliance Ledger
DN	Distinguished Name
DRP	Disaster Recovery Plan
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
id-ce	Object Identifier for Version 3 Certificate extensions. (OID value: 2.5.29)
IETF	Internet Engineering Task Force
IP	Internet Protocol
iso	Independent System Operators
IT	Information Technology
MA	Management Authority
OID	Object Identifier
OU	Organizational Unit
PA	Policy Authority
PAA	Product Attestation Authority
PAI	Product Attestation Intermediate
PID	Product Identifier
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure

Term	Description
PKI-PA	Public Key Infrastructure Policy Authority
RA	Registration Authority
RAD	Requestor Agreement Document
RFC	Request for Comment
VID	Vendor Identifier

Chapter 2. Publication and Repository Responsibilities

2.1. Repositories

PAA Certificates will be published in the Distributed Compliance Ledger (DCL) as a repository.

2.2. Publication of Certification Information

This CP and CA Certificates SHALL be publicly available (e.g., on the Connectivity Standards Alliance website, see www.csa-iot.org). The CPS for the PAAs will not be published; a redacted version of the CPS MAY be publicly available upon request to the Matter PKI-PA. There is no requirement for the publication of CPSs of PAIs that issue Certificates under this CP. The CAs SHALL protect information not intended for public dissemination.

The Table below is a matrix of the various Matter PKI practice documents, showing whether they are publicly available, and their locations. The list is not intended to be exhaustive, nor will each document listed be applicable to every CA. Documents not expressly made public are confidential to preserve the security of the Matter PKI.

Table 5. Availability of Matter PKI Information

Item	Classification	Available From:
Matter PKI CP	Public	Connectivity Standards Alliance [6]
PAA Certificates	Public	Connectivity Standards Alliance [6]
PAI Certificates	(Optional) Public	Connectivity Standards Alliance [6]
PAA CPSs	Confidential	N/A
PAI CPSs	Confidential	N/A

2.3. Time or Frequency of Publication

Changes to this CP SHALL be made publicly available within thirty (30) days of approval by the PKI-PA.

PAA Certificates SHALL be made publicly available (through the DCL) at the time of submission of a request for inclusion in the Matter PKI.

2.4. Access Controls on Repositories

The CAs SHALL implement controls to prevent unauthorized addition, deletion, or modification of repository entries.

Chapter 3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

For Certificates issued under this CP, the CA SHALL assign X.501 Distinguished Names (DNs) [2] . The Issuer and Subject DN fields in Certificates SHALL be populated with a non-empty DN as described in PAA/PAI section of the Matter Specification section 6.1.2.1:

3.1.2. Need for Names to Be Meaningful

The Certificates issued pursuant to this CP are meaningful if the names that appear in the Certificates can be understood by the Relying Parties. Names used in the Certificates SHALL identify the object to which they are assigned in a meaningful way.

Requestor Certificates for PAA and PAI SHALL contain meaningful names that represent the Requestor in a way that is easily understandable for humans. For DACs, there is no such requirement.

The Subject name in CA Certificates SHALL match the issuer name in Certificates issued by the CA, as required by RFC 5280 [3] .

3.1.3. Anonymity or Pseudonymity of Requestors

Matter PKI CAs SHALL NOT issue anonymous or pseudonymous Certificates.

3.1.4. Rules for Interpreting Various Name Forms

Rules for interpreting DN forms are specified in X.501 [2] .

3.1.5. Uniqueness of Names

Each CA and RA SHALL enforce the uniqueness of subject names within the scope of the issuing CA. Multiple Certificates with the same subject name MAY be issued to the same Requestor. Name uniqueness is enforced for the entire Subject DN of the Certificate rather than an attribute (e.g., the common name). Each CA and RA SHALL identify the method for checking uniqueness of the Subject DNs within its domain.

3.1.6. Recognition, Authentication, and Role of Trademarks

Certificate Applicants SHALL NOT use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. Neither the Connectivity Standards Alliance, the PKI-PA, nor any Connectivity Standards Alliance CA/RA are required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any Intellectual Property Rights, including, without limitation, rights in a domain name, trade name, trademark, or

service mark; and the Connectivity Standards Alliance, the PKI-PA, and any Matter PKI CA SHALL be entitled, without liability to any Certificate Applicant, to reject or suspend any RAD because of such dispute. The PKI-PA SHALL resolve disputes involving names and trademarks.

3.2. Initial Identity Validation

No stipulation.

3.2.1. Method to Prove Possession of Private Key

In all cases where the party named in a Certificate generates its own keys, that party SHALL be required to prove possession of the private key, which corresponds to the public key in the Certificate request. The CA SHALL prove that the Requestor possesses the private key by verifying the Requestor's digital signature on the PKCS #10 Certificate Signing Request (CSR) with the public key in the CSR.

When the key pair is generated by the CA on behalf of a Requestor; then in this case, proof of possession of the private key by the Requestor is not required.

The PKI-PA MAY approve other methods to prove possession of a private key by a Requestor.

3.2.2. Authentication of Organization Identity

The CA's Certificate issuance process SHALL authenticate the identity of the organization named in the RAD by confirming that the organization:

- Exists in a business database (e.g., Dun & Bradstreet), or alternatively, has organizational documentation issued by or filed with the applicable government (e.g., government issued business credentials) that confirms the existence of the organization, such as Articles of Incorporation, Certificate of Formation, Charter Documents, or a business license that allows it to conduct business;
- Conducts business at the address listed in the RAD; and
- Is a CSA and Matter WG member in good standing.

3.2.3. Authentication of Individual Identity

This CP allows a Certificate to be issued only to a single entity. Certificates that contain a public key whose associated private key is shared SHALL NOT be issued.

The CA/RA's Certificate issuance process SHALL authenticate the individual identity of the following:

- That the representative submitting the RAD and Certificate Application is a duly authorized representative of the organization as an employee, partner, member, agent, etc. and is authorized to act on behalf of the organization;
- That the corporate contact listed in the RAD is an officer in the organization and can act on behalf of the organization; and

- That the administrator listed in the RAD and Certificate Application is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization.

3.2.4. Non-verified Requestor Information

Non-verifiable information MAY be included in Matter PKI Certificates, such as:

- Organizational Unit (OU); or
- Any other information designated as non-verified in the Certificate.

3.2.5. Validation of Authority

The CA's Certificate issuance process SHALL confirm that the:

- Corporate contact listed in the RAD is an officer in the organization who can sign on behalf of the organization and bind the organization to the terms and conditions of the agreement;
- Representative submitting the RAD and Certificate Application is authorized to act on behalf of the organization;
- Administrators listed in the RAD are authorized to act on behalf of the organization; and
- Contacts listed in the RAD are authorized to act on behalf of the organization.

3.2.6. Criteria for Inter-operation

No stipulation.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-key

CA Certificate re-key requests SHALL follow the same procedures as initial CA Certificate issuance.

3.3.2. Identification and Authentication for Re-key After Revocation

No stipulation.

3.4. Identification and Authentication for Revocation Request

No stipulation.

Chapter 4. Certificate Lifecycle Operational Requirements

4.1. Certificate Application

A CA SHALL include the processes, procedures, and requirements of its Certificate issuance process in its CPS.

4.1.1. Certificate Application Submitters

Only Requestors who are authorized by the Connectivity Standards Alliance to receive Matter PKI Certificates MAY submit a Certificate Application. A Certificate Application for a CA Certificate SHALL be submitted by an authorized representative of the Requestor. A Certificate Applicant for a Certificate SHALL be the Requestor or an authorized representative of the Requestor.

4.1.2. Enrollment Process and Responsibilities

All communications among CAs/RAs supporting the Certificate Application and issuance process SHALL be authenticated and protected from modification; any electronic transmission of shared secrets SHALL be protected. Communications MAY be electronic or out-of-band and SHALL protect the confidentiality and integrity of the data.

The enrollment process for a Certificate Applicant SHALL consist of:

- Completing a RAD and Certificate Application;
- Providing the requested information;
- Responding to authentication requests in a timely manner; and
- Submitting required payment.

4.2. Certificate Application Processing

It is the responsibility of the CA/RA to verify that the information in a Certificate Application is accurate.

4.2.1. Performing Identification and Authentication Functions

Prior to Certificate issuance, a Requestor SHALL sign a RAD detailing Requestor responsibility, which includes the requirement that the Requestor SHALL protect the private keys and use the Certificates and private keys for authorized purposes only.

4.2.2. Approval of Certificate Applications

A CA/RA SHALL approve a Certificate Application if all the following criteria are met:

- Receipt of a fully executed RAD;

- Receipt of a signed Certificate Application;
- Successful identification and authentication of all required information;
- Receipt of all requested supporting documentation;
- Payment (if applicable) has been received;
- Acceptance of the certificate application would not cause a violation of the CPS or the CP; and
- The CA approves the Certificate Application.

4.2.3. Time to Process Certificate Applications

This SHALL be negotiated in the RAD (Requestor Agreement Document) between the vendor and the CA.

4.3. Certificate Issuance

Upon receiving a request for a Certificate, the CA/RA SHALL verify that the information in the Certificate Application is correct and accurate.

4.3.1. CA Actions During Certificate Issuance

Upon receiving the request, the CAs SHALL:

- Verify the identity of the requestor;
- Verify the authority of the requestor and the integrity of the information in the Certificate request; and
- Create and sign a Certificate if all Certificate requirements have been met.

Information received from a prospective Requestor SHALL be verified before inclusion in a Certificate.

4.3.2. Notification to Requestor by the CA of Issuance of Certificates

CAs SHALL notify Requestors that they have created the requested CA Certificate(s) and provide Requestors with access to the CA Certificate(s) by notifying them that their CA Certificate(s) are available and the means for obtaining them. CA Certificates SHALL be made available to Requestors, either via download from a website or via a message sent to the Requestor containing the Certificates or through a standardized protocol for automating certificate issuance.

4.4. Certificate Acceptance

Certificates will be deemed valid immediately after issuance.

4.4.1. Conduct Constituting Certificate Acceptance

The following conduct constitutes Certificate acceptance by the Requestor:

- Transferring a Certificate; and

- Failure to object to the Certificate or its content within five (5) business days after transfer.

Note: Completing the transfer of a Certificate constitutes Certificate acceptance by the Requestor wherever automated issuance processes are used.

4.4.2. Publication of the Certificate by the CA

PAA Certificates SHALL be published in a publicly available repository.

This CP makes no stipulation regarding publication of Requestor Certificates.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.5. Key Pair and Certificate Usage

4.5.1. Requestor Private Key and Certificate Usage

Requestor private key usage SHALL be specified through Certificate extensions, including the key usage, and extended key usage extensions, in the associated Certificate. PAIs SHALL protect their private keys from unauthorized use and SHALL discontinue use of the private key following expiration, or key compromise. PAI private keys that have not been Compromised MAY be used for new certificates for the same device.

Certificate use SHALL be consistent with the *keyUsage* field extensions included in the Certificate.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties SHOULD assess:

- The restrictions on key and Certificate usage specified in critical Certificate extensions, including the *basicConstraints* and *keyUsage* extensions.

Relying Parties acknowledge the following:

- They are solely responsible for deciding whether to rely on the information in a Certificate and agree that they have enough information to make an informed decision.
- To the extent permitted by applicable law, the Connectivity Standards Alliance hereby disclaims all warranties regarding the use of any Certificates, including, but not limited to, any warranty of merchantability or fitness for a purpose. In addition, the Connectivity Standards Alliance hereby limits its liability, and excludes all liability for indirect, special, incidental, and consequential damages.
- That reliance on Certificates is restricted to the purposes for which those Certificates were issued.

4.6. Certificate Renewal

No stipulation.

All certificate issuance, including re-issuing certificates intended for the same devices but with different keys, lifetimes or other fields, is subject to the same requirements described in this document.

4.7. Certificate Re-key

No stipulation.

All certificate issuance, including re-issuing certificates intended for the same devices but with different keys, lifetimes or other fields, is subject to the same requirements described in this document.

4.8. Certificate Modification

No stipulation.

All certificate issuance, including re-issuing certificates intended for the same devices but with different keys, lifetimes or other fields, is subject to the same requirements described in this document.

4.9. Certificate Revocation and Suspension

No stipulation.

4.10. Certificate Status Services

No stipulation.

4.10.1. Operational Characteristics

No stipulation.

4.10.2. Service Availability

Relying Parties are bound to their obligations and the stipulations of this CP irrespective of the availability of the Certificate status service.

4.10.3. Optional Features

No stipulation.

4.11. Key Escrow and Recovery

4.11.1. Key Escrow and Recovery Policy and Practices

No stipulation.

4.11.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

Chapter 5. Facility, Management, and Operational Controls

All entities performing CA functions implement and enforce the following physical, procedural, logical, and personnel security controls for a CA.

Some of the measures described in this chapter need consideration in case of a CA which is (partly) implemented in a cloud-based environment suitable for secure cryptographic operations, typically hosted by a party independent from the CA and providing such services. In this case, the CA needs to rely on the Delegated Service Provider (DSP) to implement the measures in this CP.

When the term "CA" is used in this chapter, it denotes the combination of the CA and any contracted provider as appropriate with the division of functions.

5.1. Physical Controls

CA equipment SHALL be protected from unauthorized access while the cryptographic module is installed and activated. The CA SHALL implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens SHALL be protected against theft, loss, and unauthorized use.

All physical control requirements specified below apply equally to the Matter PKI CAs and any workstations or systems used to administer the CAs, except where specifically noted. For the case of a CA using a cloud-based environment, the administration and operation of the cloud components SHALL be performed from a secure workstation and over secure connections that enforce the access controls, confidentiality and integrity of the CA. Monitoring of the cloud components (e.g. from the CA’s own site to the cloud-based environment) when using a non-administration account SHOULD be performed from secure workstations or systems and over secure connections. Administration and operation of cloud components SHALL NOT be possible using this account.

5.1.1. Site Location and Construction

All CA operations SHALL be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. The site location and construction, when combined with other physical security protection mechanisms such as security locks and intrusion sensors, SHALL provide robust protection against unauthorized access to the CA equipment and records.

Such requirements are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door, a closed gate, or an alarm system that provides mandatory access control for individuals and requires a positive response (e.g., door unlocks, gate opens, or alarm system is disarmed) for everyone to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access.

5.1.2. Physical Access

Access to each tier of physical security SHALL be auditable and controlled so that only authorized

personnel can access each tier.

CAs SHALL control access to their facilities including:

- Minimizing exposure of privileged functions through definition of function-specific roles or authorization groups;
- Access control enforcement of these roles or groups;
- Use of proximity card identification badges;
- Logging of access into and out of the facility;
- Automated notification to outside alarm monitoring agency of a potential security breach to the facility; and
- Video surveillance.

At a minimum, the physical access controls for CA equipment SHALL:

- Ensure that no unauthorized access to the hardware is permitted;
- Ensure that all removable media and paper containing sensitive plaintext information is stored in secure containers;
- Ensure an access log is maintained and inspected periodically; and
- Require at least two-person physical access control to both the cryptographic module and computer systems.

When not attached, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment SHALL be placed in secure containers. Activation data SHALL be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and SHALL NOT be stored with the cryptographic module or removable hardware associated with workstations used to administer the CA.

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs SHALL occur if the facility is to be left unattended. At a minimum, the check SHALL verify the following:

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

For the case of a CA with a cloud-based environment which use local equipment at the CA's own site for administration and operation of the cloud components, such equipment SHALL be secured using up-to-date software controls (like anti-virus, secure boot, etc.) and checked for physical tampering. When not in use, such equipment SHOULD be kept in a physically secure facility to prevent change to software components or against physical tampering. Equipment which can only be used to monitor the CA operation for daily management (but not influence it) MAY be excluded

from this requirement.

5.1.2.1. RA Equipment Physical Access

RA equipment SHALL be protected from unauthorized access. The RA SHALL implement physical access controls to reduce the risk of equipment tampering. These security mechanisms SHALL be commensurate with the level of threat in the RA equipment environment.

5.1.3. Power and Air Conditioning

CA facilities when in use SHALL be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these facilities when in use SHALL be equipped with the appropriate system to control temperature and ventilation as needed.

The CA SHALL have backup capability enough to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

5.1.4. Water Exposures

CA facilities SHALL be constructed, equipped, and installed, and procedures SHALL be implemented to prevent CA equipment to damaging exposure to water when in use. Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5. Fire Prevention and Protection

CA facilities SHALL be constructed and equipped, and procedures SHALL be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures SHALL meet all local applicable safety regulations.

5.1.6. Media Storage

CAs SHALL protect the media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and SHALL use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

5.1.7. Waste Disposal

CAs SHALL implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

CA media and documentation that are no longer needed for operations SHALL be destroyed in a secure manner. For example, paper documentation SHALL be shredded, burned, or otherwise rendered unrecoverable.

5.1.8. Off-site Backup

CAs SHALL maintain backups of critical system data or any other sensitive information, including Audit data, in a secure off-site facility. Full system backups enough to recover from system failure SHALL be made on a periodic schedule. At least one full backup copy SHALL be stored at an off-site location (separate from CA equipment). Only the latest full backup needs to be retained. The backup SHALL be stored at a site with a minimum of three (3) physical and procedural controls. When the backup is stored in encrypted form, the corresponding backup decryption keys and/or devices with the physical and procedural controls SHALL commensurate to that of the operational CA. The site for storage of the corresponding decryption keys and/or devices MAY be at a different location from the location of the backups. If the backup is not encrypted, then the data SHALL be stored and protected at a site with physical and procedural controls commensurate to that of the operation CA.

5.2. Procedural Controls

Procedural controls are requirements on roles that perform functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles SHALL be extraordinarily responsible, or the integrity of the CA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. 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.

5.2.1. Trusted Roles

Employees, contractors, and consultants that are designated to manage the CA's trustworthiness SHALL be "Trusted Persons" serving in "Trusted Positions".

CAs SHALL consider the categories of their personnel identified in this section as Trusted Persons having a Trusted Position. Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that MAY materially affect:

- The validation of information in Certificate Applications
- The acceptance, rejection, or other processing of Certificate Applications, renewal requests, or enrollment information
- The issuance including (in the case of Processing Centers) personnel having access to restricted portions of its repository
- The handling of Requestor information or requests

Trusted Persons include, but are not limited to, customer service personnel, CA system administrators, designated engineering personnel, CA operators, Compliance Auditors (Auditors), and executives that are designated to manage infrastructural trustworthiness.

5.2.2. Number of Persons Required per Task

Multiparty control procedures are designed to ensure that at a minimum, two parties are required to have either physical or logical access to the CA. Access to CA cryptographic hardware (e.g. HSM,

security USB storage) SHALL be strictly enforced by multiparty access throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a CA cryptographic hardware is activated with operational keys, further access controls SHALL be invoked to maintain split control over both physical and logical access to the device.

Two or more persons are required for the following tasks:

- Access to CA cryptographic hardware;
- Management of CA cryptographic hardware;
- CA key generation;
- CA signing key activation;
- CA private key backup; and
- CA Certificate renewal.

Multiparty control SHALL NOT be achieved using personnel that serve in the Auditor trusted role. CAs SHALL establish, maintain, and enforce control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Other manual operations, such as the validation and issuance of Certificates not issued by an automated validation and issuance system, require the participation of at least two Trusted Persons, or a combination of at least one Trusted Person and an automated validation and issuance process. Manual operations for key recovery MAY optionally require the validation of two authorized administrators.

In cases where the plaintext CA private key is only used in hardware operated by a Delegated Service Provider (DSP), lifecycle and maintenance tasks performed by the DSP using that key MAY be done without involvement of the PKI administrators.

5.2.3. Identification and Authentication for Each Role

CAs SHALL confirm the identity and authorization of all personnel seeking to become Trusted Persons before such personnel are:

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

Authentication of identity SHALL include the personal (physical) presence of such personnel before human resources or other personnel performing security functions and a check of well-recognized forms of identification, such as passports and driver’s licenses.

5.2.4. Roles Requiring Separation of Duties

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

- Acceptance, rejection, or other processing of Certificate Applications, key recovery requests or renewal requests, or enrollment information

- Issuance of Certificates including personnel having access to restricted portions of the repository
- Generation, issuance, or destruction of a CA Certificate and loading of a CA to a production environment

Individuals SHALL NOT have more than one trusted role. The CA SHALL have in place procedures to identify and authenticate its users and SHALL ensure that no user identity can assume multiple roles.

For the case of a PAA which is only providing services to one vendor ID (VID-scoped PAA), individuals MAY have more than one trusted role, as long as the multi-party control requirements are respected.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

CAs SHALL require that personnel assigned to trusted roles have the requisite background, qualifications, and experience or be provided the training needed to perform their prospective job responsibilities competently and satisfactorily.

5.3.2. Background Check Procedures

CAs SHALL conduct background check procedures for personnel tasked to become Trusted Persons. These procedures SHALL align with any limitations on background checks imposed by local law and company policies, and be proportional to the Trusted Role(s) they will perform. To the extent one of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law, the investigating entity SHALL utilize a substitute investigative technique permitted by law that provides substantially similar information, including, but not limited to, obtaining a background check performed by an applicable agency. Background investigations MAY include:

- Confirmation of previous employment;
- Check of one or more professional references;
- Confirmation of the highest or most relevant educational degree obtained;
- Search of criminal records (local, state, or provincial, and national);
- Check of credit/financial records; or
- Search of driver’s license records.

Factors revealed in a background check that MAY be considered grounds for rejecting candidates for Trusted Positions or for acting against an existing Trusted Person MAY include, but are not limited to, the following:

- Misrepresentations made by the candidate or Trusted Person;
- Highly unfavorable or unreliable personal references;
- Certain criminal convictions, including related to acts of violence, fraud, false statements or

omissions, wrongful taking of property, bribery, perjury, forgery, counterfeiting, and/or extortion; and

- Indications of a lack of financial responsibility.

5.3.3. Training Requirements

CAs SHALL ensure their personnel have the skills and qualifications and access to on-the-job training needed for their personnel to perform their job responsibilities relating to CA operations competently and satisfactorily. They SHALL also periodically review their training programs, and their training SHALL address the elements relevant to functions performed by their personnel.

Training programs SHALL address the elements relevant to the environment of the person being trained, including, without limitation:

- Security principles and mechanisms of the CA and its environment;
- Hardware and software versions in use;
- All duties the person is expected to perform;
- Incident and Compromise reporting and handling;
- Disaster recovery and business continuity procedures; and
- The stipulations of this CP.

5.3.4. Retraining Frequency and Requirements

CAs SHALL provide refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

All individuals responsible for PKI trusted roles SHALL be made aware of changes in the CA/RA 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/RA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

CAs SHALL establish, maintain, and enforce policies for the discipline of personnel following unauthorized actions. Disciplinary actions MAY include measures up to and including termination and SHALL be commensurate with the frequency and severity of the unauthorized actions.

5.3.7. Independent Contractor Requirements

CAs MAY permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly defined outsourcing relationships. CAs SHOULD only use contractors or consultants as Trusted Persons if the CA does not have suitable employees available

to fill the roles of Trusted Persons. Accordingly, independent contractors and consultants SHALL be escorted and directly supervised by Trusted Persons when they are given access to the CA and its secure facility.

Contractors fulfilling trusted roles SHALL follow all personnel requirements stipulated in this CP and SHALL establish procedures to ensure that any subcontractors perform in accordance with this CP.

5.3.8. Documentation Supplied to Personnel

CAs SHALL give their personnel the requisite training and documentation needed to perform their job responsibilities competently and satisfactorily.

5.4. Audit Logging Procedures

Audit log files SHALL be generated for all events relating to the security of the CA, RA, and Certificate Status Server (CSS). Where possible, the Audit logs SHALL be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism SHALL be used. All Audit logs, both electronic and non-electronic, SHALL be retained in accordance with Section Retention Period for Audit Logs and made available during Audits.

For the case of a CA using a cloud-based environment, the audit logging of the cloud components by the CA are limited to the APIs available from the cloud provider and any additional audit logging requirements SHALL be met by the cloud providers certified audit logging procedures.

5.4.1. Types of Events Recorded

All auditing capabilities of the CA, RA and CSS operating systems and applications SHALL be enabled during installation. All Audit logs, whether recorded automatically or manually, SHALL contain the date and time, the type of event, and the identity of the entity that caused the event.

CAs/RAs SHALL record in Audit log files all events relating to the security of the CA/RA system, including, without limitation (see Archive Event Types for additional reference):

- Physical Access/Site Security:
  - Personnel access to facility housing CA/RA
  - Access to the CA/RA server
  - Known or suspected violations of physical security
- CA/RA Configuration Management (see normative note 1 below for additional details):
  - CA/RA hardware configuration baseline
  - Approvals for installation of the operating system
  - Approvals for installation of the CA/RA software
  - Approvals for system configuration changes and maintenance
  - Approvals for installation of hardware cryptographic modules
  - Cryptographic module lifecycle management-related events (e.g., receipt, use, de-

installation, and retirement)
    - Anytime cryptographic keys are accessed directly in plaintext or exported
- Account Administration:
    - System administrator accounts
    - Roles and users added to or deleted from the CA/RA system
    - Access control privileges of user accounts
    - Attempts to create, remove, set passwords, or change the system privileges of the privileged users (trusted roles)
    - Attempts to delete or modify Audit logs
    - Changes to the value of maximum authentication attempts
    - Resetting operating system clock
- CA Operational events:
    - Key generation
    - Start-up and shutdown of CA systems and applications
    - Changes to CA details or keys
    - Records of the destruction of media containing key material, activation data, or personal Requestor information
- Certificate lifecycle events:
    - Issuance
    - Re-key
- Backup to store off-site material
    - Trusted Person events (see normative note 2 below for additional details):
- Logon and logoff
- Attempts to create, remove, set passwords, or change the system privileges of the privileged users
- Unauthorized attempts to access the CA/RA system
- Unauthorized attempts to access system files
- Failed read and write operations on the Certificate
- Personnel changes at the CA/RA related to trusted administrative roles

Regarding the above list, the following notes apply:

- Normative note 1: audit logs for CA/RA Configuration Management events SHALL be required for PKI Participants in the scope of running their CA. A Delegated Service Provider MAY keep such logs for their own records, but sharing those records is not required for the CA to be compliant with this policy.
- Normative note 2: audit logs for Trusted Person Events SHALL be required for PKI Participants and their own personnel. A Delegated Service Provider MAY keep such logs for their own

records, but sharing those records is not required for the CA to be compliant with this policy.

5.4.2. Frequency of Processing Log

CAs/RAs/CSSs SHALL review their Audit logs in response to alerts based on irregularities and incidents within their systems. CA/RA/CSSs SHALL review the Audit logs at least once every three (3) months and SHALL compare their Audit logs with supporting manual and electronic logs when any action is deemed suspicious.

Audit log processing SHALL consist of a review of the Audit logs and documenting the reason for all significant events in an Audit log summary. Audit log reviews SHALL include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on Audit log reviews SHALL be documented.

5.4.3. Retention Period for Audit Log

Audit logs SHALL be retained for at least five (5) years. Audit logs SHALL be retained for frequent access at least two (2) months after processing and thereafter MAY be archived. The individual who removes Audit logs from the CA/RA/CSS system SHALL be different from the individuals who, in combination, command the CA signature key.

5.4.4. Protection of Audit Log

Audit logs SHALL be protected from unauthorized viewing, modification, deletion, or other tampering. CA/RA/CSS system configuration and procedures SHALL be implemented together to ensure that only authorized people archive or delete security Audit data. Procedures SHALL be implemented to protect archived data from deletion or destruction before the end of the security Audit data retention period.

5.4.5. Audit Log Backup Procedures

Incremental backups of Audit logs SHALL be created frequently, at least monthly.

5.4.6. Audit Collection System (Internal vs. External)

The Audit log collection system MAY or MAY NOT be external to the CA/RA/CSS system. Automated Audit processes SHALL be invoked at system or application activation 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.

Whenever a Delegated Service Provider is used, the CA/RA SHALL collect and store all logs related to certificate issuance or signing operations directly delegated to the DSP, such that there are no more than five (5) business days of delay between an operation being directly delegated to the DSP, and the audit logs of that operation being captured. It is RECOMMENDED that audit logs be gathered in real time as requests are made to a DSP.

5.4.7. Notification to Event-Causing Subject

Where an event is logged by the Audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8. Vulnerability Assessments

The CA/RA/CSS SHALL perform routine self-assessments of security controls for vulnerabilities. Events in the Audit process are logged, in part, to monitor system vulnerabilities. The assessments SHALL be performed following an examination of these monitored events. The assessments SHALL be based on real-time automated logging data and SHALL be performed at least on an annual basis as input into an entity's annual Audit.

The Audit data SHOULD be reviewed by the Auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Auditors SHOULD check for continuity of the Audit data.

5.5. Records Archival

CA/RA/CSS archive records SHALL be sufficiently detailed to determine the proper operation of the PKI and the validity of any Certificate (including those that are expired) issued by the CA. Records MAY be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate, reliable, and complete.

5.5.1. Types of Events Archived

Matter PKI CA/RA/CSS records SHALL include all relevant evidence in the recording entity's possession, including, without limitation (see Recorded Types for additional reference):

- Time stamps;
- CP;
- CPS;
- Contractual obligations and other agreements concerning operations of the CA/RA/CSS system and equipment configuration;
- Modifications and updates to system or configuration;
- Certificate request documentation;
- Records of all actions taken on Certificates issued and/or published;
- Record of re-key;
- Audit reports;
- Appointment of an individual to a Trusted Position;
- Destruction of cryptographic modules; and
- All Certificate Compromise notifications.

Matter PKI-PA records SHALL include all relevant evidence in the recording entity's possession,

including, without limitation:

- RAD(s);
- Audit reports;
- Destruction of cryptographic modules; and
- All Certificate Compromise notifications.

5.5.2. Retention Period for Archive

Archive records SHALL be kept for a minimum of five (5) years without any loss of data.

5.5.3. Protection of Archive

An entity maintaining an archive of records SHALL protect the archive so that only the entity's authorized Trusted Persons are able to obtain access to the archive. The archive SHALL be protected against unauthorized viewing, modification, deletion, or other tampering. The archive media and the applications required to process the archive data SHALL be maintained to ensure that the archive data can be accessed for the retention time.

5.5.4. Archive Backup Procedures

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

5.5.5. Requirements for Time-Stamping of Records

CA archive records SHALL be automatically time-stamped as they are created. System clocks used for time-stamping SHALL be checked with an alternative authoritative time standard.

5.5.6. Archive Collection Systems (Internal or External)

Archive data MAY be collected in any expedient manner.

5.5.7. Procedures to Obtain and Verify Archive Information

Only authorized Trusted Persons can obtain access to the archive. The integrity of the information is verified as usable when it is restored.

5.6. Key Changeover

To minimize risk from Compromise of a CA's private signing key, that key MAY be changed as required. From that time on, the CA will only use the new key to sign Certificates.

A CA Certificate MAY be renewed if the CA's Superior Entity reconfirms the identity of the CA. Following such reconfirmation, the Superior Entity SHALL either approve or reject the Certificate Application.

When a CA updates its private signature key and thus generates a new public key, the CA SHALL notify all CAs and Requestors that rely on the CA's Certificate that it has been changed.

When a CA that distributes self-signed Certificates updates its private signature key, the CA SHALL generate key rollover Certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued Certificates without distribution of the new self-signed Certificate to current users. Key rollover Certificates are optional for CAs that do not distribute self-signed Certificates.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

The PKI-PA SHALL be notified if any CA/CSSs operating under this CP experience the following:

- Suspected or detected Compromise of the CA/CSS systems;
- Physical penetration of the site housing the CA/CSS systems; or
- Successful denial of service attacks on CA/CSS components.

The PKI-PA will take appropriate steps to protect the integrity of the Matter PKI.

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

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

When computing resources, software, and/or data are corrupted, CA/CSSs operating under this CP SHALL respond as follows:

- Ensure that the system's integrity has been restored before returning to operation;
- If the CA or CSS signature keys are not destroyed, CA/CSS operations SHALL be re-established;
- If the CA or CSS signature keys are destroyed, CA/CSS operations SHALL be re-established as quickly as possible, giving priority to the generation of a new CA key pair;
- The PKI-PA SHALL be notified as soon as possible; and
- A report of the incident and a response to the event, SHALL be promptly made by the affected CA/CSS in accordance with the documented incident and Compromise reporting and handling procedures in the applicable CPS.

5.7.3. Entity (CA) Private Key Compromise Procedures

In the event of a CA private key Compromise, the following operations SHALL be performed:

- The PKI-PA SHALL be immediately informed, as well as any entities known to be distributing the CA Certificate;
- The CA SHALL generate new keys;
- The CA SHALL initiate procedures to notify Requestors of the Compromise; and

- Requestor Certificates MAY be renewed automatically by the CA under the new key pair, or the CA MAY require Requestors to repeat the initial Certificate Application process.

If the CA distributed the public key in a Certificate, the CA SHALL perform the following operations:

- Generate a new Certificate;
- Securely distribute the new Certificate; and
- Initiate procedures to notify Requestors of the Compromise.

If a CSS key is compromised the CSS will generate a new key pair and request new Certificate(s), if applicable.

If RA signature keys are Compromised, lost, or suspected of Compromise:

- A new RA key pair SHALL be generated in accordance with procedures set forth in the applicable CPS;
- A new RA Certificate SHALL be requested in accordance with the initial Certificate Application process described in this CP; and
- All Certificate Application requests approved by the RA since the date of the suspected Compromise SHALL be reviewed to determine which are legitimate.

5.7.4. Business Continuity Capabilities After a Disaster

Entities operating CAs SHALL develop, test, and maintain a Disaster Recovery Plan (DRP) designed to mitigate the effects of any kind of natural or man-made disaster. The DRP SHALL identify conditions for activating the recovery and what constitutes an acceptable system outage and recovery time for the restoration of information systems services and key business functions within a defined recovery time. Such conditions will likely be different between a PAA providing services to multiple companies versus a PAA only providing services to one vendor ID (VID-scoped PAA), where PAA operations might be infrequent and thus disaster recovery focuses on PAI(s).

Additionally, the DRP SHALL include:

- Frequency for taking backup copies of essential business information and software;
- Requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
- Separation distance of the disaster recovery site to the CA's main site; and
- Procedures for securing the disaster facility during the period following a disaster and prior to restoring a secure environment either at the original or a remote site.

The DRP SHALL include administrative requirements including:

- Maintenance schedule for the DRP;
- Awareness and education requirements;
- Responsibilities of the individuals; and
- Regular testing of contingency plans.

CAs SHALL have the capability of restoring or recovering essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance.

The disaster recovery equipment SHALL have physical security protections comparable to the production CA system, which includes the enforcement of physical security tiers.

A CA's DRP SHALL make provisions for full recovery within one (1) week following a disaster at the primary site.

5.8. CA and RA Termination

Prior to CA termination, the CA SHALL provide archived data to an archive facility, as specified in the CPS (if applicable). As soon as possible, the CA will make commercially reasonable efforts to inform its Subscribers and PKI-PA of the termination, using an agreed-upon method of communication.

The termination of a CA SHALL be according to the contract between the terminating CA and its Superior Entity. A terminating CA and its Superior Entity SHALL, in good faith, use commercially reasonable effort to agree on a termination plan that minimizes disruption to Requestors and Relying Parties. The termination plan SHALL cover the destruction of the CA's private signing keys related to the PAA(a) and/or PAI(s) being terminated. The termination plan MAY cover further issues such as:

- Providing notice to parties affected by the termination, such as Requestors and Relying Parties;
- Who bears the cost of such notice, the terminating CA, or the Superior Entity;
- The preservation of the CA's archives and records for the time periods;
- The continuation of Requestor and customer support services;
- Disposition of the CA's private key and the hardware token containing such private key; or
- Provisions needed for the transition of the CA's services to a successor CA.

In addition, the RA:

- SHALL archive all Audit logs and other records prior to termination;
- SHALL destroy all its private keys upon termination; and
- SHALL transfer all archive records to an appropriate authority such as the PKI-PA.

Chapter 6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1.1. CA Key Pair Generation

PAA key pair generation SHALL be performed using FIPS 140-3 Level 3 [4] or Common Criteria (EAL 4+) validated cryptographic modules and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys.

PAI key pair generation SHALL be performed using FIPS 140-3 Level 2 [4] or Common Criteria (EAL 4+) validated cryptographic modules.

New CA keys SHALL be generated in a Key Generation Ceremony using multi-person control for CA key pair generation.

CA key pair generation SHALL create a verifiable Audit trail documenting that the security requirements for procedures were followed. The documentation of the procedure SHALL be detailed enough to show that appropriate role separation was used. An independent third party SHALL validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.1.2. Requestor Key Pair Generation

Requestor key pair generation MAY be performed by the Requestor or CA. If the Requestors themselves generate private keys, then private key delivery to a Requestor is unnecessary.

When CA/RAs generate key pairs on behalf of the Requestor, then the private key SHALL be delivered securely to the Requestor. Private keys MAY be delivered electronically or on a hardware cryptographic module. In all cases, the following requirements SHALL be met:

- The CA SHALL NOT retain any copy of the key for more than two weeks after delivery of the private key to the Requestor.
- CAs SHALL use Trustworthy Systems to deliver private keys to Requestors and SHALL secure such delivery using a PKCS #8 or PKCS #12 package or, in the CA's sole discretion, a comparably equivalent means of encryption to prevent the loss, disclosure, modification, or unauthorized use of such private keys.
- Where key pairs are pre-generated on hardware tokens, the entities distributing such tokens SHALL use best efforts to provide physical security of the tokens to prevent the loss, disclosure, modification, or unauthorized use of the private keys on the token. The CA SHALL maintain a record of the Requestor acknowledgement of receipt of the token.
- The Requestor SHALL acknowledge receipt of the private key(s).
- Delivery SHALL be accomplished in a way that ensures that the correct tokens and activation

data are provided to the correct Requestors.

- For hardware modules, accountability for the location and state of the module SHALL be maintained until the Requestor accepts possession of it.
- For electronic delivery of private keys, the key material SHALL be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data SHALL be delivered using a separate secure channel.
- The CA/RA SHALL maintain a record of the Requestor's acknowledgement of receipt of the token.

6.1.2. Private Key Delivery to Requestor

The Requestors themselves typically generate Requestors' private keys, and therefore private key delivery to a Requestor is usually unnecessary. Private keys, however, generated by the CA for the Requestor SHALL be delivered to Requestors only when:

- Their Certificate Applications are approved by the PKI-PA; and
- Their key pairs are generated and are distributed to Certificate Applicants in connection with the enrollment process.

CAs SHALL use Trustworthy Systems to deliver private keys to Requestors and SHALL secure such delivery using a PKCS #8 or PKCS #12 package or, in the CA's sole discretion, any other comparably equivalent means (e.g., encryption) to prevent the loss, disclosure, modification, or unauthorized use of such private keys. Where key pairs are pre-generated on hardware tokens, the entities distributing such tokens SHALL use best efforts to provide physical security to prevent the loss, disclosure, modification, or unauthorized use of the private keys on the tokens.

6.1.3. Public Key Delivery to Certificate Issuer

Where key pairs are generated by the Requestor or RA, the public key SHALL be transferred to the issuing CA to be certified; it SHALL be delivered through a mechanism validating the identity of the Requestor and ensuring that the public key has not been altered during transit, and that the Certificate Applicant possesses the private key corresponding to the transferred public key. The Certificate Applicant SHALL deliver the public key in a PKCS #10 CSR package or an equivalent method ensuring that the public key has not been altered during transit, and the Certificate Applicant possesses the private key corresponding to the transferred public key.

6.1.4. CA Public Key Delivery to Relying Parties

CA public key Certificates SHALL be delivered to Relying Parties in a fashion to preclude substitution attacks. Acceptable methods for Certificate delivery are:

- Distribution of CA Certificates through secure out-of-band mechanisms; or
- Downloading the CA Certificates from trusted websites (CA or PKI-PA website).

6.1.5. Key Sizes

Certificates issued under this CP SHALL use cryptographic primitives and associated key sizes as

defined in the mapping table in the Public Key Cryptography section of the Matter [6] specification.

6.1.6. Public Key Parameters Generation and Quality Checking

CSRs SHALL be reviewed to confirm that the public key meets the key sizes defined in CP section Key Sizes.

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

Certificates issued under this CP SHALL use the key usage extensions as specified in the Device Attestation section of the Matter Specification [6] .

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

Private keys within the Matter PKI SHALL be protected using Trustworthy Systems. Private key holders SHALL take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such private keys in accordance with this CP and contractual obligations specified in the appropriate RAD.

The relevant standard for cryptographic modules is FIPS 140-3 [4] or Common Criteria (EAL 4+).

PAAs SHALL perform all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-3 Level 3 [4] or Common Criteria (EAL 4+).

PAIs, RAs, and CSSs SHALL perform cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-3 Level 2 [4] or Common Criteria (EAL 4+).

Requestors SHOULD perform cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-3 Level 1 [4] or Common Criteria (EAL 4+).

6.2.2. Private Key (n out of m) Multi-Person Control

Multi-person control is enforced to protect the activation data needed to activate CA private keys so that a single person SHALL NOT be permitted to activate or access any cryptographic module that contains the complete CA private signing key.

Multi-person controls MAY be done virtually over encrypted video and desktop sessions, or using a secure system which requires authenticated approvals from multiple people and includes an audit trail of all such transactions.

Plaintext CA private keys SHALL be backed up only under multi-person control, unless the backup is performed entirely by automation without human involvement or access to plaintext CA private keys at any point in the process. Physical access by any personnel to CA private keys backed up for disaster recovery SHALL be under multi-person control. The names of the parties used for multi-person control SHALL be maintained on a list that SHALL be made available for inspection during

Audits.

CAs MAY use “Secret Sharing” to split the private key or activation data needed to operate the private key into separate parts called “Secret Shares” held by individuals called “Shareholders.” Some threshold number of Secret Shares (m) out of the total number of Secret Shares (n) SHALL be required to operate the private key. The minimum threshold number of shares (m) needed to sign a CA Certificate SHALL be three (3). The total number of shares (n) used SHALL be greater than the minimum threshold number of shares (m).

CAs MAY also use Secret Sharing to protect the activation data needed to activate private keys located at their respective disaster recovery sites. The minimum threshold number of shares (m) needed to sign a CA Certificate at a disaster recovery site SHALL be three (3). The total number of shares (n) used SHALL be greater than the minimum threshold number of shares (m).

6.2.3. Private Key Escrow

CA private signature keys and Requestor private signature keys SHALL NOT be escrowed.

If the CA retains Requestor private encryption keys for business continuity purposes, the CA SHALL escrow such Requestor private keys to protect them from unauthorized modification or disclosure through physical and cryptographic means.

6.2.4. Private Key Backup

CAs SHALL back up their private keys under the same multi-person control as the original signature key. The backups allow the CA to be able to recover from disasters and equipment malfunction. At least one copy of the private signature key SHALL be stored off-site. Private keys that are backed up SHALL be protected from unauthorized modification or disclosure through physical or cryptographic means. Backups, including all activation data needed to activate the cryptographic token containing the private key, SHALL be protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within the CA site, such as at a disaster recovery site or at another secure off-site facility, such as a bank safe. All copies of the CA private signature key SHALL be accounted for and protected in the same manner as the original.

Device private keys MAY be backed up or copied but SHALL be held under the control of the Requestor or other authorized administrator. Private keys that are backed up, SHALL NOT be stored in plaintext form and storage SHALL ensure security controls consistent with the Matter security specifications with which the device is compliant. Requestors MAY have the option of using enhanced private key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys.

CSS private keys MAY be backed up. If backed up, all copies SHALL be accounted for and protected in the same manner as the original.

6.2.5. Private Key Archival

CA private signature keys and Requestor private signature keys SHALL NOT be archived. If the CA retains Requestor private encryption keys for business continuity purposes, the CA SHALL archive

such Requestor private keys, in accordance with CP section 5.5.

6.2.6. Private Key Transfer into or from a Cryptographic Module

CA and CSS private keys MAY be exported from the cryptographic module only to perform CA/CSS key backup procedures, as described in CP section Private Key Backup. At no time SHALL the private key exist in plaintext outside the cryptographic module.

All other keys SHALL be generated by and in a cryptographic module. If a private key is to be transported from one cryptographic module to another, the private key SHALL be encrypted during transport; private keys SHALL never exist in plaintext form outside the cryptographic module boundary.

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

Entry of a private key into a cryptographic module SHALL use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

Processing Centers generating CA private keys on one hardware cryptographic module and transferring them into another, SHALL securely transfer such private keys into the second cryptographic module to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. Such transfers SHALL be limited to making backup copies of the private keys on tokens.

CAs pre-generating private keys and transferring them into a hardware token, for example transferring generated end-user Requestor private keys into a smart card, SHALL securely transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.2.7. Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140-3 [4] or Common Criteria (EAL 4+).

6.2.8. Method of Activating Private Keys

The following section is only applicable to CAs whose private key is stored on a device that requires explicit user activation and deactivation of the key using some secret data. Some platforms, such as certain HSM platforms, have no notion of cryptographic key activation. For such platforms, key activation SHALL NOT be required as long as the private key is protected from unauthorized access at all times.

All CA/RA/CSSs SHALL protect the activation data for their private keys against loss, theft, modification, disclosure, or unauthorized use.

CA administrators SHALL be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include, but are not limited to, passphrases, PINs, or biometrics. Entry of activation data SHALL be protected from disclosure (i.e., the data SHOULD not be displayed while it is entered).

For Certificates, the device MAY be configured to activate its private key, provided that appropriate physical and logical access controls are implemented for the device. The strength of the security controls SHALL be commensurate with the level of threat in the device's environment, and SHALL protect the device's hardware, software, private keys, and its activation data from Compromise.

6.2.8.1. CA Administrator Activation

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

- Use of a smart card, biometric access device, password or security of equivalent strength to authenticate the administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Microsoft Windows logon or screen saver password, or a network logon password; and
- Commercially reasonable measures for the physical protection of the administrator's workstation to prevent use of the workstation and its associated private key without the administrator's authorization.

6.2.8.2. Offline CA Private Keys

Once the CA system has been activated, a threshold number of Shareholders SHALL be required to supply their activation data to activate an offline CA's private key. Once the private key is activated, it SHALL be active until termination of the session.

6.2.8.3. Online CA Private Keys

An online CA's private key SHALL be activated by a threshold number of Shareholders supplying their activation data (stored on secure media). Once the private key is activated, the private key MAY be active for an indefinite period until it is deactivated when the CA goes offline.

6.2.8.4. Requestor Private Keys

The PAA standards for protecting activation data for Requestors' private keys SHALL be in accordance with the specific obligations appearing in the applicable agreement executed between the PAA and the Requestor.

6.2.9. Method of Deactivating Private Keys

Cryptographic modules that have been activated SHALL NOT be available to unauthorized access. After use, the cryptographic module SHALL be deactivated., via a manual logout procedure or automatically after a period of inactivity. CA cryptographic modules SHALL be stored securely when not attached.

With respect to the private keys of offline CAs, after the completion of a Key Generation Ceremony, in which such private keys are used for private key operations, the CA SHALL remove the token containing the private keys from the reader to deactivate them, or take similar action based upon the type of hardware used to store the private key. Once removed from the reader or hardware, tokens SHALL be securely stored.

When deactivated, private keys SHALL be kept in encrypted form only.

6.2.10. Method of Destroying Private Keys

Private keys SHALL be destroyed in a way that prevents their theft, disclosure, or unauthorized use.

CA private signature keys SHALL be destroyed by individuals in trusted roles following a documented procedure that additionally guarantees that a destroyed key can neither be restored nor be re-computed (e.g., from backups or residual remains of the key) under any circumstances. For PAAs, this process SHALL be witnessed by one or more persons authorized by the PKI-PA to perform such a function.

Requestors MAY destroy their private signature keys when they are no longer needed or when the Certificates to which they correspond expire. Physical destruction of hardware is not required.

6.2.11. Cryptographic Module Rating

See CP section Cryptographic Module Standards and Controls

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

CAs MAY archive their public keys by archiving their public key Certificate.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The Certificate Validity Period (i.e., Certificate operational period and key pair usage period) SHALL be set to the time limits appropriate to the ecosystem, expected device lifetimes, and to cryptographic expectations for protection based on key size, algorithm, and available computational processing.

As necessary to ensure the continuity and security of the Matter PKI, the Connectivity Standards Alliance Trustees SHALL approve new CAs to be added to the DCL.

Matter PKI Participants SHALL cease all use of their key pairs after their usage periods have expired. Uncompromised keys can be reused for new Certificates for the same device.

6.4. Activation Data

This section is only applicable to CAs whose private key is stored on a device that requires explicit user activation and deactivation of the key using some secret data. Some platforms, such as certain HSM platforms, have no notion of cryptographic key activation. For such platforms, key activation SHALL NOT be required as long as the private key is protected from unauthorized access at all times.

6.4.1. Activation Data Generation and Installation

The activation data (e.g., PINs, passwords, or manually-held key shares) used to unlock private keys, in conjunction with any other access control procedure, SHALL have an appropriate level of

strength for the keys or data to be protected and SHALL meet the applicable Security Policy requirements of the cryptographic module used to store the keys. CAs SHALL generate and install activation data for their private keys and SHALL use methods that protect the activation data to the extent necessary to prevent the loss, theft, modification, disclosure, or unauthorized use of such activation data.

When a CA uses passwords as activation data for the CA signing key, at a minimum the activation data SHALL be changed upon CA re-key.

Requestor activation data MAY be user selected.

6.4.2. Activation Data Protection

Data used to unlock private keys SHALL be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data SHOULD be either biometric in nature or memorized. If written down, it SHALL be secured at the level of the data that the associated cryptographic module is used to protect and SHALL NOT be stored with the cryptographic module. In all cases, the protection mechanism SHALL include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed logins attempts as set forth in the respective CPS.

CAs SHALL protect the activation data for their private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

CAs SHALL use multi-party control and provide the procedures and means to enable Shareholders to take the precautions necessary to prevent the loss, theft, modification, disclosure, or unauthorized use of the Secret Shares that they possess. Shareholders SHALL NOT:

- Copy, disclose, or make the Secret Share available to a third party, or make any unauthorized use of it whatsoever; or
- Disclose their or any other person’s status as a Shareholder to any third party.

The Secret Shares and any information disclosed to the Shareholder in connection with their duties as a Shareholder SHALL constitute Confidential/Private Information.

CAs SHALL include in their DRPs provisions for making Secret Shares available at a disaster recovery site after a disaster (Note: The important aspect of disaster recovery vis-à-vis shares is that a process exists for making the necessary number of shares available, even if the requisite Shareholders are not available.) CAs SHALL maintain an Audit trail of Secret Shares, and Shareholders SHALL participate in the maintenance of an Audit trail.

6.4.3. Aspects of Activation Data

CAs, RAs, and CSSs SHALL change the activation data whenever the token is re-keyed or returned from maintenance.

6.4.3.1. Activation Data Transmission

To the extent activation data for their private keys is transmitted, activation data participants

SHALL protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent a desktop computer or a network logon username/password combination is used as activation data for an end-user Requestor, the passwords transferred across a network SHALL be protected against access by unauthorized users.

6.4.3.2. Activation Data Destruction

Activation data for CA private keys SHALL be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention period lapses, CAs SHALL decommission activation data by overwriting and/or physical destruction.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

CA/RA/CSSs SHALL ensure that the systems maintaining software and data files are Trustworthy Systems secure from unauthorized access. In addition, CA/RA/CSSs SHALL limit access to production servers to those individuals with a valid business reason for access. General application users SHALL NOT have accounts on the production servers.

CA/RA/CSSs SHALL have production networks logically separated from other components. This separation prevents network access except through defined application processes. CA/RA/CSSs SHALL use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that might access production systems.

To the extent that passwords are used, CA/RA/CSSs SHALL require the use of passwords with a minimum character length and a combination of alphanumeric and special characters and SHALL require that passwords be changed whenever necessary, such as if they have been exposed. Direct access to a CA's database maintaining the CA's repository SHALL be limited to Trusted Persons having a valid business reason for such access.

Computer security controls are required to ensure CA operations are performed securely. The following computer security functions MAY be provided by the operating system, or through a combination of operating system, software, and physical safeguards:

- Require authenticated logins
- Provide discretionary access control
- Provide a security Audit capability
- Enforce access control for CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object reuse or require separation for CA random access memory
- Require use of cryptography for session communication and database security

- Archive CA history and Audit data
- Require self-test security-related CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanism for keys and the CA system
- Enforce domain integrity boundaries for security-critical processes

For other CAs operating under this CP, the computer security functions listed below are required. These functions MAY be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts SHALL include the following functionality:

- Authenticate the identity of users before permitting access to the system or applications
- Manage privileges of users to limit users to their assigned roles
- Generate and archive Audit records for all transactions
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

CSSs, operating under this CP, SHALL follow the computer security functions listed:

- Authenticate the identity of users before permitting access to the system or applications
- Manage privileges of users to limit users to their assigned roles
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

Remote workstations used to administer the CAs SHALL follow the computer security functions listed below:

- Authenticate the identity of users before permitting access to the system or applications
- Manage privileges of users to limit users to their assigned roles
- Generate and archive Audit records for all transactions
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

All communications between any PKI trusted role and the CA SHALL be authenticated and protected from modification.

6.5.2. Computer Security Rating

No stipulation.

6.6. Lifecycle Technical Controls

6.6.1. System Development Controls

The system development controls for the CA and CSS are as follows:

- For hardware and software used in PKI operations that are run by a trusted third-party provider, a SOC2 Type 2 report from that trusted third-party provider MAY be used along with a CPS to satisfy hardware and software security requirements that are not within the control of the CA.
- Use software 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 component was tampered with (e.g., by ensuring the Vendor cannot identify the PKI component that will be installed on a device).
- Hardware and software developed specifically for the CA and CSS SHALL be developed in a controlled environment, and the development process SHALL be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- A CA SHALL employ access controls around hardware and software to prevent access to its signing private keys by unauthorized parties or systems.
- Hardware and software used to administrate PKI operations as a client to cloud-based services SHALL require a modern operating system that is verified at boot, is actively patched, runs only authorized applications, and is actively monitored.
- The CA shall implement controls to prevent the introduction of malicious software onto its PKI equipment. All applications required to perform PKI operations SHALL be obtained from documented sources and vulnerability scans SHALL be performed at least quarterly and after significant changes to detect critical vulnerabilities.
- Hardware and software updates SHALL be purchased or developed in the same manner as original equipment and SHALL be installed by trusted and trained personnel in a defined manner.

6.6.2. Security Management Controls

The configuration of the CA and CSS system, in addition to any modifications and upgrades, SHALL be documented and controlled. There SHALL be a mechanism for detecting unauthorized modification to the software or configuration. The CA and CSS software, when first loaded, SHALL be verified as being that supplied from the Vendor, with no modifications, and be the version intended for use.

In addition, only applications required to perform the organization’s mission SHALL be loaded onto the RA workstation, and all such software SHALL be obtained from sources authorized by local policy.

6.6.3. Lifecycle Security Controls

No stipulation.

6.7. Network Security Controls

CAs, CSSs, and RAs SHALL employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures SHALL include the use of network guards, firewalls, or filtering routers. The network guard, firewall, or filtering router SHALL limit services allowed to and from the Signing System to those required to perform its functions.

Protection of the Signing System against known network attacks SHALL be provided. All unused network ports and services SHALL be turned off. Any network software present on the Signing System SHALL be strictly necessary to perform its functions.

Any boundary control devices used to protect the network on which a Signing System is hosted SHALL deny all but the necessary services to the Signing System.

Repositories and remote workstations used to administer the CAs SHALL employ appropriate network security controls. Networking equipment SHALL turn off unused network ports and services. Any network software present SHALL be necessary to the functioning of the equipment.

The CA SHALL establish connection with a remote workstation used to administer the CA only after successful authentication of the workstation at a level of assurance commensurate with that of the CA.

6.8. Time-Stamping

Certificates SHALL contain time and date information. Such time information need not be cryptographic based. Asserted times SHALL be accurate to within three (3) minutes. Electronic or manual procedures MAY be used to maintain system time. Clock adjustments are auditable events.

Chapter 7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profile

Matter PKI Certificates SHALL conform to RFC 5280 [3] .

As required by the Matter specification, all Matter PKI certificates SHALL NOT be longer than 600 bytes when represented as ASN.1 DER encoding.

Matter PKI Certificates SHALL contain the identity and attribute data of a Subject using the base Certificate with applicable extensions. The base Certificate SHALL contain the version number of the Certificate, the Certificate's identifying serial number, the signature algorithm used to sign the Certificate, the issuer's DN, the Validity Period of the Certificate, the Subject's DN, information about the Subject's public key, and extensions.

Table 6. Certificate Profile Basic Fields

Field	RFC 5280 Section	Comments
tbsCertificate	4.1.1.1	Follows RFC 5280 [3] guidance
Version	4.1.2.1	See CP section 7.1.1
serialNumber	4.1.2.2	A non-sequential value greater than zero (0) containing at least 64 bits of output from a CSPRNG. The encoded value SHALL be 20 octets or less.
signature	4.1.2.3	See CP section 7.1.3
issuer	4.1.2.4	See CP section 7.1.4
validity	4.1.2.5	See CP section 6.3.2
subject	4.1.2.6	See CP section 7.1.4
subjectPublicKeyInfo	4.1.2.7	See CP section 7.1.3
extensions	4.1.2.9	See CP section 7.1.2
signatureAlgorithm	4.1.1.2	Follows RFC 5280 [3] guidance
algorithmIdentifier	4.1.1.2	
algorithm	4.1.1.2	See CP section 7.1.3
parameters	4.1.1.2	See CP section 7.1.3
signatureValue	4.1.1.3	Follows RFC 5280 [3] guidance

7.1.1. Version Number(s)

Matter PKI Certificates SHALL be X.509 v3 Certificates. The Certificate version number SHALL be

set to the integer value of "2" for Version 3 Certificates.

7.1.2. Certificate Extensions

Matter PKI Certificate extensions provide methods for associating additional attributes and values with public keys and for managing relationships between CAs. Matter PKI Certificates SHALL follow the guidance in RFC 5280 [3] and SHALL contain the standard extensions shown in the tables below, unless they are denoted as optional.

Certificates issued under this CP SHALL use standard Certificate extensions as defined in the Device Attestation Section of the Matter Specification [6] .

7.1.2.1. Subject Key Identifier Extension

Certificates issued under this CP SHALL use the subject key identifier extensions that are defined in the Device Attestation section of the Matter Specification [6] .

7.1.2.2. Basic Constraints Extension

Certificates issued under this CP SHALL use Basic Constraints Extension attributes as defined in the Device Attestation section of the Matter Specification [6] .

7.1.3. Algorithm Object Identifiers (OIDs)

Certificates issued under this CP SHALL use OIDs defined in the Device Attestation section of the Matter [6] specification.

7.1.4. PAA Certificate

A PAA issues a PAI. A PAA can be restricted to one vendor (VID-scoped PAA) by including the vendor's Vendor Identifier (VID value) in the PAA Certificate.

The attributes and values in a PAA Certificate are referenced in Section 6.1.2.1 of the Matter Specification [6] :

7.1.5. PAI Certificate

A PAI issues a DAC to a Device or other commissionable software component. A PAI is restricted to a vendor by including the vendor's Vendor Identifier (VID value) in the PAI Certificate and can be further restricted to a particular product line by including a Product Identifier (PID value) in that extension.

The attributes and values in a PAI Certificate are referenced in Section 6.1.2.1 of the Matter Specification [6] :

7.1.6. Device Attestation Certificate (DAC)

The attributes and values of a DAC are referenced in Section 6.1.2 of the Matter Specification [6] :

7.1.7. Name Forms

See CP section Types of Names.

7.1.8. Name Constraints

The CAs SHALL NOT assert name constraints in Matter PKI Certificates.

7.1.9. Certificate Policy Object Identifier

No stipulation.

7.1.10. Usage of Policy Constraints Extension

The CAs SHALL NOT assert policy constraints in CA Certificates.

7.1.11. Policy Qualifiers Syntax and Semantics

Certificates issued under this CP SHALL NOT contain policy qualifiers or userNotice qualifiers.

7.1.12. Processing Semantics for the Critical *Certificate Policies* Extension

Certificates issued under this CP SHALL NOT contain a critical *certificate policies* extension.

7.2. CRL Profile

No stipulation.

Chapter 8. Compliance Audit and Other Assessments

The requirements in this section apply to PAAs that provide services for multiple Vendor IDs. For PAAs that are restricted to one vendor ID (VID-scoped PAA) or to PAIs (which are inherently restricted to one vendor ID), the operator SHALL only attest that internal Audits are periodically performed.

CAs that perform internal Audit under the rules above SHALL share the results of the internal Audit with the PKI-PA to enable inclusion of the PAA in the DCL.

The CA SHALL be responsible for providing proof that the DSP used for services and/or infrastructure is ISO 27001 and SOC 2 Type 2 certified. The CA is responsible for monitoring the compliance with these requirements for all DSPs it uses. The CA SHALL describe in the CPS how security responsibilities are split between the CA and every DSP, for the relevant services and infrastructure.

8.1. Frequency or Circumstances of Assessment

CAs operating under this CP SHALL undergo a periodic CAAF Audit as defined by the Connectivity Standards Alliance.

8.2. Identity/Qualifications of Assessor

Auditors performing the Audit SHALL be from an independent Audit firm that is approved to Audit according to the CAAF.

8.3. Assessor’s Relationship to Assessed Entity

The Auditor either SHALL be a private firm that is independent from the entity being audited, or it SHALL be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. Auditors SHALL NOT have a conflict of interest that hinders their ability to perform auditing services.

8.4. Topics Covered by Assessment

The purpose of an Audit SHALL be to verify that a PKI component complies with all the requirements of the current versions of this CP.

The Audit SHALL be in accordance with the CAAF standard approved by PKI-PA which includes:

- A Report of Policies and Procedures in Operation and Test of Operational Effectiveness.

All aspects of the CA operation SHALL undergo inspection and SHOULD:

- Identify foreseeable internal and external threats that could result in unauthorized access,

disclosure, misuse, alteration, or destruction of any Certificate data or Certificate management processes;

- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate data and Certificate management processes; and
- Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

8.5. Actions Taken because of Deficiency

When the Auditor finds a discrepancy between the requirements of this CP and the design, operation, or maintenance of the PKI-PA, the following actions SHALL be performed:

- The Auditor SHALL note the discrepancy;
- The Auditor SHALL notify the responsible parties promptly; and
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the PKI-PA.

In the event the audited entity fails to develop a corrective action plan or implement it, or if the report reveals exceptions or deficiencies that the PKI-PA reasonably believes pose an immediate threat to the security or integrity of the Matter PKI, then the PKI-PA:

- SHALL determine whether Compromise reporting is necessary;
- SHALL be entitled to suspend services to the audited entity; and
- If necessary, MAY terminate such services related to this CP and the terms of the audited entity's contract.

8.6. Communication of Results

Audit results SHALL be communicated to the PKI-PA and MAY be communicated to others as deemed appropriate.

Chapter 9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

Requestors MAY be charged a fee for the issuance, management, and renewal of Certificates.

9.1.2. Certificate Access Fees

CAs SHALL NOT charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3. Revocation or Status Information Access Fees

No Stipulation.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

Refund policies SHOULD be stipulated in the appropriate agreement (i.e., RAD).

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Matter PKI Participants SHOULD maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

9.2.2. Other Assets

CAs SHALL have enough financial resources to maintain their operations and perform their duties, and they SHALL be reasonably able to bear the risk of liability to Requestors and Relying Parties.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The following Requestor information SHALL be kept confidential and private:

- CA application records;
- Certificate Application records;
- Personal or non-public information about Requestors;
- Transactional records (both full records and the Audit trail of transactions); and
- Security measures controlling the operations of CA hardware and software.

9.3.2. Information Not Within the Scope of Confidential Information

Certificates and other status information, Matter repositories, and information contained within them, SHALL NOT be considered Confidential/Private Information.

9.3.3. Responsibility to Protect Confidential Information

Matter PKI Participants receiving private information SHALL secure it from Compromise and disclosure to third parties.

9.4. Privacy of Personal Information

9.4.1. Privacy Policy

No Stipulation

9.4.2. Information Treated as Private

CAs SHALL protect all Requestors' personally identifying information from unauthorized disclosure. Records of individual transactions MAY be released upon request of any Requestors involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under the CP SHALL NOT be released except as required by law.

9.4.3. Information Not Deemed Private

Information included in the Certificates is deemed public information and is not afforded protections.

9.4.4. Responsibility to Protect Private Information

Sensitive information SHALL be stored securely and MAY be released only as required by law.

9.4.5. Notice and Consent to Use Private Information

The PKI-PA or Matter PKI CAs are not required to provide any notice or obtain the consent of the Requestor to release private information.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

The PKI-PA or Matter PKI CAs SHALL NOT disclose private information to any third party unless authorized by this CP, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property Rights

CAs retain all Intellectual Property Rights in and to the Certificates that they issue.

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and DN within any Certificate issued to such Certificate Applicant.

Private keys corresponding to Certificates of CAs and Requestors are the property of the CAs and Requestors that are the respective Subjects of these Certificates. Secret Shares of a CA's private key is the property of the CA, and the CA retains all Intellectual Property Rights in and to such Secret Shares.

9.6. Representations and Warranties

The PKI-PA SHALL:

- Approve the CPS for each CA that issues Certificates under this CP;
- Review periodic Audits to ensure that CAs are operating in compliance with their approved CPSs;
- Review name space control procedures to ensure that DNs are uniquely assigned for all Certificates issued under this CP;
- Revise this CP to maintain the level of assurance and operational practicality;
- Publicly distribute this CP; and
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs.

9.6.1. CA Representations and Warranties

CAs operating under this CP SHALL warrant that:

- The CA procedures are implemented in accordance with this CP;
- The CA will provide its CPS to the PKI-PA, as well as any subsequent changes, for conformance assessment;
- The CA operations are maintained in conformance to the stipulations of the approved CPS;

- Any Certificate issued is in accordance with the stipulations of this CP;
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate;
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application because of a failure to exercise reasonable care in managing the Certificate Application; and
- Its Certificates meet all material requirements of this CP and the applicable CPS.

9.6.2. RA Representations and Warranties

To the extent permitted by applicable law, Connectivity Standards Alliance disclaims any warranties, including any warranty of merchantability or fitness for a purpose.

9.6.3. Requestor Representations and Warranties

Requestors SHALL sign an agreement containing the requirements the Requestor SHALL meet, including protection of their private keys and use of the Certificates before being issued the Certificates. In addition, Requestors SHALL warrant that:

- The Requestor SHALL abide by all the terms, conditions, and restrictions levied on the use of their private keys and Certificates.
- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Requestor and the Certificate has been accepted and is operational (not expired) at the time the digital signature is created.
- Requestor's private keys are protected from unauthorized use or disclosure.
- All representations made by the Requestor in the Certificate Application the Requestor submitted are true.
- All information supplied by the Requestor and contained in the Certificate is true.
- The Certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CP.
- The Requestor will promptly notify the appropriate CA upon suspicion of loss or Compromise of their private key(s).
- The Requestor is an end-user Requestor and not a CA and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) as a CA or otherwise.
- RAD MAY include additional representations and warranties.

9.6.4. Relying Party Representations and Warranties

This CP does not specify the steps a Relying Party SHOULD take to determine whether to rely upon a Certificate. The Relying Party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., Certificates) needed to perform the trust path creation, validation, and CP mappings that the Relying Party MAY wish to employ in its determination. Relying Parties

acknowledge that they have enough information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they SHALL bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. Disclaimers of Warranties

To the extent permitted by applicable law, RAD SHALL disclaim the CA's and the applicable Requestor's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8. Limitations of Liability

The liability (and/or limitation thereof) of Requestors SHALL be as set forth in the applicable RAD.

9.9. Indemnities

To the extent permitted by applicable law, Requestors are required to indemnify CAs for:

- Falsehood or misrepresentation of fact by the Requestor on the Certificate Application;
- Failure by the Requestor to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party;
- The Requestor's failure to take the precautions necessary to prevent the Compromise, loss, disclosure, modification, or unauthorized use of the Requestor's private key(s) or a digital Certificate; and
- The Requestor's use of a name, including that which infringes upon the Intellectual Property Rights of a third party.

9.10. Term and Termination

9.10.1. Term

This CP becomes effective when approved by the PKI-PA. Amendments to this CP become effective upon publication. This CP has no specified term.

9.10.2. Termination

This CP, as amended from time to time, SHALL remain in force until it is replaced by a new version. Termination of this CP is at the discretion of the PKI-PA.

9.10.3. Effect of Termination and Survival

Upon termination of this CP, Matter PKI Participants are nevertheless bound by its terms for all Certificates issued for the remainder of the Validity Periods of such Certificates.

9.11. Individual Notices and Communications with PKI Participants

Unless otherwise specified by agreement between the parties, Matter PKI Participants SHALL use commercially reasonable methods to communicate with each other, considering the criticality and subject matter of the communication.

9.12. Amendments

9.12.1. Procedure for Amendment

The PKI-PA SHALL review this CP at least once every year. Corrections, updates, or changes to this CP SHALL be made publicly available. Suggested changes to this CP SHALL be communicated to the PKI-PA; such communication SHALL include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2. Notification Mechanism and Period

The PKI-PA reserves the right to amend this CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to web links, and changes to contact information. The PKI-PA's decision to designate amendments as material or non-material SHALL be within the PKI-PA's sole discretion.

Change notices to this CP SHALL be distributed electronically to Matter PKI Participants and observers in accordance with the PKI-PA document change procedures.

9.12.3. Circumstances Under Which OID SHALL be Changed

If the PKI-PA determines that a change is necessary in the OID corresponding to a Certificate Policy, the amendment SHALL contain new object identifiers for the Certificate Policies corresponding to each class of Certificate. Otherwise, amendments SHALL NOT require a change in Certificate Policy object identifier.

9.13. Dispute Resolution Provisions

The PKI-PA SHALL facilitate the resolution between entities when conflicts arise because of the use of Certificates issued under this CP.

9.14. Governing Law

The Matter PKI Certificate Policy, and all the rights and duties arising from or relating in any way to

the subject matter thereof SHALL be governed by, construed and enforced in accordance with the laws of the State of California (excluding any conflict of laws provisions of the State of California that would refer to and apply the substantive laws of another jurisdiction). This choice of law is made to ensure uniform procedures and interpretation for all Matter PKI Participants, no matter where they are located.

9.15. Compliance with Applicable Law

This CP is subject to applicable national, state, local, and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. All CAs operating under this CP SHALL comply with applicable law.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP SHALL remain in effect until this CP is updated.

If a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of this CP SHALL remain valid.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5. Force Majeure

To the extent permitted by applicable law, Matter PKI agreements (e.g., RAD) SHALL include a force majeure clause protecting the Connectivity Standards Alliance and the applicable Requestor.

9.17. Other Provisions

No stipulation.