Contents

1. INTRODUCTION **6**
1.1 Overview . . . 6
1.2 Document name and identification . . . 6
Changelog: . . . 6
1.3 PKI participants . . . 7
1.3.1 Certification authorities . . . 7
1.3.2 Registration authorities . . . 7
1.3.3 Subscribers . . . 7
1.3.4 Relying parties . . . 7
1.3.5 Other participants . . . 7
1.4 Certificate usage . . . 7
1.4.1. Appropriate certificate uses . . . 7
1.4.2 Prohibited certificate uses . . . 7
1.5 Policy administration . . . 8
1.5.1 Organization administering the document . . . 8
1.5.2 Contact person . . . 8
1.5.3 Person determining CPS suitability for the policy . . . 8
1.5.4 CP approval procedures . . . 8
1.6 Definitions and acronyms . . . 8

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES **11**
2.1 Repositories . . . 11
2.2 Publication of certification information . . . 11
2.3 Time or frequency of publication . . . 11
2.4 Access controls on repositories . . . 11

3. IDENTIFICATION AND AUTHENTICATION **12**
3.1 Naming . . . 12
3.1.1 Types of names . . . 12
3.1.2 Need for names to be meaningful . . . 12
3.1.3 Anonymity or pseudonymity of subscribers . . . 12
3.1.4 Rules for interpreting various name forms . . . 12
3.1.5 Uniqueness of names . . . 12
3.1.6 Recognition, authentication, and role of trademarks . . . 12
3.2 Initial identity validation . . . 12
3.2.1 Method to prove possession of private key . . . 12
3.2.2 Authentication of organization identity . . . 12
3.2.3 Authentication of individual identity . . . 12
3.2.4 Authentication of machine identity . . . 13
3.2.5 Non-verified subscriber information . . . 14
3.2.6 Validation of authority . . . 14
3.2.7 Criteria for interoperation . . . 14
3.3 Identification and authentication for re-key requests . . . 15
3.3.1 Identification and authentication for routine re-key . . . 15
3.3.2 Identification and authentication for re-key after revocation . . . 15
3.4 Identification and authentication for revocation request . . . 15

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS **16**
4.1 Certificate Application . . . 16
4.1.1 Who can submit a certificate application . . . 16
4.1.2 Enrollment process and responsibilities . . . 16
4.2 Certificate application processing . . . 16
4.2.1 Performing identification and authentication functions . . . 16
4.2.2 Approval or rejection of certificate applications . . . 16
4.2.3 Time to process certificate applications . . . 16

4.3 Certificate issuance . . . 16
4.3.1 CA actions during certificate issuance . . . 16
4.3.2 Notification to subscriber by the CA of issuance of certificate . . . 16
4.4 Certificate acceptance . . . 17
4.4.1 Conduct constituting certificate acceptance . . . 17
4.4.2 Publication of the certificate by the CA . . . 17
4.4.3 Notification of certificate issuance by the CA to other entities . . . 17
4.5 Key pair and certificate usage . . . 17
4.5.1 Subscriber private key and certificate usage . . . 17
4.5.2 Relying party public key and certificate usage . . . 17
4.6 Certificate renewal . . . 17
4.6.1 Circumstance for certificate renewal . . . 17
4.6.2 Who may request renewal . . . 18
4.6.3 Processing certificate renewal requests . . . 18
4.6.4 Notification of new certificate issuance to subscriber . . . 18
4.6.5 Conduct constituting acceptance of a renewal certificate . . . 18
4.6.6 Publication of the renewal certificate by the CA . . . 18
4.6.7 Notification of certificate issuance by the CA to other entities . . . 18
4.7 Certificate re-key . . . 18
4.7.1 Circumstance for certificate re-key . . . 18
4.7.2 Who may request certification of a new public key . . . 18
4.7.3 Processing certificate re-keying requests . . . 18
4.7.4 Notification of new certificate issuance to subscriber . . . 18
4.7.5 Conduct constituting acceptance of a re-keyed certificate . . . 19
4.7.6 Publication of the re-keyed certificate by the CA . . . 19
4.7.7 Notification of certificate issuance by the CA to other entities . . . 19
4.8 Certificate modification . . . 19
4.8.1 Circumstance for certificate modification . . . 19
4.8.2 Who may request certificate modification . . . 19
4.8.3 Processing certificate modification requests . . . 19
4.8.4 Notification of new certificate issuance to subscriber . . . 19
4.8.5 Conduct constituting acceptance of modified certificate . . . 19
4.8.6 Publication of the modified certificate by the CA . . . 19
4.8.7 Notification of certificate issuance by the CA to other entities . . . 19
4.9 Certificate revocation and suspension . . . 20
4.9.1 Circumstances for revocation . . . 20
4.9.2 Who can request revocation . . . 21
4.9.3 Procedure for revocation request . . . 21
4.9.4 Revocation request grace period . . . 21
4.9.5 Time within which CA must process the revocation request . . . 21
4.9.6 Revocation checking requirement for relying parties . . . 22
4.9.7 CRL issuance frequency (if applicable) . . . 22
4.9.8 Maximum latency for CRLs (if applicable) . . . 22
4.9.9 On-line revocation/status checking availability . . . 22
4.9.10 On-line revocation checking requirements . . . 22
4.9.11 Other forms of revocation advertisements available . . . 22
4.9.12 Special requirements re key compromise . . . 22
4.9.13 Circumstances for suspension . . . 22
4.9.14 Who can request suspension . . . 22
4.9.15 Procedure for suspension request . . . 23
4.9.16 Limits on suspension period . . . 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 End of subscription . . . 23

4.12 Key escrow and recovery . . . 23
4.12.1 Key escrow and recovery policy and practices . . . 23
4.12.2 Session key encapsulation and recovery policy and practices . . . 23

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 24
5.1 Physical controls . . . 24
5.1.1 Site location and construction . . . 24
5.1.2 Physical access . . . 25
5.1.3 Power and air conditioning . . . 25
5.1.4 Water exposures . . . 25
5.1.5 Fire prevention and protection . . . 25
5.1.6 Media storage . . . 25
5.1.7 Waste disposal . . . 25
5.1.8 Off-site backup . . . 25
5.2 Procedural controls . . . 25
5.2.1 Trusted roles . . . 25
5.2.2 Number of persons required per task . . . 25
5.2.3 Identification and authentication for each role . . . 26
5.2.4 Roles requiring separation of duties . . . 26
5.3 Personnel controls . . . 26
5.3.1 Qualifications, experience, and clearance requirements . . . 26
5.3.2 Background check procedures . . . 26
5.3.3 Training requirements . . . 26
5.3.4 Retraining frequency and requirements . . . 26
5.3.5 Job rotation frequency and sequence . . . 26
5.3.6 Sanctions for unauthorized actions . . . 26
5.3.7 Independent contractor requirements . . . 26
5.3.8 Documentation supplied to personnel . . . 27
5.4 Audit logging procedures . . . 27
5.4.1 Types of events recorded . . . 27
5.4.2 Frequency of processing log . . . 27
5.4.3 Retention period for audit log . . . 28
5.4.4 Protection of audit log . . . 28
5.4.5 Audit log backup procedures . . . 28
5.4.6 Audit collection system (internal vs. external) . . . 28
5.4.7 Notification to event-causing subject . . . 28
5.4.8 Vulnerability assessments . . . 28
5.5 Records archival . . . 28
5.5.1 Types of records archived . . . 28
5.5.2 Retention period for archive . . . 29
5.5.3 Protection of archive . . . 29
5.5.4 Archive backup procedures . . . 29
5.5.5 Requirements for time-stamping of records . . . 29
5.5.6 Archive collection system (internal or external) . . . 29
5.5.7 Procedures to obtain and verify archive information . . . 29
5.6 Key changeover . . . 29
5.7 Compromise and disaster recovery . . . 29
5.7.1 Incident and compromise handling procedures . . . 29
5.7.2 Computing resources, software, and/or data are corrupted . . . 30
5.7.3 Entity private key compromise procedures . . . 30
5.7.4 Business continuity capabilities after a disaster . . . 30
5.8 CA or RA termination . . . 30

6. TECHNICAL SECURITY CONTROLS 31
6.1 Key pair generation and installation . . . 31
6.1.1 Key pair generation . . . 31
6.1.2 Private key delivery to subscriber . . . 31

6.1.3 Public key delivery to certificate issuer . . . 31
6.1.4 CA public key delivery to relying parties . . . 31
6.1.5 Key sizes . . . 32
6.1.6 Public key parameters generation and quality checking . . . 32
6.1.7 Key usage purposes (as per X.509 v3 key usage field) . . . 32
6.2 Private Key Protection and Cryptographic Module Engineering Controls . . . 32
6.2.1 Cryptographic module standards and controls . . . 32
6.2.2 Private key (n out of m) multi-person control . . . 33
6.2.3 Private key escrow . . . 33
6.2.4 Private key backup . . . 33
6.2.5 Private key archival . . . 33
6.2.6 Private key transfer into or from a cryptographic module . . . 33
6.2.7 Private key storage on cryptographic module . . . 33
6.2.8 Method of activating private key . . . 33
6.2.9 Method of deactivating private key . . . 33
6.2.10 Method of destroying private key . . . 33
6.2.11 Cryptographic Module Rating . . . 33
6.3 Other aspects of key pair management . . . 34
6.3.1 Public key archival . . . 34
6.3.2 Certificate operational periods and key pair usage periods . . . 34
6.4 Activation data . . . 34
6.4.1 Activation data generation and installation . . . 34
6.4.2 Activation data protection . . . 34
6.4.3 Other aspects of activation data . . . 34
6.5 Computer security controls . . . 34
6.5.1 Specific computer security technical requirements . . . 34
6.5.2 Computer security rating . . . 34
6.6 Life cycle technical controls . . . 34
6.6.1 System development controls . . . 35
6.6.2 Security management controls . . . 35
6.6.3 Life cycle security controls . . . 35
6.7 Network security controls . . . 35
6.8 Time-stamping . . . 35

7. CERTIFICATE, CRL, AND OCSP PROFILES 36
7.1 Certificate profile . . . 36
7.1.1 Version number(s) . . . 36
7.1.2 Certificate extensions . . . 36
7.1.3 Algorithm object identifiers . . . 40
7.1.4 Name forms . . . 41
7.1.5 Name constraints . . . 43
7.1.6 Certificate policy object identifier . . . 44
7.1.7 Usage of Policy Constraints extension . . . 44
7.1.8 Policy qualifiers syntax and semantics . . . 44
7.1.9 Processing semantics for the critical Certificate Policies extension . . . 44
7.2 CRL profile . . . 44
7.2.1 Version number(s) . . . 44
7.2.2 CRL and CRL entry extensions . . . 45
7.3 OCSP profile . . . 45
7.3.1 Version number(s) . . . 45
7.3.2 OCSP extensions . . . 45

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 46
8.1 Frequency or circumstances of assessment . . . 46
8.2 Identity/qualifications of assessor . . . 46
8.3 Assessor's relationship to assessed entity . . . 46
8.4 Topics covered by assessment . . . 46

8.5 Actions taken as a result of deficiency . . . 46
8.6 Communication of results . . . 47

9. OTHER BUSINESS AND LEGAL MATTERS 48
9.1 Fees . . . 48
9.1.1 Certificate issuance or renewal fees . . . 48
9.1.2 Certificate access fees . . . 48
9.1.3 Revocation or status information access fees . . . 48
9.1.4 Fees for other services . . . 48
9.1.5 Refund policy . . . 48
9.2 Financial responsibility . . . 48
9.2.1 Insurance coverage . . . 48
9.2.2 Other assets . . . 48
9.2.3 Insurance or warranty coverage for end-entities . . . 48
9.3 Confidentiality of business information . . . 48
9.3.1 Scope of confidential information . . . 48
9.3.2 Information not within the scope of confidential information . . . 49
9.3.3 Responsibility to protect confidential information . . . 49
9.4 Privacy of personal information . . . 49
9.4.1 Privacy plan . . . 49
9.4.2 Information treated as private . . . 49
9.4.3 Information not deemed private . . . 49
9.4.4 Responsibility to protect private information . . . 49
9.4.5 Notice and consent to use private information . . . 49
9.4.6 Disclosure pursuant to judicial or administrative process . . . 49
9.4.7 Other information disclosure circumstances . . . 49
9.5 Intellectual property rights . . . 50
9.6 Representations and warranties . . . 50
9.6.1 CA representations and warranties . . . 50
9.6.2 RA representations and warranties . . . 50
9.6.3 Subscriber representations and warranties . . . 50
9.6.4 Relying party representations and warranties . . . 50
9.6.5 Representations and warranties of other participants . . . 51
9.7 Disclaimers of warranties . . . 51
9.8 Limitations of liability . . . 51
9.9 Indemnities . . . 51
9.10 Term and termination . . . 52
9.10.1 Term . . . 52
9.10.2 Termination . . . 52
9.10.3 Effect of termination and survival . . . 52
9.11 Individual notices and communications with participants . . . 52
9.12 Amendments . . . 52
9.12.1 Procedure for amendment . . . 52
9.12.2 Notification mechanism and period . . . 52
9.12.3 Circumstances under which OID must be changed . . . 52
9.13 Dispute resolution provisions . . . 52
9.14 Governing law . . . 53
9.15 Compliance with applicable law . . . 53
9.16 Miscellaneous provisions . . . 53
9.16.1 Entire agreement . . . 53
9.16.2 Assignment . . . 53
9.16.3 Severability . . . 53
9.16.4 Enforcement (attorneys' fees and waiver of rights) . . . 53
9.16.5 Force Majeure . . . 53
9.17 Other provisions . . . 54

1. INTRODUCTION

1.1 Overview

Base Policy

Fortanix may make certain claims towards its customers, users, or other interested parties ("the public") regarding its services. For example, we may claim that a particular key is managed by us. Or that a particular API endpoint is provided by a Confidential Computing service with particular security properties. When these claims are done in a binding way using cryptography, we say that Fortanix attests these claims, and this process is called attestation. Such claims are made by entities in the Fortanix Attestation and Provisioning PKI.

The Fortanix Service Attestation PKI is part of the Fortanix Attestation and Provisioning PKI, and entitities in the Fortanix Service Attestation PKI make claims about Fortanix Data Security Manager (DSM) clusters. This Certificate Policy is intended to communicate the minimum operating requirements for CAs and end-entities in the Fortanix Service Attestation PKI.

This Certificate Policy extends the Fortanix Attestation and Provisioning PKI Certificate Policy (OID 1.3.6.1.4.1.49690.6.1) unless explicitly mentioned in the section.

1.2 Document name and identification

Base Policy

This document is the Fortanix Attestation and Provisioning PKI Certificate Policy. This document is identified by the Object Identifier 1.3.6.1.4.1.49690.6.1.

This document is the Fortanix Service Attestation PKI Certificate Policy. This document is identified by the Object Identifier 1.3.6.1.4.1.49690.6.1.3.

Changelog:

Base Policy

date	description	version
2023-08-25	Draft	0.1
2023-08-31	Initial release	1.0
2024-08-29	Annual Review	1.1
2025-01-27	Correct CP OID	1.2
2025-02-11	Correct CP OID	1.3
2025-05-21	Minor copyediting	1.4

Fortanix Service Attestation PKI Certificate Policy

date	description	version
2025-05-09	Draft	0.1
2025-05-21	Initial release	1.0
2025-06-02	Minor copyediting	1.1
2025-06-12	Remove IAS attestation option for CSRs	1.2

Please note that certificates issued prior to a specific date mentioned in the changelog do not necessarily reflect the stipulations mentioned in the version of the Certificate Policy at that time.

1.3 PKI participants

1.3.1 Certification authorities

Base Policy

Fortanix is the CA.

1.3.2 Registration authorities

Base Policy

No stipulation.

1.3.3 Subscribers

A Subscriber is a Fortanix DSM Cluster or Fortanix DSM SaaS that is authorized to use the Private Key that corresponds to the Public Key in the Certificate.

1.3.4 Relying parties

Base Policy

See Section 1.6

Such parties include, but aren't limited to:

- Fortanix DSM clusters that wish to obtain data from other Fortanix DSM clusters. For example, one or more of following use cases may apply:
  - Clusters that comprise Fortanix DSM SaaS are allowed to share a Fortanix Key Attestation Authority private key and its corresponding certificate. This exchange process requires that both sending and receiving sides cryptographically identify themselves to each other with their Service Certificates.
  - Additionally, for clusters that wish to make use of the Account Replication feature in Fortanix Data Security Manager, which allows transfer of objects between accounts (from a *source* cluster to a *destination* cluster), the source cluster must cryptographically identify itself to the destination using a service certificate. Likewise, the destination cluster may choose to identify itself to the source.
- The Fortanix Key Attestation CA (when deciding whether to issue Fortanix Key Attestation Authority certificates). Please refer to section 3.2.4 of the Fortanix Key Attestation PKI Certificate Policy for more information.

1.3.5 Other participants

Base Policy

No stipulation.

1.4 Certificate usage

1.4.1. Appropriate certificate uses

Base Policy

The primary goal of this PKI is to enable efficient and secure electronic Attestation, while addressing user concerns about the trustworthiness of such Attestations and related Certificates. This Certificate Policy also serves to inform users and help them to make informed decisions when relying on these Certificates.

1.4.2 Prohibited certificate uses

Base Policy

Certificates MAY not be used in any way that conflicts with the stipulations of this Certificate Policy.

1.5 Policy administration

1.5.1 Organization administering the document

Base Policy

The Fortanix security team maintains this document.

1.5.2 Contact person

Base Policy

Contact information for the Fortanix security team may be found at https://www.fortanix.com/security.txt.

1.5.3 Person determining CPS suitability for the policy

Base Policy

The Fortanix CISO SHALL review and approve the suitability of the CPS of any CA that issues Certificates under this CP.

1.5.4 CP approval procedures

Base Policy

The Fortanix CISO SHALL review and approve any amendments to this CP.

1.6 Definitions and acronyms

Base Policy

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. The coverage rules and maximum length of audit periods are defined in Section 8.1.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of this Certificate Policy

CA Key Pair: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Fortanix DSM Cluster: A collection of Fortanix Data Security Manager nodes that all adhere to the same security policy and that are collectively administered as an ensemble. A DSM cluster is identified by its cluster ID, a UUID.

Fortanix DSM SaaS: A collection of Fortanix DSM Clusters that have been designated by Fortanix as such and all adhere to the same security policy and are all administered by Fortanix.

Fortanix Service Certificate: A Certificate issued to a Fortanix DSM Cluster in the Fortanix Service Attestation PKI, a separate part of the Fortanix Attestation and Provisioning PKI.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.)

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy

Relying parties: Anyone who relies on a Valid Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage and/or Name Constraint extensions, as defined within the relevant Certificate Profiles of this document, to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Trustworthy System: 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

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280

Validation Specialist: Someone who performs the information verification duties specified by this Certificate Policy

Validity Period: From RFC 5280 (http://tools.ietf.org/html/rfc5280): "The period of time from notBefore through notAfter, inclusive."

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

For more information about Intel Software Guard Extensions and the terminology defined below, please refer to Intel documentation, such as the Intel Software Guard Extensions Programming Reference. Please note that Intel is a registred trademark of Intel Corporation.

Intel SGX Intel Software Guard Extensions, a set of CPU instruction codes available for certain Intel microprocessors to implement trusted execution environments.

Intel SGX enclave A protected area of memory in an application's memory address space, made available via Intel SGX.

MRENCLAVE The enclave build measurement value of an Intel SGX enclave (in this case, the Fortanix Data Security Manager software).

MRSIGNER The enclave signing identity that signed the Intel SGX enclave. In this case, the signer is Fortanix, and the enclave is the Fortanix Data Security Manager software.

ISVPRODID The product identifier assigned to the Intel SGX enclave (in this case, the Fortanix Data Security Manager software).

ISVSVN The security version number assigned to the Intel SGX enclave, which, in this case, is the Fortanix Data Security Manager Software.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Base Policy

All CAs in scope of this CP which are hosted and operated by Fortanix MUST make the CA certificates and accompanying revocation information (where applicable) available in a public Repository in accordance with this Policy.

2.2 Publication of certification information

Base Policy

The CA maintains controls to provide reasonable assurance that timely, complete and accurate certificate status information (including CRLs and other certificate status mechanisms) is made available to any entity in accordance with the CA's disclosed business practices.

The CA SHALL publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis.

The Certificate Policy and/or Certification Practice Statement SHALL be structured in accordance with RFC 3647 and SHALL include all material required by RFC 3647.

2.3 Time or frequency of publication

Base Policy

The CA SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements.

The CA SHALL indicate conformance with this requirement by incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

CRL requirements are described in section 4.9 of this CP.

2.4 Access controls on repositories

Base Policy

The CA SHALL make its Repository publicly available in a read-only manner. Access controls MUST be implemented to prevent unauthorized modification of the repository.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Base Policy

Names SHALL be compliant X.500 distinguished names. Subject Alternative Names (SAN) MAY be used.

3.1.2 Need for names to be meaningful

Base Policy

No stipulation.

3.1.3 Anonymity or pseudonymity of subscribers

No organizations or individuals are identified in end-entity certificates.

3.1.4 Rules for interpreting various name forms

Base Policy

No stipulation.

3.1.5 Uniqueness of names

Base Policy

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

Base Policy

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Base Policy

The issuance process SHALL involve procedures in which the subscriber demonstrates the possession of the Private Key using a method approved by the Issuing CA.

3.2.2 Authentication of organization identity

Base Policy

No stipulation.

3.2.3 Authentication of individual identity

Base Policy

No stipulation.

3.2.4 Authentication of machine identity

Base Policy

As described in Section 1.3.3, the Subscribers to which Certificates are issued under this policy are not organizations or individuals but are a machine identity. A Fortanix DSM Cluster SHALL identify itself by providing the following information in a Certificate Signing Request (CSR):

- The cluster ID of the Fortanix DSM Cluster in question
- The primary domain name used by Relying Parties to resolve the Fortanix Data Security Manager service running on the cluster

If the Fortanix DSM cluster is a part of Fortanix DSM SaaS, its cluster ID and primary domain will be checked against the list of known IDs and domain names for all Fortanix DSM clusters that make up Fortanix DSM SaaS.

Additionally, the DSM cluster MUST cryptographically prove its identity as a legitimate Fortanix Data Security Manager service. This can be done either via

- A valid Intel SGX attestation report indicating that the cluster is running a legitimate version of the Data Security Manager software, encoded as per 3.2.4.1, or
- The public TLS certificate corresponding to the DSM cluster in question

It is RECOMMENDED for a Subscriber to prove its identity via an Intel SGX attestation report.

If relying on an Intel SGX attestation report, the CA SHALL verify that the following properties in the report match with the generated values produced when Fortanix first built and signed the Fortanix Data Security Manager software that is currently running on the Fortanix DSM cluster.

- `MRENCLAVE`
- `MRSIGNER`
- `ISVPRODID`
- `ISVSVN`

Otherwise, if relying on a public TLS certificate, the CA SHALL establish a TLS connection with the Fortanix DSM cluster, using the public TLS certificate provided, and obtain a separate CSR for the Service Attestation PKI, hereafter referred to as the "TLS-validated CSR." The CA SHALL then verify that the public key and cluster ID present in the original CSR matches the public key and cluster ID, respectively, present in the "TLS-validated CSR." This check is sufficient to validate the identity of the Fortanix DSM cluster because the cluster ID will always be preserved across the lifetime of the cluster, and the public key present in any generated Service Attestation CSR only changes upon provisioning of a new Serivce Certificate. Hence, the cluster ID and public key from both the original CSR and the "TLS-validated CSR" should match.

3.2.4.1 CSR extension for storing Intel SGX attestation reports The following extension SHALL be used to encode a valid Intel SGX attestation report for the Fortanix Data Security Manager software running on the Fortanix DSM cluster:

Extension	Critical	OID	Value
`DCAP attestation node certificate`	NO	1.3.6.1.4.1.49690.2.2.5	A `DcapAttestation` value (see 3.2.4.2)

(Please note that older CSRs may include an `Intel Attestation Service (v2)` extension instead, which is no longer accepted by the CA.)

3.2.4.2 SGX report data types The following ASN.1 definitions comprise the `DcapAttestation` data type, along with some related types:

```
DcapAttestationQuote ::= SEQUENCE {
    -- If this is a quote with certification data type 5 (PCK certificate chain)
    -- the certification data shall be set to the empty byte array (truncated),
    -- and the certification data size shall be set to 0. The original
    -- certification data shall have the certificates parsed and added to the
    -- DcapAttestation certificate set.
    quote OCTET STRING,
    -- A list of indices into the DcapAttestation certificate set. This can be
    -- used to reconstruct the quote above.
    certificates SEQUENCE OF INTEGER
}

DcapAttestationSignedJson ::= SEQUENCE {
    -- the signed JSON response from the API
    json OCTET STRING,
    signature OCTET STRING,
    -- The index into the DcapAttestation certificate set of the signing
    -- certificate. Note: the exact chain is not included. The chain may be
    -- reconstructed by looking at the certificate issuers.
    certificate INTEGER
}

DcapAttestation ::= SEQUENCE {
    quote DcapAttestationQuote,
    -- DER-encoded CRL embedded directly as ASN.1 object
    tcbInfo DcapAttestationSignedJson,
    qe3Identity DcapAttestationSignedJson,
    processorCrl Crl,
    -- The set of certificates (embedded directly as ASN.1 objects) used
    -- for this attestation. Each unique certificate appears only once.
    certificates SEQUENCE OF Certificate
}
```

Information about Intel SGX Data Center Attestation Primitives (DCAP) can be found at https://download.01.org/intel-sgx/sgx-dcap/1.7/linux/docs/Intel_SGX_ECDSA_QuoteLibReference_DCAP_API.pdf.

In the above definitions, `Certificate` and `Crl` are ASN.1 structures as defined in RFC 5280.

3.2.5 Non-verified subscriber information

Base Policy

No stipulation.

3.2.6 Validation of authority

Base Policy

Validation of authority (i.e. the determination of whether an Applicant or Subscriber has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a Certificate) is the responsibility of the CA or CA-appointed Registration Authority (RA).

An authenticated Fortanix DSM Cluster is authorized to request a Certificate under this Certificate Policy for itself.

3.2.7 Criteria for interoperation

Base Policy

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Base Policy

See Section 4.7.

3.3.2 Identification and authentication for re-key after revocation

Base Policy

See Section 4.7.

3.4 Identification and authentication for revocation request

Base Policy

No stipulation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificate applications MAY be submitted to the CA by a Fortanix DSM Cluster.

4.1.2 Enrollment process and responsibilities

Base Policy

The enrollment process SHALL include the following steps:

- Generating a key pair using secure methods
- Submitting a request for a certificate containing the public key and any necessary information.

A Fortanix DSM Cluster SHALL submit a certificate request to the CA in an automated way defined by the CA.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Base Policy

The CA SHALL verify that

- the certificate application is intended for the CA
- the certificate application is authenticated by the subscriber

4.2.2 Approval or rejection of certificate applications

Base Policy

The CA SHALL verify that

- the subscriber is authorized to apply for a certificate in name of the subject mentioned in the certificate application
- the certificate application includes a proof of possession of the private key corresponding to the public key mentioned in the certificate application

4.2.3 Time to process certificate applications

Base Policy

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Base Policy

Certificate issuance by the Root CA SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Base Policy

No stipulation.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Base Policy

No stipulation.

4.4.2 Publication of the certificate by the CA

Base Policy

No stipulation.

4.4.3 Notification of certificate issuance by the CA to other entities

Base Policy

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The Subscriber private key MUST only be used for the following purposes:

- Signing a Subscriber's key attestation authority private key, if present
- Decrypting another Fortanix DSM cluster's key attestation authority key (encrypted with the public key associated with that cluster's service certificate)
- Establishing a TLS handshake with a Relying Party that wishes to utilize the Data Security Manager service running on the Subscriber
- Cryptographically identifiying the Subscriber to the Fortanix Key Attestation CA (please refer to section 3.2.4 of the Fortanix Key Attestation PKI Certificate Policy for more information)

4.5.2 Relying party public key and certificate usage

Base Policy

The Relying Parties SHALL ensure that a public key in a certificate is used only for the purposes indicated by the key usage extension and the extended key usage extension, if either of those extensions are present.

The Relying Parties SHALL ensure that a public key in a certificate is used only for the purposes indicated by the certificate policies the certification path is valid for. If the certification path is not valid for any policy (e.g., certificate policies extension is absent in a certificate in the certification path or there is no policy OID common to all the certificates in the certification path after considering policy mapping), the Relying Party SHALL reject the certificate.

4.6 Certificate renewal

Base Policy

Certificate renewal requests are treated as applications for new certificates.

4.6.1 Circumstance for certificate renewal

Base Policy

No stipulation.

4.6.2 Who may request renewal

Base Policy

No stipulation.

4.6.3 Processing certificate renewal requests

Base Policy

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

Base Policy

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

Base Policy

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

Base Policy

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

Base Policy

No stipulation.

4.7 Certificate re-key

Base Policy

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

4.7.1 Circumstance for certificate re-key

Base Policy

No stipulation.

4.7.2 Who may request certification of a new public key

Base Policy

No stipulation.

4.7.3 Processing certificate re-keying requests

Base Policy

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

Base Policy

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Base Policy

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

Base Policy

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

Base Policy

No stipulation.

4.8 Certificate modification

Base Policy

Certificate modification requests are treated as applications for new certificates.

4.8.1 Circumstance for certificate modification

Base Policy

No stipulation.

4.8.2 Who may request certificate modification

Base Policy

No stipulation.

4.8.3 Processing certificate modification requests

Base Policy

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

Base Policy

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

Base Policy

No stipulation.

4.8.6 Publication of the modified certificate by the CA

Base Policy

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

Base Policy

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Base Policy

4.9.1.1 Reasons for revoking a certificate The CA SHALL revoke a Certificate within 24 hours and use the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

1. The Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 (CRLReason #1, keyCompromise);
2. The CA is made aware of a demonstrated or proven method that can easily compute the Certificate's Private Key based on the Public Key in the Certificate (CRLReason #1, keyCompromise);

The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days and use the corresponding CRLReason if one or more of the following occurs:

3. Fortanix no longer uses the service the certificate/CA is issued for. (CRLReason #5, cessationOfOperation);
4. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 (CRLReason #4, superseded);
5. The CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
6. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
7. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement CRLReason #4, superseded;
8. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
9. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement for a reason that is not otherwise required to be specified by this Section 4.9.1.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or
11. The CA is made aware of a demonstrated or proven method that exposes the Certificate's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

4.9.1.2 Reasons for revoking a subordinate certificate The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation because Fortanix no longer uses the service the CA is issued for;
2. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
3. The Issuing CA obtains evidence that the Certificate was misused;

4. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
5. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
6. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
7. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirments expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
8. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement

4.9.2 Who can request revocation

Base Policy

The Issuing CA can initiate revocation. Additionally, Relying Parties, and other third parties MAY submit Certification Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for revocation request

Base Policy

The CA SHALL provide Relying Parties and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates.

The CA SHALL publicly disclose the instructions through a readily accessible online means and in Section 1.5.2 of their CPS.

4.9.4 Revocation request grace period

Base Policy

No stipulation.

4.9.5 Time within which CA must process the revocation request

Base Policy

Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the CA SHALL work with any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate.

The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed 24 hours. The date selected by the CA SHOULD consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;

4. The entity making the complaint (for example, a complaint from a law enforcement official that a Website is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
5. Relevant legislation.

4.9.6 Revocation checking requirement for relying parties

Base Policy

No stipulation.

4.9.7 CRL issuance frequency (if applicable)

Base Policy

Fortanix CA will update and reissue CRLs for Subordinate CA Certificates with a frequency greater than or equal to once every 12 months OR within 24 hours after revoking a Subordinate CA Certificate. The value of the `nextUpdate` field MUST NOT be more than twelve months beyond the value of the `thisUpdate` field.

4.9.8 Maximum latency for CRLs (if applicable)

Base Policy

Regularly scheduled CRLs are posted prior to the next Update field in the previously issued CRL of the same scope.

4.9.9 On-line revocation/status checking availability

Base Policy

No stipulation.

4.9.10 On-line revocation checking requirements

Base Policy

No stipulation.

4.9.11 Other forms of revocation advertisements available

Base Policy

No stipulation.

4.9.12 Special requirements re key compromise

Base Policy

See Section 4.9.1.

4.9.13 Circumstances for suspension

Base Policy

No stipulation.

4.9.14 Who can request suspension

Base Policy

No stipulation.

4.9.15 Procedure for suspension request

Base Policy

No stipulation.

4.9.16 Limits on suspension period

Base Policy

No stipulation.

4.10 Certificate status services

4.10.1 Operational characteristics

Base Policy

Revocation entries on a CRL MUST NOT be removed until after the Expiry Date of the revoked Certificate.

4.10.2 Service availability

Base Policy

The CA SHALL operate and maintain its CRL with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Optional features

Base Policy

No stipulation.

4.11 End of subscription

Base Policy

No stipulation.

4.12 Key escrow and recovery

Base Policy

Key escrow SHALL NOT be used for any private key covered by this Certificate Policy.

4.12.1 Key escrow and recovery policy and practices

Base Policy

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

Base Policy

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Base Policy

The Fortanix Security Policy applies to Fortanix managed CAs in conjunction with the requirements below.

The CA SHALL develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process MUST include:

1. physical security and environmental controls;
2. system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, separate trusted-role assignments, education, awareness, and training; and
5. logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The CA's security program MUST include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

The security plan MUST include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST also take into account then-available technology and the cost of implementing the specific measures, and SHALL implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical controls

5.1.1 Site location and construction

Base Policy

No stipulation.

5.1.2 Physical access

Base Policy

No stipulation.

5.1.3 Power and air conditioning

Base Policy

No stipulation.

5.1.4 Water exposures

Base Policy

No stipulation.

5.1.5 Fire prevention and protection

Base Policy

No stipulation.

5.1.6 Media storage

Base Policy

No stipulation.

5.1.7 Waste disposal

Base Policy

No stipulation.

5.1.8 Off-site backup

Base Policy

No stipulation.

5.2 Procedural controls

5.2.1 Trusted roles

Base Policy

Each CA SHALL follow a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them.

Each CA SHALL grant administration access to Certificate Systems only to persons acting in Trusted Roles and require their accountability for the Certificate System's security.

5.2.2 Number of persons required per task

Base Policy

All operations related to the CA private key(s) SHALL be performed under at least dual control by persons acting in Trusted Roles. The dual control SHALL be enforced via a HSM backed Quorum Approval process.

5.2.3 Identification and authentication for each role

Base Policy

Each CA SHALL require that each individual in a Trusted Role use a unique credential created by or assigned to that person in order to authenticate to Certificate Systems

5.2.4 Roles requiring separation of duties

Base Policy

Each CA SHALL document the responsibilities and tasks assigned to Trusted Roles. The CA SHALL implement "separation of duties" using a Quorum Approval process if deemed necessary for such Trusted Roles based on the security-related concerns of the functions to be performed.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Base Policy

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, the CA SHALL verify the identity and trustworthiness of such person.

5.3.2 Background check procedures

Base Policy

No stipulation.

5.3.3 Training requirements

Base Policy

The CA SHALL ensure all personal in a Trusted Role is familiar with basic PKI knowledge, known threats, policies and procedures (including the CP, CPS and Fortanix Security Policy) and these Requirements.

5.3.4 Retraining frequency and requirements

Base Policy

All personnel in Trusted roles SHALL maintain skill levels consistent with the training requirements.

5.3.5 Job rotation frequency and sequence

5.3.6 Sanctions for unauthorized actions

Base Policy

The CA MUST maintain controls to provide reasonable assurance that compliance with the CA's security policies and procedures is ensured.

Each CA SHALL ensure that an individual in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role.

5.3.7 Independent contractor requirements

Base Policy

No stipulation.

5.3.8 Documentation supplied to personnel

Base Policy

No stipulation.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Base Policy

The CA SHALL record events related to the security of their Certificate Systems, Certificate Management Systems and Root CA Systems. The CA SHALL record events related to their actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. The CA SHALL make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

The CA SHALL record at least the following events:

1. CA certificate and key lifecycle events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction;
    b. Certificate requests, renewal, and re-key requests, and revocation;
    c. Approval and rejection of certificate requests;
    d. Cryptographic device lifecycle management events;
    e. Generation of Certificate Revocation Lists (CRL)
    f. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes
    d. Installation, update and of software on a Certificate System;
    e. System crashes, hardware failures, and other anomalies;
    f. Firewall and router activities; and
    g. Entries to and exits from the CA facility

Log records MUST include the following elements:

1. Date and time of event;
2. Identity of the person making the journal record; and
3. Description of the event.

5.4.2 Frequency of processing log

Base Policy

No stipulation.

5.4.3 Retention period for audit log

Base Policy

The CA SHALL retain, for at least two (2) years:

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of:
   a. the destruction of the CA Private Key; or
   b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 `basicConstraints` extension with the `cA` field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Any security event records (as set forth in Section 5.4.1 (2)) after the event occurred.

Note: While these Requirements set the minimum retention period, the CA MAY choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past audit log events

5.4.4 Protection of audit log

Base Policy

No stipulation.

5.4.5 Audit log backup procedures

Base Policy

No stipulation.

5.4.6 Audit collection system (internal vs. external)

Base Policy

No stipulation.

5.4.7 Notification to event-causing subject

Base Policy

No stipulation.

5.4.8 Vulnerability assessments

Base Policy

Additionally, the CA's security program MUST include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.5 Records archival

5.5.1 Types of records archived

Base Policy

The CA SHALL archive all audit logs (as set forth in Section 5.4.1).

Additionally, the CA SHALL archive:

1. Documentation related to the security of their Certificate Systems, Certificate Management Systems and Root CA Systems; and
2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

5.5.2 Retention period for archive

Base Policy

Archived audit logs (as set forth in Section 5.5.1) SHALL be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

Note: While these Requirements set the minimum retention period, the CA MAY choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past records archived.

5.5.3 Protection of archive

Base Policy

No stipulation.

5.5.4 Archive backup procedures

Base Policy

No stipulation.

5.5.5 Requirements for time-stamping of records

Base Policy

No stipulation.

5.5.6 Archive collection system (internal or external)

Base Policy

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Base Policy

No stipulation.

5.6 Key changeover

Base Policy

No stipulation.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Base Policy

CA organizations SHALL have an Incident Response Plan and a Disaster Recovery Plan.

The CA SHALL document a business continuity and disaster recovery procedures designed to notify Relying Parties in the event of a disaster, security compromise, or business failure. The CA is not required to publicly disclose its business continuity plans but SHALL make its business continuity plan and security plans available to the CA's auditors upon request. The CA SHALL annually test, review, and update these procedures.

The business continuity plan SHALL include:

1. The conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Resumption procedures;
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans;
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site

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

Base Policy

No stipulation.

5.7.3 Entity private key compromise procedures

Base Policy

No stipulation.

5.7.4 Business continuity capabilities after a disaster

Base Policy

No stipulation.

5.8 CA or RA termination

Base Policy

No stipulation.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Base Policy

For CA Key Pairs that are used as a CA Key Pair for a Root Certificate the CA SHALL:

1. prepare and follow a Key Generation Script,
2. have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process, and
3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs the CA SHOULD:

1. prepare and follow a Key Generation Script and
2. have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process.

In all cases, the CA SHALL:

1. generate the CA Key Pair in a physically secured environment as described in the CA's Certificate Policy and/or Certification Practice Statement;
2. generate the CA Key Pair using personnel in Trusted Roles while under witness by the Qualified Auditor.
3. generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement;
4. log its CA Key Pair generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

A Fortanix DSM Cluster SHALL generate and store the private key itself.

6.1.2 Private key delivery to subscriber

Base Policy

No stipulation.

6.1.3 Public key delivery to certificate issuer

Base Policy

No stipulation.

6.1.4 CA public key delivery to relying parties

Base Policy

No stipulation.

6.1.5 Key sizes

Base Policy

6.1.5.1 Root and Subordinate CA key sizes For Keys corresponding to Root and Subordinate CAs:

- If the Key is RSA, then the modulus MUST be at least 4096 bits in length.
- If the Key is ECDSA, then the curve MUST be one of NIST P-256, P-384, or P-521.

6.1.5.2 Attestation and other Certificate key sizes For Keys corresponding to generating Attestations or other Certificates in the CA:

- If the Key is RSA, then the modulus MUST be at least 3072 bits in length.
- If the Key is ECDSA, then the curve MUST be one of NIST P-256, P-384, or P-521.

6.1.6 Public key parameters generation and quality checking

Base Policy

The CA shall validate public key parameters according to NIST Special Publication 800-89 "Recommendation for Obtaining Assurances for Digital Signature Applications", chapter 4.

The CA shall validate public keys using explicit validation according to NIST Special Publication 800-89 "Recommendation for Obtaining Assurances for Digital Signature Applications", chapter 5.

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

Base Policy

Private Keys corresponding to Root Certificates MUST NOT be used to sign Certificates or create other Signatures except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates);
4. Certificates for OCSP Response verification; and
5. Signatures for OCSP Responses.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Base Policy

The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. The CA SHALL encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic module standards and controls

Base Policy

No stipulation.

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

Base Policy

No stipulation.

6.2.3 Private key escrow

Base Policy

No stipulation.

6.2.4 Private key backup

Base Policy

CA private keys SHALL be stored in Fortanix DSM SaaS to ensure availability.

6.2.5 Private key archival

Base Policy

The CA SHALL not archive the private key outside the cryptographic module as set in Section 6.2.7.

6.2.6 Private key transfer into or from a cryptographic module

Base Policy

No stipulation.

6.2.7 Private key storage on cryptographic module

Base Policy

CA private keys SHALL be created, stored, and used in Fortanix DSM SaaS and will remain within the security boundaries of the solution's hardware cryptography module.

6.2.8 Method of activating private key

Base Policy

No stipulation.

6.2.9 Method of deactivating private key

Base Policy

No stipulation.

6.2.10 Method of destroying private key

Base Policy

No stipulation.

6.2.11 Cryptographic Module Rating

Base Policy

No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Base Policy

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

Base Policy Root CA certificates SHOULD NOT have a Validity Period greater than 10 years. Subordinate CA Certificates issued SHOULD NOT have a Validity Period greater than 3 years. Certificates issued SHOULD NOT have a Validity Period greater than 95 days.

6.4 Activation data

6.4.1 Activation data generation and installation

Base Policy

No stipulation.

6.4.2 Activation data protection

Base Policy

No stipulation.

6.4.3 Other aspects of activation data

Base Policy

No stipulation.

6.5 Computer security controls

Base Policy

The CA MUST maintain controls to provide reasonable assurance that compromise of information and information processing facilities is prevented.

The CA MUST maintain controls to provide reasonable assurance that the risk of CA systems failure is minimized.

6.5.1 Specific computer security technical requirements

Base Policy

The CA SHALL enforce multi-factor authentication for all trusted persons capable of directly causing certificate issuance.

6.5.2 Computer security rating

Base Policy

No stipulation.

6.6 Life cycle technical controls

Base Policy

No stipulation.

6.6.1 System development controls

Base Policy

No stipulation.

6.6.2 Security management controls

Base Policy

No stipulation.

6.6.3 Life cycle security controls

Base Policy

No stipulation.

6.7 Network security controls

Base Policy

No stipulation.

6.8 Time-stamping

Base Policy

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Base Policy

The CA SHALL meet the technical requirements set forth in Section 2.2 - Publication of Information, Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking.

The CA SHALL issue Certificates in accordance with the profile specified in these Requirements.

7.1.1 Version number(s)

Base Policy

Certificates MUST be of type X.509 v3.

7.1.2 Certificate extensions

Base Policy

All certificates that the CA issues MUST comply with one of the following certificate profiles, which incorporate, and are derived from RFC 5280. Except as explicitly noted, all normative requirements imposed by RFC 5280 SHALL apply, in addition to the normative requirements imposed by this document. CAs SHOULD examine RFC 5280, Appendix B for further issues to be aware of.

7.1.2.1 Common CA Fields This section contains several fields that are common among multiple CA Certificate profiles. However, these fields MAY not be common among all CA Certificate profiles. Before issuing a certificate, the CA MUST ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.1.1 CA Certificate Validity

Field	Minimum	Maximum
`notBefore`	One day prior to the time of signing	The time of signing
`notAfter`	The time of signing	Unspecified

7.1.2.1.3 CA Certificate Basic Constraints

Field	**Description**
`cA`	MUST be set TRUE
`pathLenConstraint`	MAY be present

7.1.2.1.4 CA Certificate Certificate Policies If present, the Certificate Policies extension MUST contain at least one `PolicyInformation`. Each `PolicyInformation` MUST match the following profile:

Table 6: Policy Restricted

Field	Presence	Contents
`policyIdentifier`	MUST	The following identifier
`Reserved Certificate Policy Identifier`	MUST	OID as in Reserved Certificate Policy Identifier
`policyQualifiers`	MUST NOT	

7.1.2.1.5 CA Certificate Key Usage

Key Usage	Permitted	Required
`digitalSignature`	Y	N[1]
`nonRepudiation`	N	–
`keyEncipherment`	N	–
`dataEncipherment`	N	–
`keyAgreement`	N	–
`keyCertSign`	Y	Y
`cRLSign`	Y	Y
`encipherOnly`	N	–
`decipherOnly`	N	–

7.1.2.1.6 Subject Key Identifier If present, the subjectKeyIdentifier MUST be set as defined within RFC 5280, Section 4.2.1.2. The CA MUST generate a subjectKeyIdentifier that is unique within the scope of all Certificates it has issued for each unique public key (the subjectPublicKeyInfo field of the tbsCertificate). For example, CAs may generate the subject key identifier using an algorithm derived from the public key, or may generate a sufficiently-large unique number, such by using a CSPRNG.

The sections below are an extension to the Base Certificate Policy.

7.1.2.1 Fortanix Service Attestation Subordinate Certificate Authorities Base requirements for the Subordinate Certificate Authorities of the Attestation and Provisioning Root CA in addition to 7.1.2 common fields and requirements.

Field	Description
`tbsCertificate`	
`version`	MUST be v3(2)
`serialNumber`	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
`signature`	See Section 7.1.3.2
`issuer`	MUST be byte-for-byte identical to the `subject` field of the Issuing CA.
`validity`	See authority specific section
`subject`	See Section 7.1.4.4
`subjectPublicKeyInfo`	See Section 7.1.3.1
`issuerUniqueID`	MUST NOT be present
`subjectUniqueID`	MUST NOT be present
`extensions`	See authority specific section

[1] If a CA Certificate does not assert the `digitalSignature` bit, the CA Private Key MUST NOT be used to sign an OCSP Response.

Field	Description
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
`signature`	

7.1.2.1.1 Common Certificate Authorities Extensions

Extension	Critical	OID	Value
`certificatePolicies`	NO	2.5.29.32	See Base CP Section CA Certificate Certificate Policies. Use ONLY the OID defined in Section 7.1.6.1
`basicConstraints`	YES	2.5.29.19	See Base CP Section CA Certificate Basic Constraints
`keyUsage`	YES	2.5.29.15	See Base CP Section CA Certificate Key Usage
`authorityKeyIdentifier`	NO	2.5.29.35	See 7.1.2.1.2

7.1.2.1.2 Common Authorities Key Identifier

Field	Description
`keyIdentifier`	MUST be present. MUST be identical to the subjectKeyIdentifier field of the Issuing CA
`authorityCertIssuer`	MUST NOT be present
`authorityCertSerialNumber`	MUST NOT be present

7.1.2.2 Fortanix Service Attestation CA Extends the 7.1.2.1 common fields.

7.1.2.2.1 Fortanix Service Attestation CA Extensions

Extension	Critical	OID	Value
`cRLDistributionPoints`	NO	2.5.29.31	It MUST contain the HTTP URL of the issuer's CRL service

7.1.2.2.2 Fortanix Service Attestation CA Validity

Field	Minimum	Maximum
`notBefore`	One day prior to the time of signing	The time of signing
`notAfter`	1096 days (approx. 3 years)	1096 days (approx. 3 years)

7.1.2.3 Fortanix Service Certificate Base requirements for a Fortanix Service Certificate. Note that the certificate has a different subject depending on if it is issued for Fortanix Data Security Manager SaaS (see 7.1.4.4.1) or for non-SaaS (see 7.1.4.4.2).

Field	Description
`tbsCertificate`	
`version`	MUST be v3(2)
`serialNumber`	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.

Field	Description
signature	See 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA.
validity	See 7.1.2.3.6
subject	See 7.1.4.4.1 or 7.1.4.4.2
subjectPublicKeyInfo	See 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See 7.1.2.3.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.3.1 Fortanix DSM Service Certificate extensions Note that the certificate has a different value of the keyUsage extension depending on if it is issued for Fortanix Data Security Manager SaaS (see 7.1.2.3.2) or for non-SaaS (see 7.1.2.3.3).

Extension	Critical	OID	Value
keyUsage	YES	2.5.29.15	See 7.1.2.3.2 or 7.1.2.3.3
subjectAltName	NO	2.5.29.17	See Section 7.1.2.3.4
extKeyUsage	NO	2.5.29.37	See Section 7.1.2.3.5
cRLDistributionPoints	NO	2.5.29.31	It MUST contain the HTTP URL of the issuer's CRL service
certificatePolicies	NO	2.5.29.32	Use ONLY the OID defined in Section 7.1.6.1

7.1.2.3.2 Fortanix DSM SaaS Service Certificate keyUsage extension

Key Usage	OID	Permitted	Required
digitalSignature	2.5.29.15.0	Y	Y
keyEncipherment	2.5.29.15.2	Y	Y

7.1.2.3.3 Fortanix DSM Service Certificate keyUsage extension

Key Usage	OID	Permitted	Required
digitalSignature	2.5.29.15.0	Y	Y

7.1.2.3.4 Fortanix Service Certificate subjectAltName extension The subjectAltName Fortanix Service Certificate contains a single subject identity, which is the primary domain name used by Relying Parties to resolve the Fortanix Data Security Manager service running on the cluster for which the service certificate is issued. This domain name is encoded as a dNSName as per RFC 5280.

7.1.2.3.5 Fortanix Service Certificate extKeyUsage extension

Key Usage	OID	Permitted	Required
serverAuth	1.3.6.1.5.5.7.3.1	Y	Y
clientAuth	1.3.6.1.5.5.7.3.2	Y	Y
id-kp-fortanix-service-attestation	1.3.6.1.4.1.49690.8.2	Y	Y

7.1.2.3.6 Fortanix Service Certificate Lifetime

Field	Minimum	Maximum
`notBefore`	One day prior to the time of signing	The time of signing
`notAfter`	The time of signing	30 days from the time of signing

7.1.3 Algorithm object identifiers

Base Policy

7.1.3.1 SubjectPublicKeyInfo As defined in Section 6.1.5.

7.1.3.2 Signature AlgorithmIdentifier All objects signed by a CA Private Key MUST conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The signatureAlgorithm field of a Certificate.
- The signature field of a TBSCertificate.
- The signatureAlgorithm field of a CertificateList
- The signature field of a TBSCertList
- The signatureAlgorithm field of a BasicOCSPResponse
- The digestAlgorithms field of a SignedData corresponding to a Timestamp token

7.1.3.2.1 RSA The CA SHALL use one of the following signature algorithms:

- RSASSA-PKCS1-v1_5 with SHA-256
- RSASSA-PKCS1-v1_5 with SHA-384
- RSASSA-PKCS1-v1_5 with SHA-512
- RSASSA-PSS with SHA-256
- RSASSA-PSS with SHA-384
- RSASSA-PSS with SHA-512

7.1.3.2.2 ECDSA The CA SHALL use one of the following signature algorithms:

- ECDSA with SHA-256
- ECDSA with SHA-384
- ECDSA with SHA-512

7.1.3.1 SubjectPublicKeyInfo

7.1.3.2 Signature AlgorithmIdentifier

7.1.3.2.1 RSA

7.1.3.2.2 ECDSA

7.1.4 Name forms

Base Policy

This section details encoding rules that apply to all Certificates issued by a CA. Further restrictions may be specified within Section 7.1.2, but these restrictions do not supersede these requirements.

7.1.4.1 Name Encoding The following requirements apply to all Certificates listed in Section 7.1.2. Specifically, this includes Subordinate CA Certificates, but does not include certificates issued by such CA Certificate.

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate SHALL be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

When encoding a `Name`, the CA SHALL ensure that:

- Each `Name` MUST contain an `RDNSequence`.
- Each `RelativeDistinguishedName` MUST contain exactly one `AttributeTypeAndValue`.
- Each `RelativeDistinguishedName`, if present, is encoded within the `RDNSequence` in the order that it appears in Section 7.1.4.2.
  - For example, a `RelativeDistinguishedName` that contains a `countryName AttributeTypeAndValue` pair MUST be encoded within the `RDNSequence` before a `RelativeDistinguishedName` that contains a `stateOrProvinceName AttributeTypeAndValue`.
- Each `Name` MUST NOT contain more than one instance of a given `AttributeTypeAndValue` across all `RelativeDistinguishedName`s unless explicitly allowed in these Requirements.

7.1.4.2 Subject Attribute Encoding This document defines requirements for the content and validation of a number of attributes that may appear within the `subject` field of a `tbsCertificate`. CAs SHALL NOT include these attributes unless their content has been validated as specified by, and only if permitted by, the relevant certificate profile specified within Section 7.1.4.4.

CAs that include attributes in the Certificate `subject` field that are listed in the table below SHALL encode those attributes in the relative order as they appear in the table and follow the specified encoding requirements for the attribute.

Table 19: Encoding and Order Requirements for Selected Attributes

Attribute	OID	Specification	Encoding Requirements	Max Length[2]
`domainComponent`	`0.9.2342.19200300.100.1.25`	RFC 4519	MUST use `IA5String`	63
`countryName`	`2.5.4.6`	RFC 5280	MUST use `PrintableString`	2
`stateOrProvinceName`	`2.5.4.8`	RFC 5280	MUST use `UTF8String` or `PrintableString`	128
`localityName`	`2.5.4.7`	RFC 5280	MUST use `UTF8String` or `PrintableString`	128
`organizationName`	`2.5.4.10`	RFC 5280	MUST use `UTF8String` or `PrintableString`	64

Attribute	OID	Specification	Encoding Requirements	Max Length
organizationalUnitName	2.5.4.11	RFC 5280	MUST use UTF8String or PrintableString	64
commonName	2.5.4.3	RFC 5280	MUST use UTF8String or PrintableString	64
Cluster ID	1.3.6.1.4.1.49690.1.4.1	Fabrix	MUST use UTF8String	36

CAs that include attributes in the Certificate subject field that are listed in the table below SHALL follow the specified encoding requirements for the attribute.

Table 20: Encoding Requirements for Selected Attributes

Attribute	OID	Specification	Encoding Requirements	Max Length[3]
serialNumber	2.5.4.5	RFC 5280	MUST use PrintableString	64
organizationIdentifier	2.5.4.97	X.520	MUST use UTF8String or PrintableString	None

7.1.4.3 Other Subject Attributes When explicitly stated as permitted by the relevant certificate profile specified within Section 7.1.2, CAs MAY include additional attributes within the AttributeTypeAndValue beyond those specified in Section 7.1.4.2.

Before including such an attribute, the CA SHALL:

- Document the attributes within Section 7.1.4 of their CP or CPS, along with the applicable validation practices.
- Ensure that the contents contain information that has been verified by the CA, independent of the Applicant.

7.1.4.4 Required subject attributes The following attributes SHALL be included in the CA's subject unless noted otherwise in the certificate profile or naming requirements.

All subject names MUST be encoded as specified in Section 7.1.4.1 and Section 7.1.4.2.

The following table details the acceptable AttributeTypes that MAY appear within the type field of an AttributeTypeAndValue, as well as the contents permitted within the value field.

Attribute Name	Presence	Value	Verification
countryName	MUST	The two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.	Section 3.2.2.3
stateOrProvinceName	MUST	The CA's state or province information.	Section 3.2.2.1
localityName	MUST	The CA's locality.	Section 3.2.2.1

[2]**Note**: ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits.
[3]**Note**: ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits.

Attribute Name	Presence	Value	Verification
`organizationName`	MUST	The CA's name. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name".	Section 3.2.2.2
`organizationalUnitName`	MUST NOT	-	-
`commonName`	MUST	The contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.3

7.1.4.1 Name Encoding

7.1.4.2 Subject Attribute Encoding

7.1.4.3 Other Subject Attributes

7.1.4.4 Required subject attributes All `subject` names MUST be encoded as specified in Section 7.1.4.1 and Section 7.1.4.2.

7.1.4.4.1 Fortanix DSM SaaS Service Certificate The following subject attributes SHALL be included in a Fortanix DSM SaaS Service Certificate:

Attribute	OID	Value
`commonName`	2.5.4.3	`Fortanix DSM SaaS`
`Cluster ID`	1.3.6.1.4.1.49690.1.4.1	Subject/Subscriber DSM Cluster's UUID

7.1.4.4.2 Fortanix DSM Service Certificate The following subject attributes SHALL be included in a Fortanix DSM Service Certificate:

Attribute	OID	Value
`commonName`	2.5.4.3	`Fortanix DSM`
`Cluster ID`	1.3.6.1.4.1.49690.1.4.1	Subject/Subscriber DSM Cluster's UUID

7.1.5 Name constraints

Base Policy

No stipulation.

7.1.6 Certificate policy object identifier

Base Policy

7.1.6.1 Reserved Certificate Policy Identifiers The following Certificate Policy Identifier is reserved for use by CAs as a required means of asserting compliance with these Requirements. This document is assigned to the Fortanix Base Certificate Policy OID: `1.3.6.1.4.1.49690.6.1`

7.1.6.2 Root CA Certificates A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

7.1.6.3 Subordinate CA Certificates A Subordinate CA MUST represent, in its Certificate Policy and/or Certification Practice Statement, that all Certificates containing a policy identifier indicating compliance with these Requirements are issued and managed in accordance with these Requirements.

7.1.6.1 Reserved Certificate Policy Identifiers The following Certificate Policy Identifier is reserved for use by CAs as a required means of asserting compliance with these Requirements. This document is assigned to the Fortanix Service Certificate Policy OID: `1.3.6.1.4.1.49690.6.1.3`.

7.1.6.2 Root CA Certificates A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

7.1.6.3 Subordinate CA Certificates

7.1.7 Usage of Policy Constraints extension

Base Policy

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

Base Policy

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

Base Policy

No stipulation.

7.2 CRL profile

Base Policy

CAs under this CP SHALL publish CRLs in accordance with CP requirements.

7.2.1 Version number(s)

Base Policy

The CA SHALL issue X.509 v2 CRLs.

7.2.2 CRL and CRL entry extensions

Base Policy

The CA SHALL include the `reasonCode` extension in their CRL entries to identify the reason for the certificate revocation.

7.3 OCSP profile

Base Policy

No stipulation.

7.3.1 Version number(s)

Base Policy

No stipulation.

7.3.2 OCSP extensions

Base Policy

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Base Policy

The CA SHALL at all times:

1. Comply with these Requirements;
2. Comply with the audit requirements set forth in this section.

8.1 Frequency or circumstances of assessment

Base Policy

Certificates that are capable of being used to issue new certificates MUST be fully audited in line with all remaining requirements from this section. A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 `basicConstraints` extension, with the `cA` boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.4, then no pre-issuance readiness assessment is necessary.

8.2 Identity/qualifications of assessor

Base Policy

The CA's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in Section 8.4;
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function.

8.3 Assessor's relationship to assessed entity

Base Policy

The compliance auditor SHALL be independent from the Persons in Trusted Roles of the CA.

8.4 Topics covered by assessment

Base Policy

The purpose of a compliance audit SHALL be to verify that a CA complies with all of the requirements of the current version of this CP and the CA's CPS.

The audit MUST be conducted by a Qualified Auditor, as specified in Section 8.2.

8.5 Actions taken as a result of deficiency

Base Policy

The following actions SHALL be performed when the Qualified Auditor finds a non-conformity in the requirements of this CP, the CA's CPS or in the operation, or maintenance of the CAs:

1. Note the non conformity in the Audit Report;

2. Notify the responsible party involved with the operation of the CA of the non-conformity;
3. The responsible party SHALL provide a remediation plan, which included an expected time to resolution.

Depending on the risk that the non-conformity poses, the CA maintainer MAY decide to revoke a Certificate issued by the CA.

8.6 Communication of results

Base Policy

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1. The CA SHALL make the Audit Report publicly available

The CA MUST make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, the CA SHALL provide an explanatory letter signed by the Qualified Auditor.

The Audit Report MUST contain at least the following clearly-labelled information:

1. name of the organization being audited;
2. name and address of the organization performing the audit;
3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross-Certified Subordinate CA Certificates, that were in-scope of the audit;
4. that the certificates comply with applicable policies;
5. a list of the CA policy documents, with version numbers, referenced during the audit;
6. whether the audit assessed a period of time or a point in time;
7. the start date and end date of the Audit Period, for those that cover a period of time;
8. the point in time date, for those that are for a point in time;
9. the date the report was issued, which will necessarily be after the end date or point in time date.

An authoritative English language version of the publicly available audit information MUST be provided by the Qualified Auditor and the CA SHALL ensure it is publicly available.

The Audit Report MUST be available as a PDF, and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report MUST be uppercase letters and MUST NOT contain colons, spaces, or line feeds.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Base Policy

No stipulation.

9.1.2 Certificate access fees

Base Policy

No stipulation.

9.1.3 Revocation or status information access fees

Base Policy

No stipulation.

9.1.4 Fees for other services

Base Policy

No stipulation.

9.1.5 Refund policy

Base Policy

No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

Base Policy

Fortanix maintains reasonable levels of insurance coverage as required by applicable laws.

9.2.2 Other assets

Base Policy

Fortanix maintains sufficient financial resources to maintain operations and fulfill its obligations under this CP.

9.2.3 Insurance or warranty coverage for end-entities

Base Policy

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Base Policy

The following information is considered confidential information of Fortanix and is protected against disclosure using a reasonable degree of care:

- Private Keys;

- Account Data to manage the private keys in the key management system;
- Security Policy, Business continuity, incident response, contingency, and disaster recovery plans;
- Other security practices used to protect the confidentiality, integrity, or availability of information;
- Audit logs and archive records; and
- Transaction records, financial audit records, and external or internal audit trail records.

9.3.2 Information not within the scope of confidential information

Base Policy

No stipulation.

9.3.3 Responsibility to protect confidential information

Base Policy

No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

Base Policy

No stipulation.

9.4.2 Information treated as private

Base Policy

No stipulation.

9.4.3 Information not deemed private

Base Policy

No stipulation.

9.4.4 Responsibility to protect private information

Base Policy

No stipulation.

9.4.5 Notice and consent to use private information

Base Policy

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

Base Policy

No stipulation.

9.4.7 Other information disclosure circumstances

Base Policy

No stipulation.

9.5 Intellectual property rights

Base Policy

The following are the property of Fortanix:

- This CP,
- Any and all policies and procedures supporting the operation of the PKI services,
- The Certificates and CRLs and/or OCSP responses issued by Fortanix PKI services,
- CA infrastructure relevant to this CP.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Base Policy

Fortanix makes the following limited warranties with respect to the operation of the CAs. A CA shall:

i. provide CA services in accordance with the CPS;

ii. upon receipt of a request from an RA operating under such CA, issue a Certificate in accordance with the practices and procedures set forth in the CPS;

iii. make available Certificate revocation information by issuing Certificates and by issuing and making available Certificate CRLs and/or OCSP responses in a Repository in accordance with the CPS;

iv. issue and publish Certificate CRLs and/or OCSP responses on a regular schedule in accordance with the CPS;

v. provide revocation services consistent with the procedures set forth in the CPS; and

vi. provide Repository services consistent with the practices and procedures set forth in the CPS.

In operating the CAs, Fortanix may use one or more representatives or agents to perform its obligations under the CPS, provided that Fortanix shall remain responsible only for its performance

In no event does the Fortanix Group make any representations or warranties to any Applicants, Subscribers, Relying Parties, or any other persons, entities, or organizations with respect to (i) the techniques used by any party other than Fortanix in the generation and storage of the Private Key corresponding to the Public Key in a Certificate, including, but not limited to whether such Private Key has been compromised or was generated using proper cryptographic techniques, (ii) the reliability of any techniques or methods used in any act, transaction, or process involving or utilizing a Certificate, or (iii) the non-repudiation of any Certificate or any transaction facilitated through or by the use of a Certificate.

9.6.2 RA representations and warranties

Base Policy

No stipulation.

9.6.3 Subscriber representations and warranties

Base Policy

No stipulation.

9.6.4 Relying party representations and warranties

Base Policy

No stipulation.

9.6.5 Representations and warranties of other participants

Base Policy

No stipulation.

9.7 Disclaimers of warranties

Base Policy

Except for express warranties stated in this CP, Fortanix and the Fortanix Group Affiliates expressly disclaim and make no representation, warranty or covenant of any kind,whether express or implied, either in fact or by operation of law, with respect to this CPS or any Certificate issued hereunder, including without limitation, all warranties of quality, merchantability, non-infringement, title and fitness for a particular purpose, and all warranties, representations, conditions, undertakings, terms and obligations implied by statute or common law, trade usage, course of dealing or otherwise are hereby excluded to the fullest extent permitted by law. Except for the express warranties described above, Fortanix and the Fortanix Group Affiliates further disclaim and makes no representation, warranty or covenant of any kind, whether express or implied, either in fact or by operation of law, to any applicant, subscriber, or any relying party that (A) the Subscriber to which it has issued a Certificate is in fact the person, entity, or organization it claims to have been, (B) a Subscriber is in fact the person, entity, or organization listed in the Certificate, or (C) that the information contained in the Certificates or in any Certificate status mechanism complied, published or otherwise disseminated by Fortanix, or the results of any cryptographic method implemented in connection with the Certificates is accurate, authentic, complete or reliable.

In addition, and without limiting the foregoing the CA is not liable for any loss:

- To CA or RA services due to war, natural disasters or other uncontrollable forces;
- Incurred between the time a Certificate is revoked and the next scheduled issuance of a CRL;
- Due to unauthorized use of Certificates issued by the CA, or use of Certificates beyond the prescribed use defined by this CP;
- Arising from the negligent or fraudulent use of Certificates or CRLs issued by the CA; and
- Due to disclosure of personal information contained within Certificates, CRLs and/or OCSP response

9.8 Limitations of liability

Base Policy

Fortanix Group's entire liability under this CPS to an Applicant or Subscriber is set out in the Subscriber Agreement between Fortanix and such Subscriber. Fortanix makes no claims with regard to the suitability or authenticity of certificates issued under this CP. Relying parties may only use these RCA, CA and Subscriber certificates at their own risk. Fortanix assumes no liability whatsoever what so ever in relation with the use of certificate or associated public/private key pairs for any use other than those described in the present CP/CPS.

9.9 Indemnities

Base Policy

Fortanix makes no claims as to the suitability of certificates issued under this CP for any purpose whatsoever. Relying parties use these RCA, CA and Subscriber certificates at their own risk. Fortanix has no obligation to make any payments regarding costs associated with the malfunction or misuse of certificates issued under this CP.

9.10 Term and termination

9.10.1 Term

Base Policy

This CP becomes effective upon publication in the Repository. This CP, as amended from time to time, will remain in force until it is replaced by a new version. Amendments to this CP become effective upon publication in Repository.

9.10.2 Termination

Base Policy

This CP and any amendments remain in effect until replaced by a newer version.

9.10.3 Effect of termination and survival

Base Policy

No stipulation.

9.11 Individual notices and communications with participants

Base Policy

Upon termination of this CP, CA certified by Fortanix domain are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates.

9.12 Amendments

9.12.1 Procedure for amendment

Base Policy

Fortanix may, in its discretion, modify the CPS and the terms and conditions contained herein from time to time, and shall be approved as per Section 1.5.4.

9.12.2 Notification mechanism and period

Base Policy

No stipulation.

9.12.3 Circumstances under which OID must be changed

Base Policy

No stipulation.

9.13 Dispute resolution provisions

Base Policy

In the event of any dispute involving the services or provisions covered by this CP, the disputing parties will use their best efforts to settle the dispute or disagreement through good faith negotiations following notice from one disputing party to the other. The disputing party shall notify a member of Fortanix security team regarding the dispute.

9.14 Governing law

Base Policy

The laws of California State govern the interpretation, construction, validity, and enforcement and performance of this CP, excluding its conflicts of law rules. The application of the United Nations Convention on Contracts for the International Sale of Goods to the CPS, any Subscriber Agreements, and any Relying Party Agreements is expressly excluded. The state or federal courts located in Santa Clara County, California, shall have exclusive venue and jurisdiction over any proceedings related to this CP.

9.15 Compliance with applicable law

Base Policy

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. California law governs this CP and CPS.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Base Policy

This CP constitutes the entire understanding between the parties and supersedes all other terms, whether expressed or implied by law. No modification of this CP shall be of any force or effect unless in writing and signed by an authorized signatory. Failure to enforce any or all of these sections in a particular instance or instances shall not constitute a waiver thereof or preclude subsequent enforcement thereof. All provisions in this CP which by their nature extend beyond the term of the performance of the services such as without limitation those concerning confidential information and intellectual property rights shall survive such term until fulfilled and shall apply to any party's successors and assigns.

9.16.2 Assignment

Base Policy

Except as otherwise provided under the applicable agreements, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the other party, except that Fortanix may assign and delegate this CP to any party of its choosing.

9.16.3 Severability

Base Policy

If any provision of this CP is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Base Policy

No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CP are for convenience only and cannot be used in interpreting this CP.

9.16.5 Force Majeure

Base Policy

Fortanix shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond its reasonable control, including, but not limited to, an act of civil or military authority, natural

disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action or any unforeseeable events or situations.

FORTANIX HAS NO LIABILITY FOR ANY DELAYS, NON-DELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD PARTY ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO FORTANIX DOMAIN.

9.17 Other provisions

Base Policy

No stipulation.