

**Global Federated Identity and Privilege Management (GFIPM)**

**Member Certificate Policy Template**

**Version 1.0**

**DRAFT 2011-11-10**

**By: The Global Security Working Group**

**November 10, 2011**

**Table of Contents**

1 Introduction 8

1.1 Overview 10

1.1.1 Certificate Policy 11

1.1.2 References 11

1.2 Document Name and Identification 12

1.3 PKI Participants 12

1.3.1 Certification Authorities 12

1.3.2 Registration Authorities 12

1.3.3 Subscribers 12

1.3.4 Relying Parties 13

1.3.5 Other Participants 14

1.4 Certificate Usage 14

1.4.1 Appropriate Certificate Uses 14

1.4.2 Prohibited Certificate Uses 15

1.5 Policy Administration 15

1.5.1 Organization Administering the Document 15

1.5.2 Contact Person 15

1.5.3 Entity Determining CP Suitability 15

1.5.4 CP Approval Procedures 15

1.6 Definitions and Acronyms 16

2 Publication and Repository Responsibilities 16

2.1 Repositories 16

2.2 Publication of Certification Information 17

2.3 Time or Frequency of Publication 17

2.4 Access Controls on Repositories 17

3 Identification and Authentication 18

3.1 Naming 18

3.1.1 Types of Names 18

3.1.2 Need for Names to Be Meaningful 18

3.1.3 Anonymity or Pseudonymity of Subscribers 18

3.1.4 Rules for Interpreting Various Name Forms 18

3.1.5 Uniqueness of Names 19

3.1.6 Recognition, Authentication, and Role of Trademarks 19

3.2 Initial Identity Validation 19

3.2.1 Method to Prove Possession of Private Key 19

3.2.2 Authentication of Organization Identity 20

3.2.3 Authentication of Individual Identity 20

3.2.4 Non-Verified Subscriber Information 20

3.2.5 Validation of Authority 20

3.2.6 Criteria for Interoperation 20

3.3 Identification and Authentication for Re-Key Requests 21

3.3.1 Identification and Authentication for Routine Re-Key 21

3.3.2 Identification and Authentication for Re-Key After Revocation 21

3.4 Identification and Authentication for Revocation Request 21

4 Certificate Life-Cycle Operational Requirements 22

4.1 Certificate Application 22

4.1.1 Who Can Submit a Certificate Application 22

4.1.2 Enrollment Process and Responsibilities 22

4.2 Certificate Application Processing 23

4.2.1 Performing Identification and Authentication Functions 23

4.2.2 Approval or Rejection of Certificate Applications 23

4.2.3 Time to Process Certificate Applications 23

4.3 Certificate Issuance 23

4.3.1 CA Actions during Certificate Issuance 23

4.3.2 Notification to Subscriber by the CA Of Issuance Of Certificate 24

4.4 Certificate Acceptance 24

4.4.1 Conduct Constituting Certificate Acceptance 24

4.4.2 Publication of the Certificate by the CA 24

4.4.3 Notification of Certificate Issuance by the CA to Other Entities 24

4.5 Key Pair and Certificate Usage 25

4.5.1 Subscriber Private Key and Certificate Usage 25

4.5.2 Relying Party Public Key and Certificate Usage 25

4.6 Certificate Renewal 25

4.6.1 Circumstance for Certificate Renewal 26

4.6.2 Who May Request Renewal 26

4.6.3 Processing Certificate Renewal Requests 26

4.6.4 Notification of New Certificate Issuance to Subscriber 27

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 27

4.6.6 Publication of the Renewal Certificate by the CA 27

4.6.7 Notification of Certificate Issuance by the CA to Other Entities 27

4.7 Certificate Re-Key 27

4.7.1 Circumstance for Certificate Re-Key 28

4.7.2 Who May Request Certification of a New Public Key 28

4.7.3 Processing Certificate Re-Keying Requests 28

4.7.4 Notification of New Certificate Issuance To Subscriber 29

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 29

4.7.6 Publication of the Re-Keyed Certificate by the CA 29

4.7.7 Notification of Certificate Issuance by the CA to Other Entities 29

4.8 Certificate Modification 30

4.8.1 Circumstance for Certificate Modification 30

4.8.2 Who May Request Certificate Modification 30

4.8.3 Processing Certificate Modification Requests 31

4.8.4 Notification of New Certificate Issuance to Subscriber 31

4.8.5 Conduct Constituting Acceptance of Modified Certificate 31

4.8.6 Publication of the Modified Certificate by the CA 31

4.8.7 Notification of Certificate Issuance by the CA to Other Entities 31

4.9 Certificate Revocation and Suspension 32

4.9.1 Circumstances for Revocation 32

4.9.2 Who Can Request Revocation 32

4.9.3 Procedure for Revocation Request 32

4.9.4 Revocation Request Grace Period 33

4.9.5 Time within Which CA Must Process the Revocation Request 33

4.9.6 Revocation Checking Requirement for Relying Parties 33

4.9.7 CRL Issuance Frequency (If Applicable) 34

4.9.8 Maximum Latency for CRLs (If Applicable) 34

4.9.9 On-Line Revocation/Status Checking Availability 34

4.9.10 On-Line Revocation Checking Requirements 34

4.9.11 Other Forms of Revocation Advertisements Available 34

4.9.12 Special Requirements Re Key Compromise 34

4.9.13 Circumstances for Suspension 34

4.9.14 Who Can Request Suspension 35

4.9.15 Procedure for Suspension Request 35

4.9.16 Limits on Suspension Period 35

4.10 Certificate Status Services 35

4.10.1 Operational Characteristics 35

4.10.2 Service Availability 35

4.10.3 Optional Features 35

4.11 End of Subscription 36

4.12 Key Escrow and Recovery 36

4.12.1 Key Escrow and Recovery Policy and Practices 36

4.12.2 Session Key Encapsulation and Recovery Policy and Practices 36

5 Facility, Management, and Operational Controls 36

5.1 Physical Controls 36

5.1.1 Site Location and Construction 37

5.1.2 Physical Access 37

5.1.3 Power and Air Conditioning 37

5.1.4 Water Exposures 37

5.1.5 Fire Prevention and Protection 37

5.1.6 Media Storage 38

5.1.7 Waste Disposal 38

5.1.8 Off-Site Backup 38

5.2 Procedural Controls 38

5.2.1 Trusted Roles 38

5.2.2 Number of Persons Required Per Task 39

5.2.3 Identification and Authentication for Each Role 39

5.2.4 Roles Requiring Separation of Duties 39

5.3 Personnel Controls 39

5.3.1 Qualifications, Experience, and Clearance Requirements 39

5.3.2 Background Check Procedures 39

5.3.3 Training Requirements 39

5.3.4 Retraining frequency and requirements 40

5.3.5 Job Rotation Frequency and Sequence 40

5.3.6 Sanctions for Unauthorized Actions 40

5.3.7 Independent Contractor Requirements 40

5.3.8 Documentation Supplied To Personnel 40

5.4 Audit Logging Procedures 40

5.4.1 Types of Events Recorded 41

5.4.2 Frequency of Processing Log 41

5.4.3 Retention Period for Audit Log 41

5.4.4 Protection of Audit Log 41

5.4.5 Audit Log Backup Procedures 41

5.4.6 Audit Collection System (Internal Vs. External) 41

5.4.7 Notification to Event-Causing Subject 41

5.4.8 Vulnerability Assessments 41

5.5 Records Archival 41

5.5.1 Types of Records Archived 41

5.5.2 Retention Period for Archive 42

5.5.3 Protection of Archive 42

5.5.4 Archive Backup Procedures 42

5.5.5 Requirements for Time-Stamping Of Records 42

5.5.6 Archive Collection System (Internal or External) 42

5.5.7 Procedures to Obtain and Verify Archive Information 42

5.6 Key Changeover 42

5.7 Compromise and Disaster Recovery 42

5.7.1 Incident and Compromise Handling Procedures 42

5.7.2 Computing Resources, Software, and/or Data Are Corrupted 43

5.7.3 Entity Private Key Compromise Procedures 43

5.7.4 Business Continuity Capabilities after a Disaster 43

5.8 CA or RA Termination 43

6 Technical Security Controls 43

6.1 Key Pair Generation and Installation 43

6.1.1 Key Pair Generation 44

6.1.2 Private Key Delivery to Subscriber 44

6.1.3 Public Key Delivery to Certificate Issuer 44

6.1.4 CA Public Key Delivery to Relying Parties 44

6.1.5 Key Sizes 44

6.1.6 Public Key Parameters Generation and Quality Checking 44

6.1.7 Key Usage Purposes (As Per X.50vkey Usage Field) 44

6.2 Private Key Protection and Cryptographic Module Engineering Controls 45

6.2.1 Cryptographic Module Standards and Controls 45

6.2.2 Private Key (N out of M) Multi-Person Control 45

6.2.3 Private Key Escrow 45

6.2.4 Private Key Backup 45

6.2.5 Private Key Archival 45

6.2.6 Private Key Transfer Into or From a Cryptographic Module 46

6.2.7 Private Key Storage on Cryptographic Module 46

6.2.8 Method of Activating Private Key 46

6.2.9 Method of Deactivating Private Key 46

6.2.10 Method of Destroying Private Key 47

6.2.11 Cryptographic Module Rating 47

6.3 Other Aspects of Key Pair Management 47

6.3.1 Public Key Archival 47

6.3.2 Certificate Operational Periods and Key Pair Usage Periods 47

6.4 Activation Data 47

6.4.1 Activation Data Generation and Installation 47

6.4.2 Activation Data Protection 48

6.4.3 Other Aspects of Activation Data 48

6.5 Computer Security Controls 48

6.5.1 Specific Computer Security Technical Requirements 48

6.5.2 Computer Security Rating 49

6.6 Life Cycle Technical Controls 49

6.6.1 System Development Controls 49

6.6.2 Security Management Controls 49

6.6.3 Life Cycle Security Controls 50

6.7 Network Security Controls 50

6.8 Time-Stamping 50

7 Certificate, CRL, and OCSP Profiles 50

7.1 Certificate Profile 50

7.1.1 Version Number(s) 50

7.1.2 Certificate Extensions 51

7.1.3 Algorithm Object Identifiers 51

7.1.4 Name Forms 51

7.1.5 Name Constraints 51

7.1.6 Certificate Policy Object Identifier 51

7.1.7 Usage of Policy Constraints Extension 51

7.1.8 Policy Qualifiers Syntax and Semantics 51

7.1.9 Processing Semantics for the Critical Certificate Policies Extension 51

7.2 CRL Profile 51

7.2.1 Version Number(s) 51

7.2.2 CRL and CRL Entry Extensions 51

7.3 OCSP Profile 52

7.3.1 Version Number(s) 52

7.3.2 OCSP Extensions 52

8 Compliance Audit and Other Assessments 52

8.1 Frequency or Circumstances of Assessment 52

8.2 Identity/Qualifications of Assessor 52

8.3 Assessor's Relationship to Assessed Entity 52

8.4 Topics Covered By Assessment 53

8.5 Actions Taken As A Result Of Deficiency 53

8.6 Communication of Results 53

9 Other Business and Legal Matters 53

9.1 Fees 54

9.1.1 Certificate Issuance or Renewal Fees 54

9.1.2 Certificate Access Fees 54

9.1.3 Revocation or Status Information Access Fees 54

9.1.4 Fees for Other Services 54

9.1.5 Refund Policy 54

9.2 Financial Responsibility 54

9.2.1 Insurance Coverage 54

9.2.2 Other Assets 54

9.2.3 Insurance or Warranty Coverage for End-Entities 54

9.3 Confidentiality of Business Information 54

9.3.1 Scope of Confidential Information 55

9.3.2 Information Not Within the Scope of Confidential Information 55

9.3.3 Responsibility to Protect Confidential Information 55

9.4 Privacy of Personal Information 55

9.4.1 Privacy Plan 55

9.4.2 Information Treated As Private 55

9.4.3 Information Not Deemed Private 55

9.4.4 Responsibility to Protect Private Information 55

9.4.5 Notice and Consent to Use Private Information 55

9.4.6 Disclosure Pursuant to Judicial or Administrative Process 56

9.4.7 Other Information Disclosure Circumstances 56

9.5 Intellectual Property Rights 56

9.6 Representations and Warranties 56

9.6.1 CA Representations and Warranties 56

9.6.2 RA Representations and Warranties 56

9.6.3 Subscriber Representations and Warranties 56

9.6.4 Relying Party Representations and Warranties 56

9.6.5 Representations and Warranties of Other Participants 56

9.7 Disclaimers of Warranties 56

9.8 Limitations of Liability 56

9.9 Indemnities 57

9.10 Term and Termination 57

9.10.1 Term 57

9.10.2 Termination 57

9.10.3 Effect of Termination and Survival 57

9.11 Individual Notices and Communications with Participants 57

9.12 Amendments 57

9.12.1 Procedure for Amendment 57

9.12.2 Notification Mechanism and Period 57

9.12.3 Circumstances under Which OID Must Be Changed 57

9.13 Dispute Resolution Provisions 58

9.14 Governing Law 58

9.15 Compliance with Applicable Law 58

9.16 Miscellaneous Provisions 58

9.16.1 Entire Agreement 58

9.16.2 Assignment 58

9.16.3 Severability 58

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights) 58

9.16.5 Force Majeure 58

9.17 Other Provisions 58

**Legend for Terms in Placeholders:**

* FMO = Federation Management Organization
* BODA = Board of Directors or Advisors
* EC = Executive Committee

# Introduction

In order to allow for the connection of multiple parties in a trusted information sharing environment known as [Federation Name], [FMO Name] has adopted the Global Federated Identity and Privilege Management (GFIPM) suite of technical specifications and profiles, which provide for the establishment and operation of secure, interoperable communication profiles between [Federation Name] members for the purpose of exchanging information subject to appropriate access control policies. One of the GFIPM specifications adopted by [FMO Name] is the GFIPM Cryptographic Trust Model [GFIPM Trust], which is a normative specification that describes the structure of a *GFIPM Cryptographic Trust Fabric* document. This “Trust Fabric” concept comes from the Security Assertion Markup Language (SAML) 2.0 suite of standards – specifically from the normative *SAML 2.0 Metadata* specification[[1]](#footnote-1) – and refers to a cryptographically signed XML document containing names, service endpoints, X.509 certificates, and other ancillary information about the members of a federation. In the GFIPM security paradigm, a “Trust Fabric” document defines the membership of a federation at a specific point in time. Throughout this document, the term *[Federation Name] Cryptographic Trust Fabric* refers to a GFIPM Cryptographic Trust Fabric document used to define [Federation Name] membership.

While [Federation Name] and its members do not rely on a traditional Public Key Infrastructure (PKI) security model, their reliance on the [Federation Name] Cryptographic Trust Fabric document requires implicit reliance on the proper lifecycle management process for the X.509 certificates that appear in that Trust Fabric document, as well as the private keys corresponding to those X.509 certificates. In addition, [Federation Name] and its members rely on the cryptographic integrity of the [Federation Name] Cryptographic Trust Fabric document, which requires implicit reliance on the lifecycle management process for the X.509 certificate and corresponding private key used by [FMO Name] to sign the Trust Fabric document. For these reasons, [Federation Name] has adopted this [Federation Name] Member Certificate Policy.

This certificate policy (CP) follows the standard PKI CP format defined in [RFC 3647]; however, due to the specific details of the [Federation Name]’s GFIPM-based security model described above, this CP does not cover all the standard CP topics in the same manner that a traditional PKI CP would cover them. Instead, it covers each topic as it relates to the [Federation Name] security model, and explains the differences between a traditional PKI security model and the [Federation Name] security model where necessary.

***Definitions and Perspective of This Document***

The following paragraphs delineate the fundamental differences between the [Federation Name] trust model and a traditional PKI trust model, to provide the appropriate context for the remainder of this document.

A traditional PKI CP typically describes the responsibilities of a single *certificate authority* (CA): an entity that issues certificates for use by one or more *subscribers*, for the benefit of one or more *relying parties* (RPs). A traditional PKI CP typically also describes the responsibilities of subscribers and relying parties. This CP uses the concepts of CA, subscriber, and RP, but defines them differently, as follows.

1. Subscribers to this CP include [FMO Name] as well as all [Federation Name] member agencies; however, subscribers to this CP are not subscribers in the traditional PKI sense wherein a CA has generated an X.509 certificate for them. (See the following item about certificate self-generation by subscribers.)
2. Each [Federation Name] member agency acts as a CA in this CP for the X.509 certificates that it generates and manages, and which appear in the [Federation Name] Cryptographic Trust Fabric. No [Federation Name] member agency generates certificates for another member agency, i.e. each subscriber to this CP generates and manages its own certificates and corresponding public/private key pairs.
3. [FMO Name] acts as a CA in this CP for the X.509 certificate that it generates and manages, and which is used to cryptographically sign the [Federation Name] Cryptographic Trust Fabric and thereby ensure the integrity of the Trust Fabric document.
4. Each [Federation Name] member agency acts as a relying party (RP) in this CP, in that it relies on the integrity of the lifecycle management process for the X.509 certificates that are generated and managed by other [Federation Name] member agencies, and which appear in the [Federation Name] Cryptographic Trust Fabric.
5. Each [Federation Name] member agency acts as a relying party (RP) in this CP, in that it also relies on the integrity of the lifecycle management process for the X.509 certificate that is generated and managed by [FMO Name], and which is used to cryptographically sign the [Federation Name] Cryptographic Trust Fabric document.

Note that in this CP, organizational entities often have multiple roles (CA, subscriber, and RP), and therefore many of the sections of this document must be read from multiple perspectives to fully understand the responsibilities of each party. Note also that this CP pertains only to certificates that appear in the [Federation Name] Cryptographic Trust Fabric. This CP does not pertain to, and has no direct relation to, certificates that may be generated, managed, or purchased by [FMO Name] or [Federation Name] member agencies for other purposes, such as authenticating users or establishing secure SSL/TLS sessions between HTTP user agents (web browsers) and secure web applications. Finally, note that the traditional PKI concept of a registration authority (RA) has no meaning in this CP, since [Federation Name]’s security model does not require registration of subscribers with a CA in the traditional sense.

***Applicability of This Document***

This CP applies to [FMO Name] as well as all [Federation Name] members: Identity Provider Organizations (IDPOs), Service Provider Organizations (SPOs), and Trusted Identity Broker Organizations (TIBOs). (All of these organizations are collectively referred to as the subscribers to this CP.) However, not all statements in this document apply to all subscribers. Throughout the document, some distinctions are made between the following categories of subscribers and the requirements that apply to each category.

1. ***Level 2 Subscribers*** are agencies that are permitted to assert a NIST level of assurance (LOA) of up to Level 2[[2]](#footnote-2) for their users. The requirements for Level 2 subscribers are generally less stringent than requirements for other categories of subscribers.
2. ***Level 3 Subscribers*** are agencies that are permitted to assert a NIST level of assurance (LOA) of up to Level 3 for their users. The requirements for Level 3 subscribers are generally more stringent than requirements for other categories of subscribers.
3. ***[FMO Name]*** is also a subscriber to this CP, but it does not participate in operational information-sharing transactions with other members, and therefore does not have a need to assert NIST levels of assurance on behalf of users. In general, the requirements of [FMO Name] are at least as stringent as those of Level 3 subscribers.

All requirements in this document that are not targeted specifically towards one of the categories of subscribers above are applicable to all subscribers.

## Overview

This CP is based on the standard PKI CP document structure as outlined in [RFC 3647]. The section numbering and titles follow the [RFC 3647] recommendations. In addition, this CP was written based on the guidance provided by [GFIPM CP]. Note, however, as described in Section 1, that this CP covers each topic in a non-standard manner, and calls out the differences between a traditional PKI security model and the [Federation Name] security model where applicable.

None of the sections stipulated by [RFC 3647] have been omitted; however, some sections of this CP may state “no stipulation” when the CP imposes no requirements or makes no disclosure. Additionally, some sections make state “not applicable” if the particular topic addressed by that section does not apply to this policy. Where appropriate, additional descriptive text has been included to indicate why specific sections are not applicable.

Note that the entire content of [RFC 3647] is available at the following sources (in different formats):

* Plain text: <http://www.ietf.org/rfc/rfc3647.txt> or

<http://www.faqs.org/rfcs/rfc3647.html>

* HTML: <http://www.faqs.org/rfcs/rfc3647.html>
* Text PDF: <http://www.faqs.org/ftp/rfc/pdf/rfc3647.txt.pdf>

### Certificate Policy

The term “certificate policy” (CP) is defined by the X.509 standard as “a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements”.

A CP based on the [RFC 3647] format usually applies to a certificate authority (CA) that operates a traditional public key infrastructure (PKI) consisting of many subscribers (users or non-human system entities). In this case, however, the CP is geared not towards a certificate authority, but towards [Federation Name] and its members (subscribers) that operate trusted software system endpoints within the federation. (A trusted software system endpoint can be an identity provider, service provider, trusted identity broker, or other service.) The [Federation Name] Cryptographic Trust Fabric includes an entry for each trusted software system endpoint in the federation. The Trust Fabric entry for a trusted endpoint includes basic information about the endpoint (e.g. its URL, points of contact for the organization that manages the endpoint, etc.) as well as one or more X.509 certificates used by the endpoint for cryptographic operations. The purpose of the Trust Fabric is to attest, on behalf of [FMO Name], that the X.509 certificate(s) assigned to an endpoint are legitimate and trustworthy. The purpose of this CP is to set forth a list of rules that each subscriber must obey to help ensure that the X.509 certificates assigned to their trusted software service endpoints are in fact legitimate and trustworthy, and that the entire [Federation Name] Cryptographic Trust Fabric document maintains its legitimacy and trustworthiness at all times.

### References

Table 1 provides a list of references for documents that are related to this CP.

|  |
| --- |
| **References for Related Documents** |
| **Document ID** | **Document Name and URL** |
| GFIPM Terms | GFIPM Terminology Matrix |
| GFIPM Meta | GFIPM Metadata Specification |
| GFIPM Trust | GFIPM Cryptographic Trust Model |
| GFIPM CP | GFIPM Certificate Policy Template |
| GFIPM U2A Profile | GFIPM Web Browser User-to-Application Profile |
| GFIPM S2S Profile | GFIPM Web Services System-to-System Profile |
| [Federation Name] MA | [Federation Name] Membership Agreement |
| [Federation Name] Governance | [Federation Name] Governance Document and/or Bylaws |
| [Federation Name] OPP | [Federation Name] Operational Policies and Procedures |
| [Federation Name] CPS | [Federation Name] Certification Practice Statement |
| [Federation Name] CP | [Federation Name] Certificate Policy (This Document) |
| FIPS 140-2 | Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules,* 3 December 2002. |
| RFC 3647 | Internet Engineering Task Force (IETF) Request for Comments 3647, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, November 2003 |

Table 1: References for Related Documents

## Document Name and Identification

The name of this document is: “National Information Exchange Federation Center Certificate Policy”.

## PKI Participants

This CP does not pertain directly to the operation of a PKI; however, this CP does impact [FMO Name], and all [Federation Name] member agencies, in various ways as called out in the following subsections.

### Certification Authorities

Each [Federation Name] member agency acts as a CA for the X.509 certificates that it generates and manages, and which appear in the [Federation Name] Cryptographic Trust Fabric; however, no [Federation Name] member agency generates certificates for another member agency.

In addition, [FMO Name] acts as a CA for the X.509 certificate that it generates and manages, and which is used to cryptographically sign the [Federation Name] Cryptographic Trust Fabric and thereby ensure the integrity of the Trust Fabric document. But [FMO Name] does not generate certificates for any member agencies.

### Registration Authorities

This CP does not require the registration of subscribers with a CA in the traditional sense, since there is no CA that issues certificates to subscribers; therefore, there are no registration authorities, and this section is not applicable.

### Subscribers

Subscribers to this CP include [FMO Name] as well as all [Federation Name] member agencies; however, subscribers to this CP are not subscribers in the traditional PKI sense wherein a CA has generated an X.509 certificate for them. As noted in Section 1.3.1, each subscriber to this CP acts as its own CA for the certificates that it uses.

### Relying Parties

A relying party is a recipient of a certificate that acts in reliance on that certificate and/or any digital signatures verified using that certificate and/or any messages encrypted using that certificate.

Organizations that are [Federation Name] members are relying parties of the X.509 certificates covered by this CP, and the [Federation Name] Cryptographic Trust Fabric in which the certificates are published, in that they rely on digital signatures and message encryption operations made using certificates covered by this CP and published in the [Federation Name] Cryptographic Trust Fabric. Specifically, Service Provider Organizations (SPOs), Identity Provider Organizations (IDPOs), and Trusted Identity Broker Organizations (TIBOs) rely upon these certificates to authenticate digitally signed messages and to decrypt digitally encrypted messages, in the following scenarios.

1. When a [Federation Name] Identity Provider (IDP) or Trusted Identity Broker (TIB) receives a message from a [Federation Name] Service Provider (SP) as part of a transaction that conforms to [GFIPM U2S Profile] or [GFIPM S2S Profile], it relies on a certificate covered by this CP and published in the [Federation Name] Cryptographic Trust Fabric to support verification of a digital signature that effectively verifies that the message signer is a legitimate, trustworthy SP in [Federation Name]. In this scenario, the [Federation Name] IDP or TIB may also rely on a certificate covered by this CP and published in the [Federation Name] Cryptographic Trust Fabric to support decryption of an encrypted message, or decryption of one or more encrypted parts of a message.
2. When a [Federation Name] SP receives a message from a [Federation Name] IDP or a [Federation Name] TIB as part of a transaction that conforms to [GFIPM U2S Profile] or [GFIPM S2S Profile], it relies on a certificate covered by this CP and published in the [Federation Name] Cryptographic Trust Fabric to support verification of a digital signature that effectively verifies that the message signer is a legitimate, trustworthy IDP or TIB in [Federation Name]. In this scenario, the [Federation Name] SP may also rely on a certificate covered by this CP and published in the [Federation Name] Cryptographic Trust Fabric to support decryption of an encrypted message, or decryption of one or more encrypted parts of a message.
3. When a [Federation Name] web services component (Web Service Consumer (WSC) or Web Service Provider (WSP)) receives a message from another [Federation Name] web services component as part of a transaction that conforms to [GFIPM S2S Profile], it relies on a certificate covered by this CP and published in the [Federation Name] Cryptographic Trust Fabric to support verification of a digital signature that effectively verifies that the message signer is a legitimate, trustworthy web services component in [Federation Name]. In this scenario, the message recipient may also rely on a certificate covered by this CP and published in the [Federation Name] Cryptographic Trust Fabric to support decryption of an encrypted message, or decryption of one or more encrypted parts of a message.

In addition to these “member-to-member” trust relationships, whenever [Federation Name] members process a new version of the [Federation Name] Cryptographic Trust Fabric document, they rely on the X.509 certificate that is used by [FMO Name] to cryptographically sign the [Federation Name] Cryptographic Trust Fabric document.

### Other Participants

[Federation Name] allows for the use of a Trusted Identity Broker Organization (TIBO), which acts as a trust bridge between [Federation Name] member SPOs and non-member IDPOs. This CP does not pertain directly to the operations of non-member IDPOs; however, the security policies adopted by non-member IDPOs can have an indirect impact on [FMO Name] and [Federation Name] members. Similarly, the security policies adopted by [Federation Name], including this CP, can have an indirect impact on non-member IDPOs. For this reason, the [Federation Name] Operational Policies and Procedures [[Federation Name] OPP] stipulate that non-member IDPOs must disclose their local security policies and procedures to [Federation Name] members as part of the application and onboarding process for a TIBO.

## Certificate Usage

This section describes uses of the X.509 certificates addressed by this CP.

### Appropriate Certificate Uses

The appropriate uses of the certificates and corresponding private keys addressed by this CP are:

1. Cryptographic signing of messages that are to be sent between trusted software service endpoints within [Federation Name] as part of transactions that conform to [GFIPM U2S Profile] or [GFIPM S2S Profile].
2. Verification of digital cryptographic signatures on messages sent between trusted software service endpoints within [Federation Name] as part of transactions that conform to [GFIPM U2S Profile] or [GFIPM S2S Profile].
3. Encryption of messages or parts of messages that are to be sent between trusted software service endpoints within [Federation Name] as part of transactions that conform to [GFIPM U2S Profile] or [GFIPM S2S Profile].
4. Decryption of encrypted messages or encrypted parts of messages sent between trusted software service endpoints within [Federation Name] as part of transactions that conform to [GFIPM U2S Profile] or [GFIPM S2S Profile].

The GFIPM Communication Profiles ([GFIPM U2S Profile] and [GFIPM S2S Profile]) specify more detailed requirements for digital signing of messages, verification of digital signatures on messages, encryption of messages or parts of messages, and decryption of encrypted messages or encrypted parts of messages.

### Prohibited Certificate Uses

All certificate uses not listed as appropriate uses in Section 1.4.1 are prohibited.

## Policy Administration

This section includes the name and mailing address of the organization that is responsible for the drafting, registering, maintaining, and updating of this CP. It also includes the name, electronic mail address, and telephone number of a contact person.

### Organization Administering the Document

[FMO Name] is the administering organization for this CP. [FMO Name]’s full name and mailing address is:

[FMO Name]
[FMO Address]

### Contact Person

The contact person for [FMO Name] is:

[Contact Person Name]

[Contact Person Address]

[Contact Person Phone]

[Contact Person Email]

### Entity Determining CP Suitability

[FMO Name] and [Federation BODA Name] determine the suitability of this CP.

### CP Approval Procedures

This CP requires approval by [FMO Name] and [Federation EC Name].

## Definitions and Acronyms

The following acronyms are used in this CP and related GFIPM and [Federation Name] documents. Some of the terms listed below are defined or described in more detail in [GFIPM Terms].

|  |  |
| --- | --- |
| **Acronym** | **Meaning** |
| CA | Certificate Authority |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| DS | Discovery Service |
| GFIPM | Global Federated Identity and Privilege Management |
| IDP | Identity Provider |
| IDPO | Identity Provider Organization |
| OCSP | Online Certificate Status Protocol |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| SP | Service Provider |
| SPO | Service Provider Organization |
| TIB | Trusted Identity Broker |
| TIBO | Trusted Identity Broker Organization |
| WSP | Web Service Provider |

# Publication and Repository Responsibilities

## Repositories

[Federation Name] maintains two document repositories.

All [Federation Name] policy documents, including this CP, related [Federation Name] policies (e.g. [[Federation Name] Governance], [[Federation Name] CPS], etc.), and policy documents submitted by [Federation Name] members, are published at [Location].

The current [Federation Name] Cryptographic Trust Fabric document shall be posted at the following URL.

[URL]

In addition, for redundancy, the current Trust Fabric document shall be posted at an alternative URL, to be chosen by [FMO Name]. This secondary URL shall be chosen so as to minimize the likelihood that both copies of the Trust Fabric document are unavailable simultaneously.

The [Federation Name] Cryptographic Trust Fabric document is publicly available for download.[[3]](#footnote-3)

## Publication of Certification Information

[FMO Name] publishes subscriber certificates in the [Federation Name] Cryptographic Trust Fabric, which is publicly available at the URL specified in the previous section. Subscriber certificates are not published in any other certificate repository.[[4]](#footnote-4)

## Time or Frequency of Publication

[FMO Name] shall publish a revised version of the [Federation Name] Cryptographic Trust Fabric every 30 days, and also whenever changes to the federation membership or other circumstances necessitate it. Upon publication of a new Trust Fabric document, [FMO Name] shall notify all [Federation Name] members about the revision. Members must implement the new revision of the Trust Fabric within their local systems within one business day after receiving notification about it.

For more information about the policies and procedures that [FMO Name] follows in the maintenance of the [Federation Name] Cryptographic Trust Fabric, including methods for notifying subscribers about updates, please see [GFIPM Trust]. For more information about the policies and procedures that [FMO Name] follows in making decisions about federation membership changes, please see [[Federation Name] OPP].

## Access Controls on Repositories

The [Federation Name] Cryptographic Trust Fabric is publicly available at the URL specified in Section 2.1.

# Identification and Authentication

This section and its subsections pertain to the identification and authentication of entities that are bound to certificates that are covered by this CP. [FMO Name] does not issue private keys or certificates to [Federation Name] members; however, it does perform certain security functions and stipulate certain subscriber identification and authentication rules that parallel the subscriber identification and authentication rules stipulated for a traditional PKI. All rules described in this section are oriented towards the goal of ensuring the integrity of the [Federation Name] Cryptographic Trust Fabric and the certificates that it contains.

## Naming

This section pertains to naming and name management issues that can arise for names within X.509 certificates. As [Federation Name] does not employ a traditional PKI trust model, many naming issues that pertain to a PKI are either not applicable to [Federation Name] or are applicable in a slightly different context than what is typically expected in a PKI. Each subsection provides appropriate details as needed.

### Types of Names

A certificate that is covered by this CP may contain any type of name, as long as the name represented is meaningful according to the requirements stipulated in Section 3.1.2.

### Need for Names to Be Meaningful

A certificate that is covered by this CP must contain a name that clearly and uniquely identifies the organization that owns the certificate. In the case where multiple certificates pertain to the same organization, it is recommended that the certificate name also identify the system or service endpoint of the subscriber and/or the purpose for which the certificate is to be used (e.g. signing only, encryption only, or both).

### Anonymity or Pseudonymity of Subscribers

This CP does not permit anonymity or pseudonymity of subscribers. Subscribers to this CP include [FMO Name] and [Federation Name] members, and the identity of each subscriber is well known to all other subscribers.

### Rules for Interpreting Various Name Forms

Not applicable. The [Federation Name] Cryptographic Trust Fabric and its trust model do not require machine interpretation of any names that appear within certificates; however, as stipulated in Section 3.1.2, certificate names must be meaningful in the context of [Federation Name].

### Uniqueness of Names

Due to the naming rules stipulated in Section 3.1.2, name collisions between certificates are possible only for certificates that pertain to the same organization. In the case where multiple certificates pertain to the same organization, it is recommended that the certificate name also identify the system or service endpoint of the subscriber and/or the purpose for which the certificate is to be used (e.g. signing only, encryption only, or both).

### Recognition, Authentication, and Role of Trademarks

Not applicable.

## Initial Identity Validation

This section pertains to the validation of identities to which X.509 certificates are bound, for the purpose of installing a new certificate in the [Federation Name] Cryptographic Trust Fabric on behalf of a new subscriber. Note that in the [Federation Name] trust model, identities are bound to certificates not through the names in those certificates, but through the [Federation Name] Cryptographic Trust Fabric.

### Method to Prove Possession of Private Key

Before [FMO Name] will bind a certificate to a subscriber, the subscriber must prove possession of the private key corresponding to that certificate through a simple cryptographic challenge-response protocol. The process of proving private key possession shall proceed as follows.

1. A [FMO Name] representative contacts the subscriber via email or phone at one of its documented points of contact (POC).[[5]](#footnote-5) The purpose of this communication is to identify the technical representative of the subscriber who will be designated to participate in the challenge-response protocol on behalf of the subscriber.
2. After acquiring the email address of the subscriber’s technical representative, a [FMO Name] representative generates a sufficiently long random value (at least 160 bits), encrypts it using the public key of the certificate that the subscriber wishes to bind to its identity, and sends the encrypted value to the subscriber’s designated technical representative via email, along with a set of instructions for decrypting the value.
3. The subscriber’s designated technical representative decrypts the encrypted value using the private key corresponding to the certificate that the subscriber wishes to bind to its identity, and sends the decrypted value to the [FMO Name] representative via email.
4. The [FMO Name] representative compares the original random value with the value sent by the subscriber’s designated technical representative. If the two values match, then the subscriber has proven possession of the private key.

### Authentication of Organization Identity

During the application and onboarding process, and prior to including a subscriber in the [Federation Name] Cryptographic Trust Fabric, [FMO Name] must perform the following tasks.

1. Vet the legitimacy of the subscriber as a legal entity.
2. Vet the legitimacy of the points of contact (POCs) that have been listed on the subscriber’s application form as representatives of the subscriber.

The processes used to accomplish these tasks are outside the scope of this CP. Please refer to [[Federation Name] Governance] and/or [[Federation Name] OPP] for details about these processes.

### Authentication of Individual Identity

Not applicable. Individuals are not permitted to subscribe to this CP; only organizations may subscribe.

### Non-Verified Subscriber Information

Not applicable.

### Validation of Authority

Not applicable.

### Criteria for Interoperation

For proper interoperation with other subscribers and inclusion in the [Federation Name] Cryptographic Trust Fabric, a certificate must meet the following criteria.

1. It must be a valid X.509 certificate.
2. It must contain the following attributes.
	1. **Subject** (See Section 3.1 and its subsections for subject naming rules.)
	2. **Version** (The X.509 version number to which this certificate conforms.)
	3. **Validity** (The “Not Before” and “Not After” dates of validity.)
	4. **Algorithm ID** (The public-key algorithm used to generate the certificate.)
	5. **Signature Algorithm** (The algorithm used to sign the certificate.)
	6. **Public Key**
3. It may contain additional attributes.

## Identification and Authentication for Re-Key Requests

This section pertains to the validation of identities to which X.509 certificates are bound, for the purpose of installing a new certificate in the [Federation Name] Cryptographic Trust Fabric on behalf of a subscriber, in place of an existing certificate that is being removed due to expiration or for security reasons. Note that in the [Federation Name] trust model, identities are bound to certificates not through the names in those certificates, but through the [Federation Name] Cryptographic Trust Fabric.

### Identification and Authentication for Routine Re-Key

In the event of a routine re-key, due to expiration of an existing certificate and/or in accordance with policies pertaining to maximum key lifetime, the subscriber must prove possession of the new private key corresponding to the new certificate, via the process described in Section 3.2.1, before the new certificate can be installed in the [Federation Name] Cryptographic Trust Fabric.

### Identification and Authentication for Re-Key After Revocation

[Federation Name] does not employ a traditional PKI trust model, and does not issue subscriber certificates under this CP, so the concept of certificate revocation is not applicable to this CP. The [Federation Name] trust model does prescribe appropriate actions to prevent relying parties from trusting a certificate that is known or suspected to have been compromised; however, rather than using certificate revocation to accomplish this goal, [Federation Name] accomplishes it via removal of a certificate from the [Federation Name] Cryptographic Trust Fabric.

In the event of a re-key due to prior removal of a subscriber’s existing certificate from the [Federation Name] Cryptographic Trust Fabric, the subscriber must prove possession of the new private key corresponding to the new certificate, via the process described in Section 3.2.1, before the new certificate can be installed in the [Federation Name] Cryptographic Trust Fabric. In addition, depending on the specific details surrounding the removal from the [Federation Name] Cryptographic Trust Fabric, the subscriber may be required to perform additional actions to demonstrate that it has sufficiently mitigated the security vulnerability or risk that precipitated removal from the [Federation Name] Cryptographic Trust Fabric.

## Identification and Authentication for Revocation Request

[Federation Name] does not employ a traditional PKI trust model, and [FMO Name] does not issue subscriber certificates under this CP, so the concept of certificate revocation as it applies to a traditional PKI is not applicable to this CP. The [Federation Name] trust model does prescribe appropriate actions to prevent relying parties from trusting a certificate that is known or suspected to have been compromised; however, rather than using certificate revocation to accomplish this goal, [Federation Name] accomplishes it via removal of a certificate from the [Federation Name] Cryptographic Trust Fabric. See Section 4.9 for more information about [Federation Name] certificate revocation processes and mechanisms.

At any time, any [Federation Name] member agency representative may request that a specific certificate be removed from the [Federation Name] Cryptographic Trust Fabric by contacting [FMO Name] at the point of contact specified in Section 1.5.2. Before honoring the request, [FMO Name] shall attempt to verify the legitimacy of the request by contacting one or more of the official points of contact (POCs) for the member agency.

# Certificate Life-Cycle Operational Requirements

This section and its subsections address certificate life-cycle requirements for subscriber certificates, including application, issuance, acceptance, usage, renewal, revocation, and termination. Unlike a traditional PKI trust model, the trust model employed by [Federation Name] does not include or rely on a single, centralized certificate authority (CA). Accordingly, many of the steps involved in the traditional PKI certificate life cycle model do not apply in [Federation Name]; however, [Federation Name] does stipulate certain rules that parallel the life cycle requirements in a traditional PKI. All rules described in this section are oriented towards the goal of ensuring the integrity of the [Federation Name] Cryptographic Trust Fabric and the certificates that it contains.

## Certificate Application

This section and its subsections are not applicable to this CP. [FMO Name] does not operate a traditional CA, and therefore does not accept certificate applications in the traditional way. In lieu of a certificate application process, [Federation Name] stipulates a formal application and onboarding process, which is described in [[Federation Name] OPP].

After undergoing the formal application and onboarding process, a subscriber must generate its own certificate and prove possession of the private key corresponding to that certificate before [FMO Name] will allow that certificate to be installed in the [Federation Name] Cryptographic Trust Fabric. See Section 3.2 for more information about this process.

### Who Can Submit a Certificate Application

Not applicable. See Section 4.1 for more information about the [Federation Name] trust model and the rules that apply to this topic in lieu of traditional PKI rules.

### Enrollment Process and Responsibilities

Not applicable. See Section 4.1 for more information about the [Federation Name] trust model and the rules that apply to this topic in lieu of traditional PKI rules.

## Certificate Application Processing

This section and its subsections are not applicable to this CP. [FMO Name] does not operate a traditional CA, and therefore does not process applications for certificates in the traditional way. In lieu of a certificate application process, [Federation Name]stipulates a formal application and onboarding process, which is described in [[Federation Name] OPP].

After undergoing the formal application and onboarding process, a subscriber must generate its own certificate and prove possession of the private key corresponding to that certificate before [FMO Name] will allow that certificate to be installed in the [Federation Name] Cryptographic Trust Fabric. See Section 3.2 for more information about this process.

### Performing Identification and Authentication Functions

Not applicable. See Section 4.2 for more information about the [Federation Name] trust model and the rules that apply to this topic in lieu of traditional PKI rules.

### Approval or Rejection of Certificate Applications

Not applicable. See Section 4.2 for more information about the [Federation Name] trust model and the rules that apply to this topic in lieu of traditional PKI rules.

### Time to Process Certificate Applications

Not applicable. See Section 4.2 for more information about the [Federation Name] trust model and the rules that apply to this topic in lieu of traditional PKI rules.

## Certificate Issuance

This section and its subsections are not applicable to this CP. [FMO Name] does not operate a traditional CA, and therefore does not issue certificates in the traditional way. In lieu of a certificate application process, [Federation Name] stipulates a formal application and onboarding process, which is described in [[Federation Name] OPP].

After undergoing the formal application and onboarding process, a subscriber must generate its own certificate and prove possession of the private key corresponding to that certificate before [FMO Name] will allow that certificate to be installed in the [Federation Name] Cryptographic Trust Fabric. See Section 3.2 for more information about this process.

### CA Actions during Certificate Issuance

Not applicable. See Section 4.3 for more information about the [Federation Name] trust model and the rules that apply to this topic in lieu of traditional PKI rules.

### Notification to Subscriber by the CA Of Issuance Of Certificate

Not applicable. See Section 4.3 for more information about the [Federation Name] trust model and the rules that apply to this topic in lieu of traditional PKI rules.

## Certificate Acceptance

In a traditional PKI, the intent of certificate acceptance is for a CA to give a subscriber an opportunity to review a certificate and “accept” it before the CA formally publishes the certificate. [FMO Name] does not operate a traditional CA, and therefore does not provide a facility for subscribers to accept certificates in the traditional way. In lieu of a traditional PKI certificate acceptance process, [Federation Name] uses an alternative acceptance process wherein [FMO Name] allows a member to review any change to the [Federation Name] Cryptographic Trust Fabric that affects one or more of that member’s certificates.[[6]](#footnote-6) This allows the member to confirm whether the change is correct, and helps to prevent incorrect information from being formally published in the [Federation Name] Cryptographic Trust Fabric.

### Conduct Constituting Certificate Acceptance

[FMO Name] shall notify the subscriber via email to the subscriber’s designated point(s) of contact when requesting acceptance of a change to the [Federation Name] Cryptographic Trust Fabric. The email shall either contain the proposed revision to the [Federation Name] Cryptographic Trust Fabric as either an attachment or a pointer (URL) to a location where the revision can be downloaded and inspected.

The subscriber shall notify [FMO Name] via an email reply as soon as possible to indicate whether it formally accepts the Trust Fabric change. If the subscriber does not reply to [FMO Name] within three (3) business days after receiving the request for acceptance, [FMO Name] may proceed with the publication of the revised Trust Fabric as if the subscriber had formally accepted it.

### Publication of the Certificate by the CA

After receiving notice of the subscriber’s formal acceptance of the revised Trust Fabric, [FMO Name] shall publish the updated [Federation Name] Cryptographic Trust Fabric as indicated in Section 2.1.

### Notification of Certificate Issuance by the CA to Other Entities

After publishing the [Federation Name] Cryptographic Trust Fabric, [FMO Name] shall notify all subscribers about the update to the [Federation Name] Cryptographic Trust Fabric, as per the instructions in [GFIPM Trust].

## Key Pair and Certificate Usage

This section describes acceptable and prohibited usage of certificates to which this CP applies, as well as the public/private key pairs corresponding to those certificates.

### Subscriber Private Key and Certificate Usage

[Federation Name] members may use certificates to which this CP applies, as well as their corresponding private keys, for the following purposes.

1. Cryptographic signing of messages that are to be sent between trusted software service endpoints within [Federation Name] as part of transactions that conform to [GFIPM U2S Profile] or [GFIPM S2S Profile].
2. Decryption of encrypted messages or encrypted parts of messages sent between trusted software service endpoints within [Federation Name] as part of transactions that conform to [GFIPM U2S Profile] or [GFIPM S2S Profile].

In addition, [FMO Name] may use a certificate to which this CP applies, as well as its corresponding private key, for the purpose of cryptographically signing the [Federation Name] Cryptographic Trust Fabric document.

All other uses are prohibited.

### Relying Party Public Key and Certificate Usage

Relying parties may use certificates to which this CP applies, as well as their corresponding public keys, for the following purposes.

1. Verification of digital cryptographic signatures on messages sent between trusted software service endpoints within [Federation Name] as part of transactions that conform to [GFIPM U2S Profile] or [GFIPM S2S Profile].
2. Encryption of messages or parts of messages that are to be sent between trusted software service endpoints within [Federation Name] as part of transactions that conform to [GFIPM U2S Profile] or [GFIPM S2S Profile].
3. Verification of [FMO Name]’s digital cryptographic signature on the [Federation Name] Cryptographic Trust Fabric document.

All other uses are prohibited.

## Certificate Renewal

[FMO Name] does not operate a traditional CA, and therefore does not renew certificates in the traditional way. In lieu of a traditional PKI certificate renewal process, [Federation Name] renews a subscriber’s certificate by installing the new certificate in the [Federation Name] Cryptographic Trust Fabric as a replacement for the previously installed certificate that the new certificate is replacing. Note that it is the responsibility of the subscriber to generate the new certificate and provide [FMO Name] with a copy of it, along with a request for renewal.

The action of installing the new certificate in the [Federation Name] Cryptographic Trust Fabric indicates that the subscriber has met all the requirements of the [Federation Name] application and onboarding processes as defined in [[Federation Name] OPP]. It also indicates that the subscriber has proven possession of the private key corresponding to that certificate, as per the process described in Section 3.2. [FMO Name] shall not install a certificate in the [Federation Name] Cryptographic Trust Fabric until after the subscriber has completed these steps. Note, however, that for circumstances in which a subscriber renews a certificate but does not change the private key on which the certificate is based, the proof-of-possession process described in Section 3.2 is unnecessary.

### Circumstance for Certificate Renewal

A subscriber may request certificate renewal upon any of the following circumstances.

1. A certificate in the [Federation Name] Cryptographic Trust Fabric, belonging to the subscriber, is within 120 days of expiration.
2. A change to the [Federation Name] technical specifications necessitates a certificate renewal.

Note that certificate renewal is distinct from certificate re-key, certificate modification, certificate revocation, and certificate suspension. Please see other subsections of Section 4 for more information about how this CP addresses these other certificate lifecycle management events.

### Who May Request Renewal

[FMO Name] shall honor any request for certificate renewal that comes from a representative of the subscriber for which the request is made, provided that the request contains a new certificate with an effective date that is no later than the present date and an expiration date that is later than the expiration date of the certificate that this new certificate is intended to replace.

In addition, [FMO Name] itself may initiate the renewal process for any certificate in the [Federation Name] Cryptographic Trust Fabric when appropriate, as per the circumstances outlined in Section 4.6.1.

### Processing Certificate Renewal Requests

[FMO Name] shall process each certificate renewal request within 15 days of receiving the request, and shall ensure that the renewal process is complete no less than 15 days before the expiration date of the certificate that the renewal request is intended to replace.

Note that the certificate renewal process is not intended for use in scenarios in which an urgent change to the [Federation Name] Cryptographic Trust Fabric is required for security reasons. In such scenarios, the certificate re-key process (Section 4.7) or certificate revocation process (Section 4.9) is more appropriate.

### Notification of New Certificate Issuance to Subscriber

Not applicable. See Section 4.6 for more information about the [Federation Name] trust model and the rules that apply to this topic in lieu of traditional PKI rules.

### Conduct Constituting Acceptance of a Renewal Certificate

[FMO Name] shall notify the subscriber via email to the subscriber’s designated point(s) of contact when requesting acceptance of a change to the [Federation Name] Cryptographic Trust Fabric due to certificate renewal. The email shall contain the proposed revision to the [Federation Name] Cryptographic Trust Fabric as either an attachment or a pointer (URL) to a location where the revision can be downloaded and inspected.

The subscriber shall notify [FMO Name] via an email reply as soon as possible to indicate whether it formally accepts the Trust Fabric change. If the subscriber does not reply to [FMO Name] within three (3) business days after receiving the request for acceptance, [FMO Name] may proceed with the publication of the revised Trust Fabric as if the subscriber had formally accepted it.

### Publication of the Renewal Certificate by the CA

After renewing a subscriber’s certificate and installing it in the [Federation Name] Cryptographic Trust Fabric, [FMO Name] shall publish the updated [Federation Name] Cryptographic Trust Fabric at the URL designated in Section 2.1.

### Notification of Certificate Issuance by the CA to Other Entities

After renewing a subscriber’s certificate, installing it in the [Federation Name] Cryptographic Trust Fabric, and publishing the [Federation Name] Cryptographic Trust Fabric at its designated URL, [FMO Name] shall notify all subscribers about the update to the [Federation Name] Cryptographic Trust Fabric, as per the instructions in [GFIPM Trust].

## Certificate Re-Key

[FMO Name] does not operate a traditional CA, and therefore does not re-key certificates in the traditional way. In lieu of a traditional PKI certificate re-key process, [Federation Name] re-keys a subscriber’s certificate by installing the new certificate in the [Federation Name] Cryptographic Trust Fabric as a replacement for the previously installed certificate that the new certificate is replacing. Note that it is the responsibility of the subscriber to generate the new public/private key pair and certificate, provide [FMO Name] with a copy of it, and prove possession of the private key as per the process described in Section 3.2.

The action of installing the new certificate in the [Federation Name] Cryptographic Trust Fabric indicates that the subscriber has met all the requirements of the [Federation Name] application and onboarding processes as defined in [[Federation Name] OPP]. It also indicates that the subscriber has proven possession of the private key corresponding to that certificate, as per the process described in Section 3.2. [FMO Name] shall not install a certificate in the [Federation Name] Cryptographic Trust Fabric until after the subscriber has completed these steps.

### Circumstance for Certificate Re-Key

A subscriber may request certificate renewal upon any of the following circumstances.

1. A certificate in the [Federation Name] Cryptographic Trust Fabric, belonging to the subscriber, is within 120 days of expiration.
2. The public/private key pair corresponding to a certificate in the [Federation Name] Cryptographic Trust Fabric, belonging to the subscriber, is within 120 days of expiration in accordance with the subscriber’s local policy pertaining to maximum key lifetime.
3. The private key corresponding to a certificate in the [Federation Name] Cryptographic Trust Fabric has been compromised, or is suspected of having been compromised.
4. A change to the [Federation Name] technical specifications necessitates a certificate re-key.

### Who May Request Certification of a New Public Key

Any subscriber representative may request certificate re-key for any certificate in the [Federation Name] Cryptographic Trust Fabric, as per the circumstances outlined in Section 4.7.1. When making the re-key request, the subscriber shall indicate whether the request is being made as the result of a private key compromise or suspected private key compromise. If key compromise has occurred or is suspected, all parties involved shall treat the re-key request as urgent and cooperate to complete the re-key process as quickly as possible.

In addition, [FMO Name] may initiate the re-key process for any certificate in the [Federation Name] Cryptographic Trust Fabric when appropriate, as per the circumstances outlined in Section 4.7.1.

### Processing Certificate Re-Keying Requests

For a non-urgent certificate re-key request, [FMO Name] shall process the request within 15 days of receiving the request, and shall ensure that the renewal process is complete no less than 15 days before the expiration date of the public/private key pair corresponding to the certificate that the re-key request is intended to replace.

For an urgent re-key request, [FMO Name] shall process the request in two separate parts:

1. Immediate revocation of the compromised certificate, performed in accordance with the rules specified in Section 4.9; and
2. Acceptance of a new certificate, with a new public/private key pair, to replace the compromised certificate, performed in accordance with the rules specified in Sections 4.4 and 3.2.1.

### Notification of New Certificate Issuance To Subscriber

Not applicable. See Section 4.7 for more information about the [Federation Name] trust model and the rules that apply to this topic in lieu of traditional PKI rules.

### Conduct Constituting Acceptance of a Re-Keyed Certificate

[FMO Name] shall notify the subscriber via email to the subscriber’s designated point(s) of contact when requesting acceptance of a change to the [Federation Name] Cryptographic Trust Fabric due to certificate re-key. The email shall either contain the proposed revision to the [Federation Name] Cryptographic Trust Fabric as either an attachment or a pointer (URL) to a location where the revision can be downloaded and inspected.

The subscriber shall notify [FMO Name] via an email reply as soon as possible to indicate whether it formally accepts the Trust Fabric change. If the subscriber does not reply to [FMO Name] within three (3) business days after receiving the request for acceptance, [FMO Name] may proceed with the publication of the revised Trust Fabric as if the subscriber had formally accepted it.

### Publication of the Re-Keyed Certificate by the CA

After performing a re-key operation on a subscriber’s certificate and installing it in the [Federation Name] Cryptographic Trust Fabric, [FMO Name] shall publish the updated [Federation Name] Cryptographic Trust Fabric at the URL designated in Section 2.1.

### Notification of Certificate Issuance by the CA to Other Entities

After performing a re-key operation on a subscriber’s certificate, installing the updated certificate in the [Federation Name] Cryptographic Trust Fabric, and publishing the [Federation Name] Cryptographic Trust Fabric at its designated URL, [FMO Name] shall notify all subscribers about the update to the [Federation Name] Cryptographic Trust Fabric, as per the instructions in [GFIPM Trust].

## Certificate Modification

[FMO Name] does not operate a traditional CA, and therefore does not modify certificates in the traditional way. In lieu of a traditional PKI certificate modification process, [Federation Name] modifies a subscriber’s certificate by installing a new certificate in the [Federation Name] Cryptographic Trust Fabric as a replacement for the previously installed certificate that the new certificate is modifying. Note that it is the responsibility of the subscriber to generate the new certificate and provide [FMO Name] with a copy of it, along with a request for modification.

The action of installing the new certificate in the [Federation Name] Cryptographic Trust Fabric indicates that the subscriber has met all the requirements of the [Federation Name]application and onboarding processes as defined in [[Federation Name] OPP]. It also indicates that the subscriber has proven possession of the private key corresponding to that certificate, as per the process described in Section 3.2. [FMO Name] shall not install a certificate in the [Federation Name] Cryptographic Trust Fabric until after the subscriber has completed these steps. Note, however, that for circumstances in which a subscriber modifies a certificate but does not change the private key on which the certificate is based, the proof-of-possession process described in Section 3.2 is unnecessary.

### Circumstance for Certificate Modification

Due to [Federation Name]’s non-traditional trust model, there are few circumstances that would require certificate modification, insofar as certificate modification is considered separately from certificate renewal or certificate re-key. The only circumstances that would precipitate certificate modification are those in which an attribute of the existing certificate, other than the expiration date, needs to be changed. For example, a subscriber may request modification of its certificate(s) to update the “subject” attribute if its name (the name of the organization) changes. This is clearly a rare circumstance; nevertheless, it can sometimes occur.

### Who May Request Certificate Modification

[FMO Name] shall honor any request for certificate modification that comes from a representative of the subscriber for which the request is made, provided that the request contains a new certificate with the appropriate attribute(s) modified. If the new certificate contains a modified expiration date or a modified public key, then the request shall be handled as a certificate renewal or a certificate re-key, respectively.

In addition, [FMO Name] itself may initiate the modification process for any certificate in the [Federation Name] Cryptographic Trust Fabric when appropriate, as per the circumstances outlined in Section 4.8.1.

### Processing Certificate Modification Requests

[FMO Name] shall process each certificate modification request within 15 days of receiving the request.

Note that the certificate modification process is not intended for use in scenarios in which an urgent change to the [Federation Name] Cryptographic Trust Fabric is required for security reasons. In such scenarios, the certificate re-key process (Section 4.7) or certificate revocation process (Section 4.9) is more appropriate.

### Notification of New Certificate Issuance to Subscriber

Not applicable. See Section 4.8 for more information about the [Federation Name] trust model and the rules that apply to this topic in lieu of traditional PKI rules.

### Conduct Constituting Acceptance of Modified Certificate

[FMO Name] shall notify the subscriber via email to the subscriber’s designated point(s) of contact when requesting acceptance of a change to the [Federation Name] Cryptographic Trust Fabric due to certificate modification. The email shall either contain the proposed revision to the [Federation Name] Cryptographic Trust Fabric as either an attachment or a pointer (URL) to a location where the revision can be downloaded and inspected.

The subscriber shall notify [FMO Name] via an email reply as soon as possible to indicate whether it formally accepts the Trust Fabric change. If the subscriber does not reply to [FMO Name] within three (3) business days after receiving the request for acceptance, [Federation Name] may proceed with the publication of the revised Trust Fabric as if the subscriber had formally accepted it.

### Publication of the Modified Certificate by the CA

After modifying a subscriber’s certificate and installing it in the [Federation Name] Cryptographic Trust Fabric, [FMO Name] shall publish the updated [Federation Name] Cryptographic Trust Fabric at the URL designated in Section 2.1.

### Notification of Certificate Issuance by the CA to Other Entities

After modifying a subscriber’s certificate, installing it in the [Federation Name] Cryptographic Trust Fabric, and publishing the [Federation Name] Cryptographic Trust Fabric at its designated URL, [FMO Name] shall notify all subscribers about the update to the [Federation Name] Cryptographic Trust Fabric, as per the instructions in [GFIPM Trust].

## Certificate Revocation and Suspension

[Federation Name] does not employ a traditional PKI trust model, and does not issue subscriber certificates under this CP, so the traditional PKI concept of certificate revocation or suspension is not applicable to this CP. The [Federation Name] trust model does prescribe appropriate actions to prevent relying parties from trusting a certificate that is known or suspected to have been compromised; however, rather than using certificate revocation to accomplish this goal, [Federation Name] accomplishes it via removal of a certificate from the [Federation Name] Cryptographic Trust Fabric. The processes and mechanisms surrounding certificate revocation in [Federation Name] are described in this section.

### Circumstances for Revocation

Any subscriber may request certificate revocation upon any of the following circumstances.

1. A certificate in the [Federation Name] Cryptographic Trust Fabric has expired.
2. The private key corresponding to a certificate in the [Federation Name] Cryptographic Trust Fabric has been compromised, or is suspected of having been compromised.
3. A subscriber wishes to no longer participate as a member of [Federation Name]. (See Section 4.11 for more information.)

### Who Can Request Revocation

Any subscriber representative may request certificate revocation for any certificate in the [Federation Name] Cryptographic Trust Fabric, subject to the request procedure described in Section 4.9.3. When receiving a request for certificate revocation, [FMO Name] shall follow the rules described in Section 3.4 regarding identification and authentication of the person making the revocation request.

In addition, [FMO Name] itself may initiate the revocation process for any certificate in the [Federation Name] Cryptographic Trust Fabric when appropriate, as per the circumstances outlined in Section 4.9.1.

### Procedure for Revocation Request

At any time, any subscriber representative (“requesting subscriber”) may request that a specific certificate be removed from the [Federation Name] Cryptographic Trust Fabric by contacting [FMO Name] at the point of contact specified in Section 1.5.2.

[FMO Name] shall respond to a revocation request as follows.

1. If the subscriber to which the certificate in question belongs (“affected subscriber”) is the same as the requesting subscriber, [FMO Name] shall immediately remove the certificate from the [Federation Name] Cryptographic Trust Fabric, republish the [Federation Name] Cryptographic Trust Fabric without the certificate, and notify all subscribers, as per the instructions in [GFIPM Trust].
2. If the affected subscriber is not the same as the requesting subscriber, [FMO Name] shall immediately contact a representative of the affected subscriber and notify that person of the requesting subscriber‘s request for removal. If the affected subscriber concedes to the removal of the certificate in question, [FMO Name] shall immediately remove the certificate from the [Federation Name] Cryptographic Trust Fabric, republish the [Federation Name] Cryptographic Trust Fabric without the certificate, and notify all subscribers, as per the instructions in [GFIPM Trust]. But if the affected subscriber disputes the requesting subscriber’s claim, then [FMO Name] shall treat the matter as a dispute between the subscribers and resolve it as per [[Federation Name] Governance] and [[Federation Name] OPP].

### Revocation Request Grace Period

In general, [FMO Name] shall not implement any revocation request grace period. In the case of a dispute between subscribers that arises over a revocation request, [[Federation Name] Governance] and [[Federation Name] OPP] shall govern the resolution process. See Section 4.9.3, as well as [[Federation Name] Governance] and [[Federation Name] OPP], for more information.

### Time within Which CA Must Process the Revocation Request

[FMO Name] shall process a revocation request as soon as reasonably possible, and under no circumstances shall [FMO Name] wait longer than one business day after receiving the request, before processing it.

For requests that affect a subscriber other than the requesting subscriber, the affected subscriber must provide an initial acknowledgment of the revocation request as soon as reasonably possible, and under no circumstances shall the affected subscriber wait longer than one business day after receiving the request, before providing an initial acknowledgment of it.

Due to the time-sensitive and security-critical nature of certificate revocation requests, it is important that [FMO Name] and all subscribers treat certificate revocation requests with utmost urgency, so that requests can be resolved as quickly as possible.

### Revocation Checking Requirement for Relying Parties

In the [Federation Name] trust model, certificate “revocation” is communicated via the publication of a new [Federation Name] Cryptographic Trust Fabric document and notification of subscribers about the publication of the new document. Subscribers must update their systems to use the new [Federation Name] Cryptographic Trust Fabric as soon as possible, but no later than one business day after receiving the notification.

### CRL Issuance Frequency (If Applicable)

Not applicable. [FMO Name] does not issue or revoke certificates, and therefore does not issue a CRL. [FMO Name] communicates certificate revocations via the [Federation Name] Cryptographic Trust Fabric, which is updated as needed. [FMO Name] also notifies subscribers about updates to the [Federation Name] Cryptographic Trust Fabric document when it is updated.

### Maximum Latency for CRLs (If Applicable)

Not applicable.

### On-Line Revocation/Status Checking Availability

Not applicable. [FMO Name] does not issue or revoke certificates, and therefore does not provide an online certificate revocation status checking service. [FMO Name] communicates certificate revocations via the [Federation Name] Cryptographic Trust Fabric, which is updated as needed. [FMO Name] also notifies subscribers about updates to the [Federation Name] Cryptographic Trust Fabric document when it is updated.

### On-Line Revocation Checking Requirements

[FMO Name] does not issue or revoke certificates, and therefore does not provide an online certificate revocation status checking service. [FMO Name] communicates certificate revocations via the [Federation Name] Cryptographic Trust Fabric, which is updated as needed. Subscribers must update their systems to use the new [Federation Name] Cryptographic Trust Fabric as soon as possible, but no later than one business day after receiving the notification.

### Other Forms of Revocation Advertisements Available

[FMO Name] communicates certificate revocations via the [Federation Name] Cryptographic Trust Fabric, which is updated as needed. [FMO Name] also notifies subscribers about updates to the [Federation Name] Cryptographic Trust Fabric document when it is updated. Subscribers must update their systems to use the new [Federation Name] Cryptographic Trust Fabric as soon as possible, but no later than one business day after receiving the notification.

### Special Requirements Re Key Compromise

Not applicable.

### Circumstances for Suspension

[FMO Name] handles suspension from the federation via removal from the [Federation Name] Cryptographic Trust Fabric, which has been described in detail throughout Section 4.9.

A subscriber may be suspended by [FMO Name] at any time, and for any reason, at the discretion of [FMO Name]. At any time after a suspension has occurred, the subscriber may be reinstated via reinsertion into the [Federation Name] Cryptographic Trust Fabric, also at the discretion of [FMO Name]. Reinstatement may require new certificate(s) to be generated by the subscriber, depending on the specific circumstances surrounding the suspension.

All disputes arising out of the suspension of a subscriber shall be handled via the procedure described in [[Federation Name] Governance] and [[Federation Name] OPP].

### Who Can Request Suspension

Any subscriber representative, [Federation BODA Name] member, or [Federation EC Name] member may request suspension of a subscriber.

### Procedure for Suspension Request

To request suspension of a subscriber, the requestor must contact [FMO Name] in writing at the address or email address specified in Section 1.5.2. The suspension request must include a justification for requesting the suspension. See [[Federation Name] Governance] and [[Federation Name] Center OPP] for more information.

### Limits on Suspension Period

See [[Federation Name] Governance] and [[Federation Name] OPP].

## Certificate Status Services

The concept of certificate status is not applicable in [Federation Name]. [FMO Name] communicates certificate status to subscribers implicitly via inclusion or non-inclusion of a certificate in the [Federation Name] Cryptographic Trust Fabric.

### Operational Characteristics

Not applicable. See Section 4.10.

### Service Availability

Not applicable. See Section 4.10.

### Optional Features

Not applicable. See Section 4.10.

## End of Subscription

Termination of subscription to this CP by a subscriber shall trigger the immediate removal of all certificates belonging to the subscriber from the [Federation Name] Cryptographic Trust Fabric. In the event that a subscriber notifies [FMO Name] of its desire to end its subscription to this CP, [FMO Name] shall use the certificate revocation process described in Section 4.9 to revoke all certificates belonging to the subscriber.

## Key Escrow and Recovery

Key escrow is unnecessary in [Federation Name], because certificates governed by this CP are used only for digital signatures and encryption of messages during secure information exchanges. Certificates governed by this CP are not to be used for encryption of data-at-rest on subscriber systems.

### Key Escrow and Recovery Policy and Practices

Not applicable. See Section 4.12.

### Session Key Encapsulation and Recovery Policy and Practices

Not applicable. See Section 4.12.

# Facility, Management, and Operational Controls

This section and its subsections address issues relating to the physical facility in which sensitive key material is housed by subscribers, as well as subscribers’ operational controls relating to personnel.

## Physical Controls

As part of the [Federation Name] application and onboarding processes (see [[Federation Name] OPP]), subscribers shall fully disclose their local security policies and practices, including those related to physical controls.

When not in use, tokens and any activation information used by subscribers to access or enable cryptographic modules shall be placed in locked containers.

Subscriber servers, workstations, and other sensitive components must be located in an environment that prevents unauthorized access to equipment and records. Subscribers must use facilities that are protected with intrusion alarms regardless of assurance level.

### Site Location and Construction

The location and construction of the facility housing subscriber equipment and operations shall be locked at all times and require restricted access. The subscriber approves the authorized list of personnel into this facility.

### Physical Access

Subscriber equipment shall always be protected from unauthorized access and subversion in a manner commensurate to the data in question. Additionally, these security mechanisms shall be commensurate with the level of threat in the equipment environment.

### Power and Air Conditioning

Facilities housing subscriber equipment shall be supplied with power and environmental controls sufficient to provide reliable operation. Additionally, personnel areas must be supplied with sufficient facilities to satisfy operational requirements.

The subscriber equipment shall provide backup capabilities sufficient to automatically lockout input, complete pending operations, and record the state of the equipment and process prior to the disruption of power or environmental control systems. The subscriber shall be provided with uninterrupted power sufficient for a minimum of 10 minutes operation in the absence of commercial power, immediately followed by automated processes to support graceful shutdown of subscriber operations.

### Water Exposures

There is no stipulation concerning water exposure of the subscriber aside from best business practices of safeguarding such equipment. All equipment shall be maintained in a manner that prevents dangerous exposure to water, e.g. elevating equipment preventing such damage, such as raised floors. Also, if fire sprinklers are present, a subscriber recovery contingency plan shall be devised in case of a sprinkler malfunction or sprinkler deployment.

### Fire Prevention and Protection

There is no stipulation concerning fire prevention and protection aside from best business practices. Each subscriber shall maintain a recovery contingency plan in case of damage due to fire.

### Media Storage

Subscriber media shall be stored to safeguard against accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a separate location from the original media.

### Waste Disposal

All sensitive documents generated as a result of [Federation Name]membership and participation in [Federation Name]shall be shredded.

Sensitive equipment that is no longer in operation and considered to be waste shall be destroyed in a particular manner rendering the equipment impossible to reuse. In cases where data is involved (hard drives, tokens etc.), including all media storage as referenced in Section 5.1.6, the data shall be destroyed in a manner that prevents data recovery. Two trusted individuals shall be designated to perform the destruction.

### Off-Site Backup

System backups sufficient to recover from system failure shall be provided on a periodic schedule. However, see Sections 6.2.4 and 6.2.5 about backup provisions related to private keys governed by this CP.

## Procedural Controls

As part of the [Federation Name] application and onboarding processes (see [[Federation Name] OPP]), subscribers must fully disclose their local security policies and practices, including those related to procedural controls.

### Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be responsible for their designated actions or the integrity of the [Federation Name] Cryptographic Trust Fabric is weakened. Functions performed in these roles form the basis of trust for all uses of the [Federation Name] Cryptographic Trust Fabric.

Subscribers to this CP shall maintain a list of appropriate trusted roles, per the local procedural controls that they implement. Examples of trusted roles include the following. Note that the examples below are for illustrative purposes only; each subscriber defines its own list of trusted roles.

1. **Master User** – Authorized to install, configure and maintain all system components; perform system backup and recovery; and generate private keys used by system components.
2. **Security Officer**– Authorized to configure profiles and audit parameters; and establish policy.
3. **Auditor** – Authorized to view and maintain audit logs.

### Number of Persons Required Per Task

To ensure the integrity of subscriber operations, it is recommended that wherever possible, a separate individual be identified for each trusted role. Additionally, redundancy of personnel should also be observed in support of subscriber operations in the event of personnel absence.

### Identification and Authentication for Each Role

An individual shall be required to identify and authenticate himself/herself before being permitted to perform any actions set forth by the subscriber for that role or identity.

### Roles Requiring Separation of Duties

No stipulation.

## Personnel Controls

As part of the [Federation Name] application and onboarding processes (see [[Federation Name] OPP]), subscribers must fully disclose their local security policies and practices, including those related to personnel controls.

### Qualifications, Experience, and Clearance Requirements

Each subscriber shall positively identify and maintain an up-to-date list of the individuals that are responsible and accountable for the management of the subscriber’s operational environment. In addition, persons selected to fill trusted roles shall be chosen on the basis of loyalty, trustworthiness, and integrity.

### Background Check Procedures

Each subscriber shall implement a background check procedure to demonstrate that requirements set forth in Section 5.3.1 are met. Such procedures shall be performed solely to determine the suitability of a person to fill a trusted role as defined by a subscriber.

### Training Requirements

Each subscriber shall implement a policy whereby all personnel performing duties in trusted roles, with respect to the operation of any equipment containing certificates or private keys governed by this CP, shall receive comprehensive training. Training shall be conducted in the following areas.

1. All certificate management duties they are expected to perform
2. Operation of certificate management software and hardware in use on the system
3. Disaster recovery, incident response and business continuity procedures

### Retraining frequency and requirements

Each subscriber shall implement a policy whereby all personnel acting in trusted roles shall be aware of changes in the subscriber’s operation that may occur as a result of changes in the subscriber’s local security policy or changes to this CP.

### Job Rotation Frequency and Sequence

There is no stipulation for job frequency and sequence within the CA. However, local rules and regulations shall apply.

### Sanctions for Unauthorized Actions

Each subscriber shall take appropriate administrative and disciplinary actions against personnel who have performed actions that are not authorized in this CP and could result in security vulnerabilities for the subscriber or other [Federation Name] members. This may include revocation of digital credentials.

### Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to each subscriber’s operational environment shall meet applicable requirements set forth in this CP.

### Documentation Supplied To Personnel

Each subscriber shall make available to appropriate personnel the certificate policies it supports, as well as any relevant statutes, policies, or contracts that apply to the person’s duties.

## Audit Logging Procedures

All subscribers to this CP shall generate audit log files for all events relating to the security of the subscriber’s systems. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

In addition, as part of the [Federation Name] application and onboarding processes (see [[Federation Name] OPP]), subscribers must fully disclose their local audit logging policies and procedures.

### Types of Events Recorded

No stipulation.

### Frequency of Processing Log

No stipulation.

### Retention Period for Audit Log

No stipulation.

### Protection of Audit Log

No stipulation.

### Audit Log Backup Procedures

No stipulation.

### Audit Collection System (Internal Vs. External)

No stipulation.

### Notification to Event-Causing Subject

No stipulation.

### Vulnerability Assessments

No stipulation.

## Records Archival

As part of the [Federation Name] application and onboarding processes (see [[Federation Name] OPP]), subscribers must fully disclose their local security policies and practices, including those related to records archival.

### Types of Records Archived

No stipulation.

### Retention Period for Archive

No stipulation.

### Protection of Archive

No stipulation.

### Archive Backup Procedures

No stipulation.

### Requirements for Time-Stamping Of Records

No stipulation.

### Archive Collection System (Internal or External)

No stipulation.

### Procedures to Obtain and Verify Archive Information

No stipulation.

## Key Changeover

As part of the [Federation Name] application and onboarding processes (see [[Federation Name] OPP]), subscribers must fully disclose their local security policies and practices, including those related to key changeover.

## Compromise and Disaster Recovery

As part of the [Federation Name] application and onboarding processes (see [[Federation Name] OPP]), subscribers must fully disclose their local security policies and practices, including those related to compromise and disaster recovery.

### Incident and Compromise Handling Procedures

As part of its incident and compromise handling procedures, each subscriber shall implement a procedure whereby it contacts [FMO Name] promptly upon discovery of any incident in which private key material governed by this CP was, or might have been, compromised.

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

As part of its incident and compromise handling procedures, each subscriber shall implement a procedure whereby it contacts [FMO Name] promptly upon discovery of any incident in which private key material governed by this CP was, or may have been, compromised.

### Entity Private Key Compromise Procedures

As part of its incident and compromise handling procedures, each subscriber shall implement a procedure whereby it contacts [FMO Name] promptly upon discovery of any incident in which private key material governed by this CP was, or may have been, compromised.

### Business Continuity Capabilities after a Disaster

No stipulation.

## CA or RA Termination

The topics of certificate authority (CA) and registration authority (RA) termination are not applicable to this CP, because the concepts of CA and RA are not applicable to this CP in the context in which they are addressed within this section.

# Technical Security Controls

This section contains rules representing the minimal acceptable level of technical protection that must be applied to sensitive private key material corresponding to certificates covered by this CP and the systems on which the private key material is used. To help ensure the trustworthiness of the [Federation Name] Cryptographic Trust Fabric, all subscribers must obey the rules outlined in this section.

In some circumstances, a subscriber may already have policies and procedures in place that preclude their ability to obey these rules. In this circumstance, the subscriber must notify [FMO Name] in writing of its inability to meet these requirements, and must also provide an explanation of why it is unable to meet the requirements.

## Key Pair Generation and Installation

This section and its subsections stipulate public/private key pair generation and installation rules for key pairs that correspond to certificates covered by this CP.

### Key Pair Generation

The key pair must be generated by the subscriber using the RSA key generation algorithm[[7]](#footnote-7), and must be generated on the physical machine or module within which it will be used. In addition, private key material must not appear outside of the module from which it was generated unless it is encrypted for local transmission or for processing or storage by a key recovery mechanism.

### Private Key Delivery to Subscriber

This section is not applicable, since the subscriber is responsible for generating the key pair and maintains physical possession of it at all times. (See Section 6.1.1)

### Public Key Delivery to Certificate Issuer

This section is not applicable, as the [Federation Name] trust model does not include the traditional PKI concept of a certificate issuer. Sections 3 and 4 describe the [Federation Name] trust model in detail, including provisions for delivery of the subscriber’s public key from the subscriber to [FMO Name].

### CA Public Key Delivery to Relying Parties

This section is not applicable, as the [Federation Name] trust model does not include the traditional PKI concept of a certificate authority. Sections 3 and 4 describe the [Federation Name] trust model in detail, including provisions for delivery of the subscriber’s public key from [FMO Name] to relying parties via publication of the [Federation Name] Cryptographic Trust Fabric.

### Key Sizes

All certificates governed by this CP shall use at least 2048-bit RSA and Secure Hash Algorithm 256 (SHA-256).

If [FMO Name] determines that the security of a particular algorithm may be compromised, it shall immediately revoke all certificates that use the algorithm.

### Public Key Parameters Generation and Quality Checking

Public key parameters shall be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used.

### Key Usage Purposes (As Per X.50vkey Usage Field)

See Sections 1.4.1 and 4.5. In general, keys may be used for signing, encryption, or both. For keys that appear in the [Federation Name] Cryptographic Trust Fabric, key usage is indicated by other attributes in the [Federation Name] Cryptographic Trust Fabric document. For the key that [FMO Name] uses to sign the [Federation Name] Cryptographic Trust Fabric, key usage is limited to generating digital signatures for the [Federation Name] Cryptographic Trust Fabric.

## Private Key Protection and Cryptographic Module Engineering Controls

Not applicable.

### Cryptographic Module Standards and Controls

Cryptographic modules employed for the generation and operational use of public/private key pairs corresponding to certificates governed by this CP must conform to Security Level 1 or higher as specified in [FIPS 140-2].[[8]](#footnote-8)

### Private Key (N out of M) Multi-Person Control

No stipulation.

### Private Key Escrow

Not applicable. Key escrow is unnecessary in [Federation Name], because certificates governed by this CP are used only for encryption of data-in-transit during secure information exchanges. Certificates governed by this CP are not to be used for encryption of data-at-rest on subscriber systems.

### Private Key Backup

Copies of private keys governed by this CP are strongly discouraged, but may be made to provide a backup in the event of destruction or failure of the original. A subscriber’s private keys, if backup is required, will require multi-person control. If undertaking a private key backup procedure, a subscriber must do so in a fashion that ensures proper accountability for all actions performed. The subscriber shall identify the location of the backup, the specific roles required to complete the process, and the constraints for which the process is performed.

### Private Key Archival

Private keys governed by this CP shall not be archived.

### Private Key Transfer Into or From a Cryptographic Module

Private keys governed by this CP shall be generated by and remain in a cryptographic module. Private keys may be backed up in accordance with the rules stipulated in Section 6.2.4.

In the event a private key, generated by and in a cryptographic module, must be transported into another cryptographic module, the second or recipient module must have equal or greater security controls, the private key must be encrypted during transport, and private key material must not exist in plaintext outside the boundaries of the source or destination cryptographic modules.

### Private Key Storage on Cryptographic Module

No stipulation beyond what is specified in [FIPS 140-2].

### Method of Activating Private Key

Private keys corresponding to certificates in the [Federation Name] Cryptographic Trust Fabric are used for digital signature and encryption operations on information-sharing transactions between [Federation Name] members. According to previously articulated rules in this CP, these private keys must reside on secure servers, within cryptographic modules, at all times, except for certain exceptional conditions such as private key backup and transfer from one cryptographic module to another. Due to the location of these keys, it is generally infeasible for them to be activated (for example, via a passphrase) on a per-crypto-operation basis, or even on a short-term cache basis for use in crypto operations. It is therefore assumed that these keys require no method of activation, other than knowledge of the private key material.

The private key used by [FMO Name] to sign the [Federation Name] Cryptographic Trust Fabric must be maintained on an offline machine in a lab that is locked at all times and requires 2-factor access control (key card + PIN) for physical access. This private key shall require a pass-phrase or PIN for activation, and the pass-phrase or PIN shall be protected from disclosure to unauthorized personnel.

### Method of Deactivating Private Key

Due to the circumstances surrounding the use of private keys corresponding to certificates in the [Federation Name] Cryptographic Trust Fabric (see Section 6.2.8), this section is not applicable to those keys.

For the private key used by [FMO Name] to sign the [Federation Name] Cryptographic Trust Fabric, the cryptographic module shall be deactivated after use, e.g. via a manual logout procedure, or automatically after a period of inactivity.

### Method of Destroying Private Key

Private signature keys shall be destroyed in accordance with [FIPS 140-2] when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

### Cryptographic Module Rating

See Section 6.2.1.

## Other Aspects of Key Pair Management

All certificates governed by this CP shall be subject to revocation and/or re-key in the event of a personnel change in which a person previously authorized to perform trusted role operations on the corresponding private key is no longer authorized to do so.

### Public Key Archival

Public keys that appear in the [Federation Name] Cryptographic Trust Fabric are archived as part of their publication in the [Federation Name] Cryptographic Trust Fabric. Public keys corresponding to the private keys used by [FMO Name] to sign the [Federation Name] Cryptographic Trust Fabric shall be archived offline by [FMO Name].

### Certificate Operational Periods and Key Pair Usage Periods

Certificates that are governed by this CP and also appear in the [Federation Name] Cryptographic Trust Fabric shall be limited to a maximum lifetime of two (2) years. Certificates corresponding to private keys used by [FMO Name] to sign the [Federation Name] Cryptographic Trust Fabric shall be limited to a maximum lifetime of three (3) years.

See Section 4.7 for more information about the certificate re-key process.

## Activation Data

For certificates that are governed by this CP and also appear in the [Federation Name] Cryptographic Trust Fabric, this section and its subsections do not apply. (See Section 6.2.8 for more details.)

For certificates corresponding to private keys used by [FMO Name] to sign the [Federation Name] Cryptographic Trust Fabric, the following subsections apply.

### Activation Data Generation and Installation

For certificates corresponding to private keys used by [FMO Name] to sign the [Federation Name] Cryptographic Trust Fabric, the activation data used to unlock the private keys shall have an appropriate level of strength. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module. If [FMO Name] uses passwords as activation data for the private key, the activation data shall be changed upon re-key, if not more frequently.

### Activation Data Protection

For certificates corresponding to private keys used by [FMO Name] to sign the [Federation Name] Cryptographic Trust Fabric, the data used to unlock the keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be: (a) memorized biometric in nature, or (b) recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module. In addition, the protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts.

### Other Aspects of Activation Data

No stipulation.

## Computer Security Controls

As part of the [Federation Name] application and onboarding processes (see [[Federation Name] OPP]), subscribers must fully disclose their local security policies and practices, including those related to computer security controls.

### Specific Computer Security Technical Requirements

The following computer security functions shall be provided by the operating system, or through a combination of operating system, software, and physical safeguards for all computer systems on which one or more private keys governed by this CP reside.

1. Require authenticated logins.
2. Provide discretionary access control.
3. Provide non-discretionary access controls for policy-enforced operations.
4. Provide a security audit capability.
5. Enforce separation of duties for locally defined trusted roles. (See Section 5.2.1.)
6. Require identification and authentication of trusted roles and associated identities.
7. Require use of cryptography for session communication and database security.
8. Require a trusted path for identification of trusted roles and associated identities.
9. Enforce process isolation.

Subscriber equipment shall be configured and operated to activate these controls.

### Computer Security Rating

No stipulation.

## Life Cycle Technical Controls

The following life cycle technical controls pertain to all subscriber systems on which private keys governed by this CP reside.

1. The hardware and software shall be procured in a fashion that reduces the likelihood of tampering for any particular component.
2. The hardware and software shall be limited to performing [Federation Name] related security functions. This may include providing specific service endpoints at which the keys and certificates governed by this CP are used.
3. Proper care shall be taken to prevent malicious software from being loaded onto the equipment.
4. Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.
5. Chain of custody mechanisms shall be provided throughout the lifecycle of the system, to include (a) shipment and delivery of hardware and software from the purchase location to the subscriber’s physical location, (b) creation, storage, transport, or manipulation of subscriber key material, and (c) physical or logical access to subscriber systems.

### System Development Controls

No stipulation.

### Security Management Controls

For all subscriber systems on which private keys governed by this CP reside, there shall be controls pertaining to configuration, modifications, and upgrades. In addition, there shall be a mechanism on these systems for detecting unauthorized modification to the local software or configuration.

### Life Cycle Security Controls

No stipulation.

## Network Security Controls

Subscribers shall employ appropriate security measures to ensure they are guarded against subversion, denial of service and intrusion attacks. Such measures may include, but are not limited to, firewalls, intrusion detection devices, and filtering routers. Unused network ports and services shall be turned off, and any network software and user accounts present shall be restricted to the functioning of the subscriber systems.

In addition, as part of the [Federation Name] application and onboarding processes (see [[Federation Name] OPP]), subscribers must fully disclose their local security policies and practices, including those related to network security controls.

## Time-Stamping

Asserted times shall be accurate to within ten seconds. Electronic or manual procedures may be used to maintain system time; however, it is strongly recommended that subscribers configure their systems to use the Authenticated Network Time Protocol (NTP) for securely maintaining accurate time on all system clocks.[[9]](#footnote-9)

# Certificate, CRL, and OCSP Profiles

This section and its subsections pertain to certificate status management and notification mechanisms through which a CA can communicate information to relying parties about the status of a certificate. In particular, these mechanisms would allow the CA to report certificate revocations to relying parties in an efficient and timely manner. [Federation Name] does not use a traditional PKI, and therefore does not make use of any type of traditional certificate status notification mechanism. Instead, [FMO Name] relies on updates to the [Federation Name] Cryptographic Trust Fabric to report certificate revocations. This mechanism is unrelated to the topics addressed by the subsections of this section, and has already been covered in detail in Sections 3 and 4. Accordingly, this section and its subsections are not applicable to this CP.

## Certificate Profile

Not applicable.

### Version Number(s)

Not applicable.

### Certificate Extensions

Not applicable.

### Algorithm Object Identifiers

Not applicable.

### Name Forms

Not applicable.

### Name Constraints

Not applicable.

### Certificate Policy Object Identifier

Not applicable.

### Usage of Policy Constraints Extension

Not applicable.

### Policy Qualifiers Syntax and Semantics

Not applicable.

### Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

## CRL Profile

Not applicable.

### Version Number(s)

Not applicable.

### CRL and CRL Entry Extensions

Not applicable.

## OCSP Profile

Not applicable.

### Version Number(s)

Not applicable.

### OCSP Extensions

Not applicable.

# Compliance Audit and Other Assessments

This section and its subsections pertain to the topic of audits and assessments to ensure that parties to a CP are in compliance with the policy. In general, Level 2 Subscribers must perform periodic self-audits and publish the results at [Location]. Level 3 Subscribers must perform periodic independent audits and publish the results at [Location]. Also, [FMO Name] must perform periodic independent audits and publish the results at [Location]. The sections below provide additional details.

## Frequency or Circumstances of Assessment

All subscribers to this CP shall be subject to a periodic compliance audit that occurs once every 3 years at a minimum. In addition, each subscriber must conduct an initial compliance audit within 120 days of published date of the CP.

## Identity/Qualifications of Assessor

Level 2 Subscribers may either perform self-assessments or arrange for independent assessments to be performed. Level 3 Subscribers and [FMO Name] MUST arrange for independent assessments to be performed. The auditor must demonstrate competence in the field of compliance audits, and must perform such compliance audits as a primary responsibility.

## Assessor's Relationship to Assessed Entity

In the case of an independent assessment, the compliance auditor shall be either a private firm or a government agency, which is independent from the entity being audited, or it shall be organizationally separated sufficiently from that entity to provide an unbiased, independent evaluation and attestation.

## Topics Covered By Assessment

The purpose of a compliance audit shall be to verify that an entity is subject to the requirements of this CP. All aspects of the entity operation related to this CP shall be subject to compliance audit.

## Actions Taken As A Result Of Deficiency

A compliance audit may yield the result that a subscriber is not complying with its obligations, as set forth in this CP. When such a determination is made, the following actions may be exercised.

1. If the discrepancy is minor, the Compliance Auditor shall note the discrepancy as part of the Compliance Audit report; and
2. If the discrepancy is of magnitude to deny, revoke or suspend the subscriber from [Federation Name], the Compliance Auditor shall meet with a [FMO Name] representative and a subscriber representative promptly. The [FMO Name] representative shall determine how to remedy the discrepancy and discuss with the Compliance Auditor if the remedy is sufficient to permit continued participation as a member of [Federation Name]. An action plan with a distinct timeframe for implementing the remedy and a final report detailing the discrepancy, remedy and final outcome shall be required. The subscriber representative and the Compliance Auditor shall review the action plan. A final decision by the Compliance Auditor shall be binding and if, in the judgment of the Compliance Auditor, the discrepancy is still severe, [FMO Name] may revoke or suspend the subscriber from participation in [Federation Name]. The subscriber shall be allowed to continue operations for a maximum of thirty calendar days pending correction of any problems prior to revocation.

[FMO Name] and [Federation EC Name] shall review all discrepancies and then work with the subscriber to develop an action plan to remedy or sufficiently reduce any discrepancy.

## Communication of Results

After conducting an audit, a subscriber shall publish the results of the audit at [Location], so that representatives from other subscriber agencies can access and view the results.

# Other Business and Legal Matters

This section and its subsections pertain to the topic of business and legal matters that may affect this CP. Generally, these topics are beyond the scope of this CP and addressed in [[Federation Name] Governance].

## Fees

See [[Federation Name] Governance].

### Certificate Issuance or Renewal Fees

Not applicable.

### Certificate Access Fees

Not applicable.

### Revocation or Status Information Access Fees

Not applicable.

### Fees for Other Services

See [[Federation Name] Governance].

### Refund Policy

See [[Federation Name] Governance].

## Financial Responsibility

See [[Federation Name] Governance].

### Insurance Coverage

See [[Federation Name] Governance].

### Other Assets

Not applicable.

### Insurance or Warranty Coverage for End-Entities

Not applicable.

## Confidentiality of Business Information

Not applicable.

### Scope of Confidential Information

Not applicable.

### Information Not Within the Scope of Confidential Information

Not applicable.

### Responsibility to Protect Confidential Information

Not applicable.

## Privacy of Personal Information

See [[Federation Name] Governance] and [[Federation Name] MA] for more information.

### Privacy Plan

See [[Federation Name] Governance] and [[Federation Name] MA] for more information.

### Information Treated As Private

See [[Federation Name] Governance] and [[Federation Name] MA] for more information.

### Information Not Deemed Private

See [[Federation Name] Governance] and [[Federation Name] MA] for more information.

### Responsibility to Protect Private Information

See [[Federation Name] Governance] and [[Federation Name] MA] for more information.

### Notice and Consent to Use Private Information

See [[Federation Name] Governance] and [[Federation Name] MA] for more information.

### Disclosure Pursuant to Judicial or Administrative Process

See [[Federation Name] Governance] and [[Federation Name] MA] for more information.

### Other Information Disclosure Circumstances

See [[Federation Name] Governance] and [[Federation Name] MA] for more information.

## Intellectual Property Rights

See [[Federation Name] Governance] for more information.

## Representations and Warranties

See [[Federation Name] Governance] for more information.

### CA Representations and Warranties

See [[Federation Name] Governance] for more information.

### RA Representations and Warranties

Not applicable, as there are no registration authorities (RAs) in the [Federation Name] security model.

### Subscriber Representations and Warranties

See [[Federation Name] Governance] for more information.

### Relying Party Representations and Warranties

See [[Federation Name] Governance] for more information.

### Representations and Warranties of Other Participants

See [[Federation Name] Governance] for more information.

## Disclaimers of Warranties

See [[Federation Name] Governance] for more information.

## Limitations of Liability

See [[Federation Name] Governance] for more information.

## Indemnities

See [[Federation Name] Governance] for more information.

## Term and Termination

Not applicable.

### Term

Not applicable.

### Termination

Not applicable.

### Effect of Termination and Survival

Not applicable.

## Individual Notices and Communications with Participants

Not applicable.

## Amendments

Amendments to this CP are covered under Section 6 of [[Federation Name] OPP], “Change Management for Normative Standards”.

### Procedure for Amendment

Amendments to this CP are covered under Section 6 of [[Federation Name] OPP], “Change Management for Normative Standards”. In addition, amendments to this CP require approval by [FMO Name] and [Federation EC Name].

### Notification Mechanism and Period

See Section 6 of [[Federation Name] OPP], “Change Management for Normative Standards”.

### Circumstances under Which OID Must Be Changed

Not applicable.

## Dispute Resolution Provisions

All disputes shall be resolved as per the rules stipulated in [[Federation Name] Governance] and [[Federation Name] OPP].

## Governing Law

See [[Federation Name] MA].

## Compliance with Applicable Law

See [[Federation Name] Governance] and [[Federation Name] MA].

## Miscellaneous Provisions

Not applicable.

### Entire Agreement

See [[Federation Name] MA].

### Assignment

See [[Federation Name] MA].

### Severability

See [[Federation Name] MA].

### Enforcement (Attorneys' Fees and Waiver of Rights)

Not applicable.

### Force Majeure

Not applicable.

## Other Provisions

Not applicable.

1. See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>. [↑](#footnote-ref-1)
2. *NIST Special Publication 800-63: Electronic Authentication Guideline* defines four levels of assurance for electronic authentication. Level 1 is the lowest, and provides little or no assurance. Level 4 is the highest, and provides very high assurance; however, Level 4 is currently not possible in federated environments such as [Federation Name]. Levels 2 and 3 are therefore the only levels that are practical and provide value in a federated environment. See <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf> for more information. [↑](#footnote-ref-2)
3. The trust model used by [Federation Name] does not rely on the secrecy of the Trust Fabric document. [↑](#footnote-ref-3)
4. In a traditional PKI model, subscriber certificates are typically published in a directory, e.g. X.500 or LDAP. The Trust Fabric model used by [Federation Name] does not require separate publication of certificates in any location other than the [Federation Name] Cryptographic Trust Fabric. [↑](#footnote-ref-4)
5. At this point, the subscriber will have already submitted an application form containing one or more POCs as part of the application process. See [[Federation Name] OPP] for more information about the [Federation Name] application process. [↑](#footnote-ref-5)
6. Acceptance of a change to the [Federation Name] Cryptographic Trust Fabric is NOT required for revocation (removal from the Trust Fabric). [↑](#footnote-ref-6)
7. For more information about how to generate a public/private key pair using the RSA algorithm, please see [http://en.wikibooks.org/wiki/Transwiki:Generate\_a\_keypair\_using\_OpenSSL](http://en.wikibooks.org/wiki/Transwiki%3AGenerate_a_keypair_using_OpenSSL). For more information about the mathematics of the RSA algorithm, please see <http://en.wikipedia.org/wiki/RSA>. [↑](#footnote-ref-7)
8. FIPS PUB 140-2 states that: “Security Level 1 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system.” Note that security levels defined in [FIPS 140-2] are unrelated to levels of assurance for electronic identities as defined in NIST PUB 800-63. [↑](#footnote-ref-8)
9. See the NIST Authenticated NTP Service: <http://www.nist.gov/pml/div688/grp40/auth-ntp.cfm>. [↑](#footnote-ref-9)