Exostar FIS Certificate Policy

Version 1.9.5 FINAL

February 2024

Signature Page

5/24/2024

X Ming Chan

Ming Chan
Exostar PMA Chair
Signed by: Ming Chan_8332(Signature)

TABLE OF CONTENTS

1 Introduction

This Certificate Policy (CP) defines certificate policies to facilitate interoperability between the Exostar Federated Identity Service (FIS) Public Key Infrastructures (PKI) and industry and government PKI domains. The policies represent the Basic, Medium Software, and Medium Hardware assurance levels for public key certificates. The word “assurance” used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system which was used to produce the certificate and (if appropriate) deliver the private key to the Subscriber performs its task.

Interoperability will be achieved through the use of policy mapping between PKI Certification Authority (“CA”) systems and through the use of CA cross-certificates.

This policy covers the Exostar PKI, which includes the FIS Root CA (FISRCA), the Exostar FIS Signing Cas that operates under the governance of the Exostar Policy Management Authority (Exostar PMA).

As further described below, the Exostar PKI may cross-certify as a relying party and/or issuing organization to third party PKIs. For purposes of this CP, a cross-certified Certification Authority (“Entity” or “Entity CA”) may be a PKI bridge or enterprise PKI. However, the Exostar PKI does not operate as a PKI bridge, and no transitive trust path is intended to be expressed between or among such Entities using the Exostar PKI as an intermediary.

Any use of or reference to this CP outside the purview of the Exostar FIS completely at the using party’s risk. A cross-certified Certification Authority (“Entity”) shall not assert the certificate policy OIDs listed in Section 1.2 of this CP in any certificates the CA issues, except in the *policyMappings* extension of certificates issued by the CA to the FISRCA for the establishment of equivalency between an Exostar certificate policy OID and a policy OID the CA operates under.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework.

1.1 Overview

1.1.1 Certificate Policy (CP)

Certificates contain one or more registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The party that registers the OIDs (in this case, Exostar) also publishes the CP, for examination by Relying Parties. Cross certificates issued by the FISRCA shall, in the *policyMappings* extension and in whatever other fashion is determined by the Exostar Policy Management Authority (described in Section 1.3.1.1) to be necessary for interoperability, reflect what mappings exist between this CP and the cross-certified PKI CP.

1.1.2 Relationship between this CP & the FISRCA CPS and FIS CPS

This CP states what assurance can be placed in a certificate issued under this policy. The FISRCA Certification Practice Statement (Root CPS) and FIS CPS state how the respective certification authorities establish that assurance; Intermediate CAs are not used within the Exostar PKI.

1.1.3 Relationship between this CP and Entity CPs

With specific exceptions, levels of assurance of the certificates issued under this CP will be mapped by the Exostar Policy Management Authority (Exostar PMA) to the respective levels of assurance of the certificates issued by cross-certified PKIs.

The policy mapping information is placed into the certificates issued by the FISRCA, or otherwise published or used by the Exostar Operational Authority (described in Section 1.3.1.2) so as to facilitate interoperability.

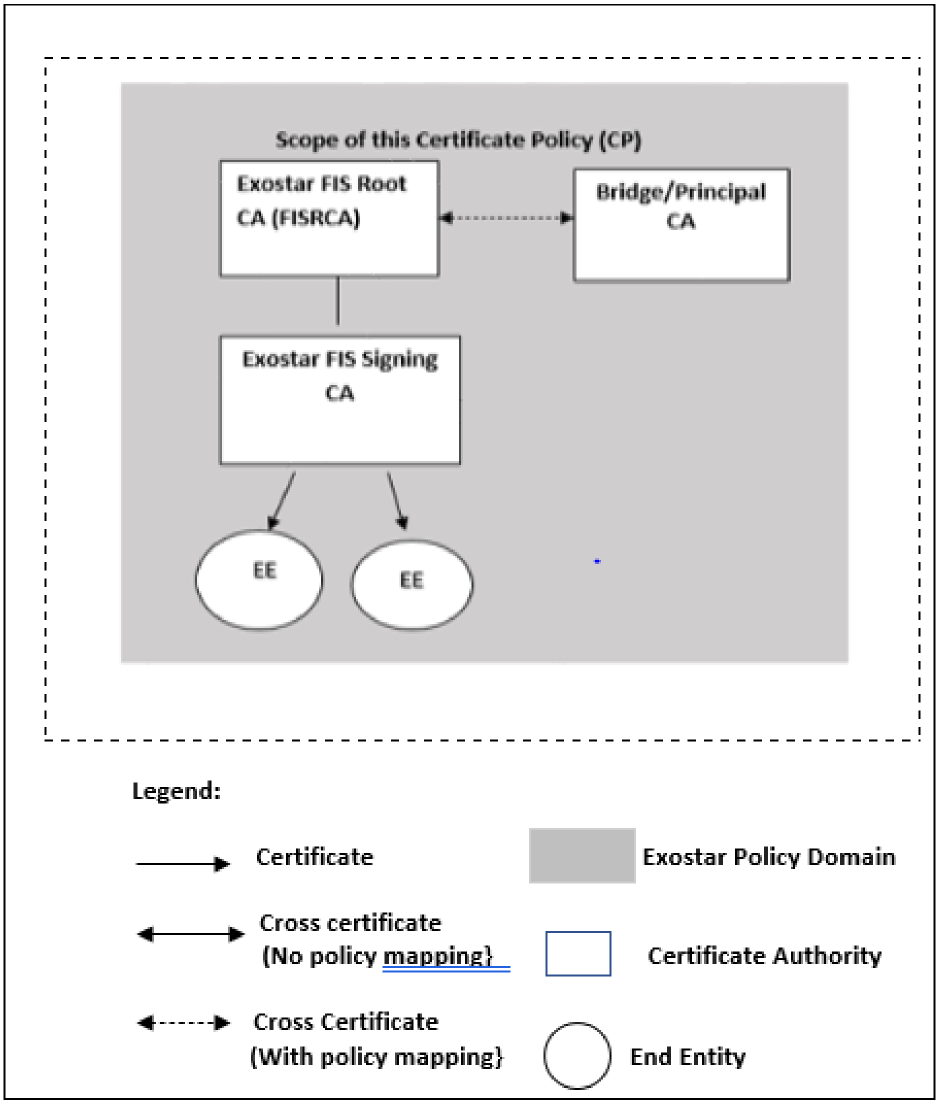
Scope of this Certificate Policy (CP)
Exostar FIS Root CA (FISRCA)
Bridge/Principal CA
Exostar FIS Signing CA
EE
EE
Legend:
Certificate
Exostar Policy Domain
Cross certificate (No policy mapping}
Certificate Authority
Cross Certificate (With policy mapping}
End Entity

Figure 1 - Scope and Domain of this CP

1.1.4 Scope

Figure 1 illustrates the scope of this CP.

This CP imposes requirements on all Exostar CAs.

Note: This CP does not govern Exostar's prior Signing CA infrastructure which is subordinate to the CertiPath Root CA, although that infrastructure is similarly governed by the Exostar PMA and is operated by the Exostar OA.

The FISRCA shall issue CA certificates only to the following:

- FIS Signing CAs;

- Cross-certified CAs;

A CA may also issue certificates to individuals who operate that CA.

Within this document, the term CA, when used without qualifier, shall refer to any certification authority subject to the requirements of this certificate policy, including the FISRCA, and FIS Signing CAs in cross-certified PKIs. The term Exostar PKI shall be used for requirements that pertain to the FISRCA, FIS Signing CA. Requirements that apply to a specific CA type will be denoted by specifying the CA type.

The scope of this CP in terms of subscriber (i.e., end entity) certificate types is limited to those listed in Section 10 and repeated here: identity, signature, encryption, web server, and code signing.

1.2 Document Identification

There are different levels of assurance in this Certificate Policy, which are defined in subsequent sections. Each level of assurance has an OID, to be asserted in certificates issued by the FISRCA, which comply with the policy stipulations herein. The OIDs are registered under the Exostar arc as follows:

id-Exostar	::= {1.3.6.1.4.1.13948}
[redacted]	[redacted]
id-security	::= { id-Exostar 1}
id-pki	::= { id-security 1}
exostar-certificate-policies	::= { id-pki 1}
id-mediumSoftware	::= {Exostar-certificate-policies 1}
id-mediumHardware	::= {Exostar-certificate-policies 2}
id-mediumSoftware-sha2	::= {Exostar-certificate-policies 5}
id-mediumHardware-sha2	::= {Exostar-certificate-policies 6}
id-basic	::= {Exostar-certificate-policies 7}
id-basic-sha2	::= {Exostar-certificate-policies 8}

id-exostarGeneralUse	::= {Exostar-certificate-policies 20}
id-mediumSoftware-device-sha2	::= {Exostar-certificate-policies 25}
id-mediumHardware-device-sha2	::= {Exostar-certificate-policies 26}
■	■
id-operations	::= { id-Exostar 2}
id-pkiOperations	::= { id-operations 2}
id-exostar-certificate-policies-pkiOperations	::= { id-pkiOperations 2}
id-exostarGeneralUseOperations	::= { id-exostar-certificate-policies-pkiOperations 1}
id-infrastructureDevices	::= { id-exostarGeneralUseOperations 20}

The Exostar OID arc is maintained by the Exostar PMA.

Medium Assurance End-Entity certificates issued to devices shall assert policies mapped to Exostar Software and Hardware certificate policies 25 and 26. All other policies defined in this document should be reserved for human subscribers when used in End-Entity certificates.

The relationship between a certificate’s LOA and the Policy OIDs it will exhibit are depicted in the table below:

Type of certificate issued **(issuing CA)**	**id-basic**	**id-mediumSoftware**	**id-mediumHardware**
Basic (FIS)	✓	■	■
Medium Software (FIS)	✓	✓	■
Medium Hardware (FIS)	✓	✓	✓

As of December 2010, Exostar’s existing “id-basic”, “id-mediumSoftware” and “id-mediumHardware” policy OID names have been aligned with industry standards to extend policy use of the SHA-1 algorithm.

Secure Hash Algorithm indicator in OID name

Unless otherwise stated, a requirement stated in this CP applies to all assurance levels. The requirements and certificate profiles for policy OIDs for SHA-256 OIDs at the same level of assurance, indicated by the absence or presence of “-sha2” at the end of the OID name (e.g. id-mediumHardware and id-mediumHardware-sha2), are identical except for the version of the Secure Hash Algorithm that is utilized.

Level of Assurance and OID names

When the level of assurance term “Basic” is used, it shall apply to id-basic and id-basic-sha2.

When the level of assurance term “Medium Software” is used, it shall apply to id-mediumSoftware and id-mediumSoftware-sha2.

When the level of assurance term “Medium Hardware” is used, it shall apply to id-mediumHardware and id-mediumHardware-sha2,.

Together, the policies designated as “id-medium” constitute the Exostar “Medium Assurance” family of certificate policies.

1.3 PKI Participants

This section contains a description of the roles relevant to the administration and operation of the Exostar PKI, the Exostar FISRCA and its Signing CAs.

1.3.1 PKI Authorities

1.3.1.1 Exostar PMA

The PMA is responsible for:

- Governance and oversight of the Exostar PKI,
- Drafting and approval of the Exostar CP,
- Drafting, compliance analysis, and approval of the FISRCA CPS and the FIS CPS,

A complete description of Exostar PMA roles and responsibilities is provided in the Exostar PMA Charter [CHARTER].

Exostar will enter into a Memorandum of Agreement (MOA) with an Entity setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in this CP and those in the Entity CP. Exostar will consult the Exostar PMA Chair prior to entering into a MOA. Thus, the term

“MOA” as used in this CP shall always refer to the Memorandum of Agreement cited in this paragraph.

1.3.1.2 Exostar Operational Authority (OA)

The Exostar Operational Authority is the organization that operates the Exostar PKI, the FISRCA, Exostar’s FIS Signing CAs, including issuing certificates when directed by the Exostar PMA Chair, posting those certificates and Certificate Revocation Lists (CRLs) into the Exostar PKI Repository, and ensuring the continued availability of the PKI Repository to all users.

1.3.1.3 Exostar Operational Authority Administrator (OAA)

The Administrator is the individual within the Exostar Operational Authority who has principal responsibility for overseeing the proper operation of the Exostar CAs including the Exostar PKI Repository. The Administrator is selected by and reports to the PMA.

1.3.1.4 Exostar Operational Authority Officers

These officers are the individuals within the Exostar Operational Authority who operate the Exostar CAs and the Exostar PKI Repository including executing the Exostar PMA direction to issue certificates to CAs or taking other action to effect interoperability between the FISRCA and Principal CAs. The roles include CA Officer, CA Administrator, and CA Operator, all described in Section 5.2.1 of this CP.

1.3.1.5 Entity Principal Certification Authority (PCA)

The Principal CA is a CA within a PKI that has been designated to interoperate directly with the FISRCA (e.g., through the exchange of cross-certificates). It should be noted that an Entity may request that the FISRCA interoperate with more than one CA within the Entity; that is, an Entity may have more than one Principal CA. A PCA may or may not be a Root CA (trust anchor) or a Bridge CA.

Exostar shall ensure that no CA within its PKI shall have more than one trust path to the US Federal Brdige CA (FBCA), regardless of path validation results.

1.3.1.6 Root CA

A Root CA is a trust anchor for subscribers of a PKI domain when the subscribers act as relying party. Normally, the PCA is also the Root CA. But, in some situations a Root CA may not be a PCA.

1.3.1.7 Intermediate CA

An Intermediate CA is a CA that is not a Root CA and whose primary function is to issue certificates to other CAs. Intermediate CAs are not utilized within the Exostar PKI.

1.3.1.8 Signing CA

A Signing CA is a CA whose primary function is to issue certificates to the end entities. A Signing CA does not issue certificates to other CAs.

1.3.1.9 Exostar Root Certification Authority (FISRCA)

The FISRCA is a Root CA operated by the Exostar Operational Authority. FISRCA issues and revokes certificates to Exostar Signing CAs upon authorization by the

Exostar PMA. As operated by the Exostar Operational Authority, the FISRCA is responsible for all aspects of the issuance and management of a certificate including:

- Control over the registration process,
- The identification and authentication process,
- The certificate manufacturing process,
- Publication of certificates,
- Revocation of certificates,
- Re-key of FISRCA signing material, and
- Ensuring that all aspects of the services, operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.10 Certificate Status Authority (CSA)

A CSA is an authority that provides status of certificates or certification paths. CSA can be operated in conjunction with the CAs or independent of the CAs. Examples of CSA are:

- Simple Certificate Validation Protocol (SCVP) Servers that validate certifications paths or provide revocation status checking services[1].

OCSP Responders that are keyless and simply repeat responses signed by other Responders and SCVP Servers that do not provide certificate validation services adhere to the same security requirements as repositories.

1.3.2 Registration Authority (RA)

An RA is the entity that collects and verifies each Subscriber’s identity and information that are to be entered into his or her public key certificate. An RA interacts with the CA to enter and approve the subscriber certificate request information. The Exostar Operational Authority acts as the RA for the FISRCA, and performs its function in accordance with the FISRCA CPS approved by the Exostar PMA. The RA functions for the FIS CA are documented in the FIS CA CPS.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate, and who does not itself issue certificates. FISRCA Subscribers include only Exostar Operational Authority personnel. FIS Signing CA Subscribers include any individuals who are issued certificates from the FIS Signing CA.

[1] There are three types of SCVP Servers: path development, path validation and revocation checking. The path development servers are not considered within the scope of this policy since the corruption of these servers does not adversely impact security and hence they need not be subject of a CP.

CAs are sometimes technically considered “subscribers” in a PKI. However, the term “Subscriber” as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.3.1 PKI Sponsor

A PKI sponsor (“PKI Sponsor”) fills the role of a Subscriber for non-human system components that are named as public key certificate subjects. The PKI Sponsor works with the RAs to register components (routers, firewalls, etc.) in accordance with Section 3.2.3.1, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

A PKI Sponsor need **not** be a Trusted Role, but should have been issued a credential that is equal to or higher assurance level than the credential that they are sponsoring

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.5 Other Participants

1.3.5.1 Related Authorities

The CAs operating under this CP require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The FISRCA CPS and the FIS CA CPS shall identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.3.5.2 Trusted Agent

A Trusted Agent is the entity that collects and verifies each Subscriber’s identity and information on behalf of an RA. A Trusted Agent does not have privilege on the CA to enter or approve subscriber information.

1.3.6 Applicability

The sensitivity of the information processed or protected using certificates issued by the Exostar PKI, the FISRCA, and the FIS CA will vary significantly. Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Entity for each application and is not controlled by this CP.

To provide sufficient granularity, this CP specifies security requirements at Basic, Medium Software, and Medium Hardware.

The certificate levels of assurance contained in this CP are set forth below, as well as a brief and non-binding description of the applicability for applications suited to each level.

Assurance Level	Applicability
Basic	This level is relevant to environments where risks and consequences of data compromise are low to moderate, and where PKI-based credentials are desired. Subscriber private keys are stored in software or hardware at this assurance level.
Medium Software	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber private keys are stored in software at this assurance level.
Medium Hardware	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber private keys are stored in hardware at this assurance level.

1.3.6.1 Factors in Determining Usage

The Relying Party must first determine the level of assurance required for an application, and then select the certificate appropriate for meeting the needs of that application. This will be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the Exostar PMA or the Exostar Operational Authority. Nonetheless, this CP contains some helpful guidance, set forth herein, which Relying Parties may consider in making their decisions.

1.3.6.2 Obtaining Certificates

This CP requires publication and access to CA certificates and CRL. This CP imposes no requirements in terms of publication and access to end entity (i.e., subscriber) certificates. The relying party applications must make their own agreement for obtaining the subscriber certificates. This could be trivially done for signature applications by including the signer certificate in the application protocol. For encryption applications, the relying party must develop a means to access subscriber certificates. Use of X.500 and LDAP Repositories is one way to achieve this, but no mechanism is mandated by this CP.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

No stipulation.

1.4.2 Prohibited Certificate Uses

No stipulation.

1.5 Policy Administration

1.5.1 Organization administering the document

The Exostar PMA is responsible for all aspects of this CP.

1.5.2 Contact Person

Questions regarding this CP shall be directed to the Chair of the Exostar PMA.

1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

No Stipulation.

1.5.4 CPS Approval Procedures

The term CPS is defined in the Internet RFC 3647, X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. It shall be more detailed than the corresponding certificate policy. CPS documentation for all CAs operating under the Exostar FIS PKI, including the FISRCA CPS and the FIS CA CPS, are contained in separate documents published and approved by the Exostar PMA, and specifies how this CP and any Memoranda of Agreements that the Exostar PMA has approved will be implemented to ensure compliance with their provisions.

1.5.5 Waivers

There shall be no waivers to this CP.

1.6 Affiliated Organizations

Subscriber certificates may be issued on behalf of an organization, other than Exostar; this is termed affiliation. The organizational affiliation will be indicated in the certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

2 PUBLICATION & PKI REPOSITORY RESPONSIBILITIES

2.1 PKI Repositories

Exostar is responsible for operation of repositories to support their PKI operations.

2.1.1 Repository Obligations

The Exostar Operational Authority may use a variety of mechanisms for posting information into their respective repositories as required by this CP. These mechanisms at a minimum shall include:

- Authority Information Access (AIA), Subject Information Access (SIA), or other Uniform Resource Identifiers (URI) accessible through the Hypertext Transfer Protocol (HTTP)
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP, and
- Access control mechanisms when needed to protect repository information as described in later sections.

Cross-certified PKIs shall use comparable mechanisms for the publication of their respective repositories.

2.2 Publication of Certificate Information

2.2.1 Publication of CA Information

The Exostar Operational Authority shall publish information concerning the Exostar CAs necessary to support its use and operation, including all CA certificates issued by or to the Exostar PKI and CRLs issued by the Exostar PKI.

The PKI Repositories containing certificates and certificate status information shall be deployed so as to provide 24 hour per day/365 day per year availability. Exostar shall implement features to provide high levels of PKI Repository reliability (99% availability or better).

CA and End Entity certificates shall only contain valid URIs that are accessible by relying parties.

All CAs, at a minimum, shall post CA certificates and CRLs.

Cross-certified PKIs shall use comparable mechanisms for the publication of their respective CA certificates and CRLs.

2.2.2 Interoperability

Exostar Repositories are available via HTTP.

2.3 Time or Frequency of Publication

This CP and any subsequent changes are made publicly available within thirty (30) days of approval.

Publication requirements for CRLs are provided in Sections 4.9.7.

2.4 Access Controls on PKI Repositories

Any PKI Repository information not intended for public dissemination or modification shall be protected. Public keys and certificate status information in the Exostar PKI Repository shall be publicly available through the Internet.

3 IDENTIFICATION & AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The CAs shall generate and sign certificates containing an X.500 Distinguished Name (DN) in the Issuer and in Subject fields; the X.500 DN may contain domain component elements. Subject Alternative Name may also be used, if marked non-critical.

3.1.1.1 Subject Names

Certificates issued to Subscribers must include distinguished names that are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs).

A Device Subscriber name must be a unique name for the device and must not take the form of a Human Subscriber name.

3.1.1.2 Subject Alternative Names

Subscriber certificates that contain id-kp-emailProtection in the EKU must include a subject alternative name extension that includes a rfc822Name.

For Device Subscriber certificates that assert serverAuth in the Extended Key Usage, wildcard domain names are permitted in the dNSName value only if all sub-domains covered by the wildcard fall within the same application, cloud service, or system boundary within the scope of the sponsoring organization.

3.1.2 Need for Names to be Meaningful

The certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

All DNs and associated directory information tree shall accurately reflect organizational structures. When User Principal Name (UPN) is used, it shall accurately reflect organizational structure.

When DNs are used, it is preferable that the common name represents the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

For certificates issued to human subscribers, the subject DN shall contain the affiliated organization name in an appropriate relative distinguished name attribute (e.g., organization (o), organizational unit (ou), or domain component (dc) attribute); certificates shall not be issued to “unaffiliated” subscribers.

End entity certificates issued under the Exostar PKI shall express namespaces that are authorized by the Exostar PMA.

3.1.3 Anonymity or Pseudonymity of Subscribers

CA certificates shall not contain anonymous or pseudonymous identities.

DNs in certificates issued to end entities may contain a pseudonym to meet local privacy regulations as long as name space uniqueness requirements are met and as long as such name is unique and traceable to the actual entity.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be contained in the applicable certificate profile.

3.1.5 Uniqueness of Names

Name uniqueness across the Exostar domains, including cross-certified domains shall be enforced. The CAs and RAs shall enforce name uniqueness within the X.500 name space, which they have been authorized.

The Exostar PMA shall be responsible for ensuring name uniqueness in certificates issued by the Exostar CAs.

Exostar will include the following information in its CPSs:

- What name forms shall be used, and
- How it will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if “Joe Smith” leaves a CA’s community of Subscribers, and a new, different “Joe Smith” enters the community of Subscribers, how will these two people be provided unique names?).

3.1.6 Recognition, Authentication & Role of Trademarks

No stipulation.

3.1.7 Name Claim Dispute Resolution Procedure

The Exostar PMA shall resolve any name collisions brought to its attention that may affect interoperability.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the issuing CA. The CA shall then validate the signature using the party’s public key. The Exostar PMA may allow other mechanisms that are at least as secure as those cited here.

3.2.2 Authentication of Organization Identity

Requests for certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. The RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

3.2.3 Authentication of Individual Identity

A CA shall ensure that the applicant's identity information is verified and checked in accordance with the CPS. The CA or an RA shall ensure that the applicant's identity information and public key are properly bound. Additionally, the CA or the RA shall record the process that was followed for issuance of each certificate. Process information shall depend upon the certificate level of assurance and shall be addressed in the applicable CPS.

For the Medium Software and Medium Hardware assurance levels, the process documentation and authentication requirements shall include the following:

- The identity of the person performing the identity verification;

- A signed declaration by that person that he or she verified the identity of the applicant as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy;

- The applicant shall present one valid national government-issued photo identification document (ID), or two valid non-national government IDs, one of which shall be a recent photo ID (e.g., drivers license), which are issued by governments or international jurisdictions recognized by the US Federal Government.

- Unique identifying numbers from the identifier (ID) of the verifier and from an ID of the applicant;

- The date and time of the verification; and

- A declaration of identity signed by the applicant using a handwritten signature or equivalent and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

  Practice Note: Examples of signatures equivalent to handwritten signature are a good fingerprint or other adequate biometric that can be linked to the individual identity. Another example of a signature equivalent to handwritten signature is digital signature that can be verified using a certificate provided to the same identity. However, that certificate must not be the same certificate for whose issuance the identity proofing is being performed.

For the Medium Software and Medium Hardware assurance levels, identity shall be established by in-person proofing before the RA, Trusted Agent, or an entity certified by a state, federal, or national government as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. Requirements for authentication of individual identity using an in-person antecedent are listed in Section 3.2.3.3.

For the Basic assurance level, applicant identity shall be established using the applicant's registered email address or email account. In-person proofing need not be conducted, and additional process documentation shall not be required.

3.2.3.1 Authentication of Component Identities

Some computing and communications components (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the component shall have a human sponsor. The PKI sponsor shall be responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name)
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required
- The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:
    - Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance than that being requested).
    - In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.

These certificates shall be issued only to devices under the PKI Sponsor's control (i.e., require registration and validation that meets all issuer requirements, as well as requiring re-validation prior to being re-issued). In the case a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

In the event an applicant is denied a credential based on the results of the identity proofing process, Exostar's General Terms and Conditions shall govern the mechanism for appeal or redress of the decision.

3.2.3.2 Human Subscriber Re-Authentication

If a human subscriber's credentials containing the private keys associated with the public key certificates are lost, damaged, or stolen, the subscriber may be issued new certificates using the process described in this section. However, the validity period of the certificates issued using this process shall not exceed the identity-reproofing requirements in Section 3.3.1. Alternatively, the subscriber can undergo an initial identity proofing process described in Section 3.2.3.

The CA or an RA shall ensure that the subscriber's identity information and public key are properly bound. Additionally, the CA or the RA shall record the process that was followed for issuance of each certificate. Process information shall depend upon the certificate level of assurance and shall be addressed in the applicable CPS.

For the basic assurance level, applicant identity shall be re-established using the applicant's registered email address or email account.

In addition, if the credentials are lost, stolen or otherwise unaccounted for, all certificates associated with the private keys on the credentials shall be revoked for the reason of key compromise. This CP also requires that when a certificate is revoked for the reason of key compromise, the derivative certificates (i.e., certificates issued on the basis of the compromised certificate) be also revoked.

3.2.3.3 Human Subscriber Initial Identity Proofing Via Antecedent Relationship

The following requirements shall apply when a human subscriber identity is verified using an antecedent relationship with a Trusted Role holder or organizational sponsor (Certificate Sponsor or PKI Sponsor):

1. The applicant (Certificate Applicant) shall personally appear before an RA or a Trusted Agent (Identity Verifier);

2. The Certificate Applicant and the Identity Verifier shall have an established working[2] relationship with the Certificate Sponsor. The relationship shall be sufficient to enable the Identity Verifier to verify with a high degree of certainty that the Certificate Applicant is the same person that was identity proofed. An example to meet this requirement is when the Certificate Applicant, RA, and Trusted Agents are employed by the same company and the company badge forms the basis for the Certificate Applicant authentication;

3. The Certificate Applicant shall present a valid Certificate Sponsor-issued photo ID. This photo ID shall have been issued on the basis of in-person identity proofing using one valid national government-issued picture ID, or two valid non-national government IDs, one of which shall be a photo ID (e.g., drivers license), which are issued by governments or international jurisdictions recognized by the US Federal Government;

4. The Identity Verifier shall record the following:

[2] An example of "established working relationship" is the person is employed by the Certificate Sponsor. Another example of "established working relationship" is the person is consultant to the Certificate Sponsor or is employed by a contractor of the Certificate Sponsor.

a) His/her own identity;
b) Unique identifying number from the identifier (ID) of the Identity Verifier;
c) Unique identifying number from the Certificate Sponsor-issued photo ID to the Certificate Applicant;
d) Date and time of the identity verification; and
e) Date and time of Sponsor-issued photo ID, if applicable.

5. The Identity Verifier shall sign a declaration that he or she verified the identity of the Certificate Applicant as required by the applicable certificate policy which may be met by establishing how the Certificate Applicant is known to the Identity Verifier as required by this certificate policy; and

6. The Certificate Applicant shall sign a declaration of identity using a handwritten signature or equivalent using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law. This declaration shall be signed in the presence of the Identity Verifier.

3.2.3.4 Authentication of Human Subscriber for Role Certificates

Subscribers may be issued role certificates. A role certificate shall identify a specific role title on behalf of which the subscriber is authorized to act rather than the subscriber's name. A role certificate can be used in situations where non-repudiation is desired. A role certificate shall not be a substitute for an individual subscriber certificate. Multiple subscribers can be assigned to a role at the same time, however, the signature key pair shall be unique to each role certificate issued to each individual; the encryption key pair and encryption certificate may be shared by the individuals assigned the role.

Subscribers issued role certificates shall protect the corresponding role credentials in the same manner as individual credentials.

The procedures for issuing role certificates shall comply with all other stipulations of this CP (e.g., subscriber identity proofing, validation of organization affiliation, key generation, private key protection, and Subscriber obligations). For the role signature certificate, the individual assigned the role or the role sponsor may act on behalf of the certificate subject for certificate management activities such as renewal, re-key and revocation. Issuance and modification of role signature certificate shall require the approval of the role sponsor. Rekey and renewal of role signature certificate shall require the approval of the role sponsor if the validity period is extended beyond that already approved by the role sponsor. For the role encryption certificate, only the role sponsor may act on behalf of the certificate subject for certificate management activities such as issuance, renewal, re-key, modification, and revocation.

The CA or the RA shall record the information identified in Section 3.2.3 for a sponsor associated with the role before issuing a role certificate. The sponsor shall hold an individual certificate in his/her own name issued by the same CA at the same or higher assurance level as the role certificate. The CA or the RA shall validate from the role sponsor that the individual subscriber has been approved for the role certificate.

The role sponsor (which is not a trusted role) shall be responsible for:

1. Authorizing individuals for a role certificate;
2. Recovery of the private decryption key
3. Revocation of individual role certificate;

4. Always maintaining a current up-to-date list of individuals who are assigned the role; and
5. Always maintaining a current up-to-date list of individuals who have been provided the decryption private key for the role.

Practice Note: When determining whether a role certificate is warranted, consider whether the role carries inherent authority beyond the job title. Role certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: “Chair PKI Process Action Team”.

3.2.3.5 Authentication of Devices

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. These certificates are issued for internal partner integration and are managed by Exostar. In such cases, the device must have a human sponsor. The sponsor is responsible for the security of the private key and for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys
- Equipment or software application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required

3.2.4 Non-verified Subscriber Information

Information that is not verified shall not be included in Certificates.

3.2.5 Validation of Authority

The issuer CA shall validate the subject CA certificate requestor's authorization to act in the name of the subject CA. All Exostar CAs operating under this CP shall obtain Exostar PMA approval prior to issuing CA certificates. Issuance of a cross-certificate by an Exostar CA shall be based on successful mapping of the subject CA CP with this CP. Creation of a FISRCA shall be based on successful CPS compliance analysis and Exostar PMA approval.

Certificates that contain explicit or implicit organizational affiliation shall be issued only after ascertaining the applicant has the authorization to act on behalf of the organization in the asserted capacity.

For issuance of a code-signing certificate, the requester shall hold an individual certificate in his/her own name issued by the same CA at the same or higher assurance level, and the issuer shall verify the certificate requestor’s authorization to request a code-signing certificate in the name of the subject organization.

3.2.6 Criteria for Interoperation

A cross-certified PKI shall adhere to the following requirements:

- Have a CP mapped to, and determined by the Exostar PMA to be in conformance with this CP;
- Operate a PKI that has undergone a successful compliance audit pursuant to Section 8 of this CP and as set forth in the applicable CP;
- Issue certificates compatible with the profiles described in this CP, and make certificate status information available in compliance with this CP; and
- Provide CA certificate and certificate status information to the relying parties.

Note: Multiple trust paths created as a result of certificate renewal or CA rekey do not violate the single trust path requirement above.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

Subscribers shall identify themselves through use of their current Signing Key or by using the initial identity-proofing process as described above. For end entities with Medium Software and Medium Hardware assurance certificates, initial identity-proofing process needs to be carried out once every nine years only; however, when the current Signing Key is used for identification and authentication purposes, the RA shall ensure that certificates issued would not expire more than nine years beyond the date of original identity proofing.

For Basic assurance, initial identity-proofing process is always used for re-key, which is more of an automated process and easily performed.

All mediumDevice and mediumDeviceHardware re-key requests are authenticated using the initial issuance process.

The assurance level of the new certificate shall not exceed the assurance level of the certificate being used for identification and authentication purposes.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked other than during a renewal or update action, the subject (i.e., a CA or an end entity) is required to go through the initial registration process described in Section 3.2 to obtain a new certificate.

3.4 Identification and Authentication for Revocation Request

Revocation requests shall be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated public key, regardless of whether or not the private key has been compromised.

3.5 Identification and Authentication for Key Recovery Requests

Exostar supports self-recovery for a subscriber’s private keys only.

The Subscriber identity must be established as previously specified. Alternatively, if the authentication cannot be verified using the public key certificates issued by the associated PKI and for at least the given certificate policy assurance level, then the identity validation can use the steps outlined in Section 3.2.3

For automated self-recovery, the Subscriber must be authenticated to the KED using a valid public key certificate. The assurance level of the Subscriber certificate must be equal to or greater than that of the certificate whose corresponding private key is being recovered.

3.5.1 Subscriber Authentication

The subscriber must authenticate using a public key certificate issued by the associated PKI. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered and must meet the requirements of an RA credential.

The Subscriber identity must be established as specified in Section 3.3.1 above. Alternatively, if the authentication cannot be verified using the public key certificates issued by the associated PKI and for at least the given certificate policy assurance level, then the identity validation can use the steps outlined in Section 3.2.3.1.

For automated self-recovery, the Subscriber must be authenticated to the KED using a valid public key certificate. The assurance level of the Subscriber certificate must be equal to or greater than that of the certificate whose corresponding private key is being recovered.

3.5.2 Third-Party Requestor Authentication

Third-Party requests for key recovery must be reviewed through the organization's legal department before further action is taken.

Third-Party Requestor identity authentication must be commensurate with the assurance level of the certificate associated with the key being recovered. Identity must be established using one of the following methods:

- Procedures specified in Section 3.2.3 for authentication of an individual identity during initial registration for the specified certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).
- Certificate-based authentication (e.g., digitally signed e-mail or client-authenticated TLS) that can be verified using current, valid (i.e., un-revoked) public key certificates at the requested certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Communication among the CA, RA, Trusted Agent, other parties confirming identities, and subscriber shall have requisite security services (i.e., source authentication, integrity, non-repudiation, or confidentiality) applied to them commensurate with the assurance level of the certificate being managed. For example, packages secured and transported in a tamper-evident manner by a certified mail carrier meet the integrity and confidentiality requirements for Medium assurance level. When cryptography is used, the mechanism shall be at least as strong as the certificates being managed. For example, web site secured using SSL certificate issued under Medium Software policy and set up with appropriate algorithms and key sizes satisfies integrity and confidentiality requirements for Medium Software certificate management.

The content of communication shall dictate if some, all, or none of the security services are required.

4.1 Certificate Application

The FISRCA may issue end-entity certificates to trusted personnel where necessary for the internal operations of the FISRCA. The FISRCA shall not issue end-entity certificates for any other reasons.

The Exostar PMA shall establish internal procedures for the approval and issuance of Signing CA certificates that are subordinate to the FISRCA. Exostar Signing CAs shall be operated according to a Certification Practices Statement which is approved by the Exostar PMA .

The Exostar PMA shall establish procedures for entities to use in applying for cross-certification with the Exostar FISRCA. Cross-certification requests shall be accompanied by a CP written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC3647]. Additionally, requests shall propose a mapping between the levels of assurance expressed in the Entity’s CP, and those in this CP.

The Exostar PMA shall make a determination regarding whether or not to issue the requested certificate(s), and what policy mappings to express in the certificate(s), if applicable. Exostar shall then enter into a MOA setting forth their respective responsibilities; the Exostar PMA will direct the Exostar Operational Authority to issue the certificate(s).

Upon issuance, each certificate issued by the FISRCA shall be manually checked to ensure each field and extension is properly populated with the correct information, before the certificate is delivered to the subject CA.

4.1.1 Submission of Certificate Application

For End Entity certificate applications, the Subscriber shall submit the certificate application to the Exostar RA.

For Signing CA certificate applications, the Exostar OA Administrator shall submit the application to the Exostar PMA.

For cross-certificate applications to the FISRCA, an authorized representative of the Subject CA shall submit the application to the Exostar PMA.

4.1.2 Enrollment Process and Responsibilities

Applicants for public key certificates shall be responsible for providing accurate information in their applications for certification.

For Exostar Signing CAs, the CPS shall describe the enrollment process for its Subject CAs and Subscribers.

4.2 Certificate Application Processing

It is the responsibility of the CA and RA to verify that the information in certificate applications is accurate. The applicable CPS shall specify procedures to verify information in certificate applications.

4.2.1 Performing Identification and Authentication Functions

For the CA certificates issued by the FISRCA, the Exostar Operational Authority shall perform the identity-proofing of cross-certification applicant CAs, the Exostar Signing CAs, and FISRCA trusted role Subscribers.

Prior to certificate issuance, a Subscriber shall be required to sign a document containing the requirements the Subscriber shall protect the private key and use the certificate and private key for authorized purposes only.

4.2.2 Approval or Rejection of Certificate Applications

For Exostar CAs, the Exostar PMA may approve or reject a certificate application.

4.2.3 Time to Process Certificate Applications

The certificate application processing from the time the request/application is posted on the CA or RA system to certificate issuance shall take no more than 30 days.

4.3 Certificate Issuance

Upon receiving a request for a certificate, the CA or RA shall respond in accordance with the requirements set forth in the CPS.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until the process set forth in the CP and CPS has been met.

It is the responsibility of the CA and the RA to verify that the information is correct and accurate.

4.3.1 CA Actions during Certificate Issuance

A CA verifies the source of a certificate request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance, a CA shall post the certificate.

4.3.2 Notification to Subscriber of Certificate Issuance

A CA shall notify a subject (CA or End Entity Subscriber) of certificate issuance.

4.4 Certificate Acceptance

The MOA shall set forth responsibilities of all parties before the Exostar PMA authorizes issuance of a CA certificate by an Exostar CA. Once a CA certificate has been issued, its acceptance by the Entity shall commence interoperability with the Exostar PKI and thus triggers the Subject CA's obligations under the MOA and hence this CP.

4.4.1 Conduct Constituting Certificate Acceptance

For certificates issued by an Exostar CA, certificate acceptance shall be governed by the MOA, Exostar's General Terms and Conditions, and/or applicable Service Agreement.

4.4.2 Publication of the Certificate by the CA

All CA certificates shall be published in a PKI Repository accessible to the Internet. There is no stipulation regarding publication of Subscriber certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Exostar OA shall inform the Exostar PMA of any certificate issuance to a CA by an Exostar CA.

Notification of intended certificate issuance by the FISRCA shall be provided to all cross-certified entities at least two weeks prior to issuance. The notification shall assert that a new CA cross-certification does not introduce multiple paths to a CA already participating in the FPKI. Following issuance, all new artifacts (CA certificates, CDP, AIA and Certificate Usage/or SIA URLs, etc.) produced as a result of the issuance shall be provided to all cross-certified entities within 24 hours following issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers shall protect their private keys from access by any other party.

Subscribers shall use their private keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates issued to them.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall use public key certificates and associated public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates.

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed in order to reduce the size of CRLs. A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged.

After certificate renewal, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been revoked or compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must not exceed the remaining lifetime of the private key, as specified in Section 5.6. The identity proofing requirement listed in Section 3.3.1 shall also be met.

4.6.2 Who may Request Renewal

A Subject may request the renewal of its certificate.

A PKI Sponsor may request renewal of a sponsored component certificate.

A CA may request renewal of its subscriber certificates, e.g., when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

A certificate renewal shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3, except the old key can also be used as the new key.

For CA certificates issued by an Exostar CA, certificate renewal also requires that a valid MOA exists between the Exostar PMA and the Subject CA, and the term of the MOA is beyond the expiry period for the new certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.7 Certificate Re-Key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and reestablishes its identity. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.
After certificate rekey, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-key

A CA may issue a new certificate to the Subject when the Subject has generated a new key pair and is entitled to a certificate.

4.7.2 Who may Request Certification of a New Public Key

A Subscriber may request the re-key of its certificate.

A PKI Sponsor may request may request re-key of a sponsored component certificate.

4.7.3 Processing Certificate Re-keying Requests

A certificate re-key shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3.

For CA certificates issued by an Exostar CA, certificate re-key also requires that a valid MOA exists between the Exostar PMA and the Subject CA, and the term of the MOA is beyond the expiry period for the new certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

Updating a certificate means creating a new certificate that has the same or a different key and a different serial number, and that it differs in one or more other fields, from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

Further, if an individual’s name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or the trusted agent in order for an updated certificate having the new name to be issued.

After certificate modification, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1 Circumstance for Certificate Modification

A CA may issue a new certificate to the Subject when some of the Subject information has changed, e.g., name change due to change in marital status, change in subject attributes, etc., and the Subject continues to be entitled to a certificate.

4.8.2 Who may Request Certificate Modification

A Subject may request modification of its certificate.

A PKI Sponsor may request may request modification of a sponsored component certificate.

4.8.3 Processing Certificate Modification Requests

A certificate modification shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3. In addition, the validation of the changed subject information shall be in accordance with the initial identity-proofing process as described in Section 3.2.

For CA certificates issued by an Exostar CA, certificate modification also requires that a valid MOA exists between the Exostar PMA and the Subject CA, and the term of the MOA is beyond the expiry period for the new certificate.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised**.**

For High, Medium Hardware, Medium, and Basic Assurance, all CAs shall publish CRLs.

For Entity CAs, the Exostar PMA shall be notified at least two weeks prior to the revocation of a CA certificate, whenever possible. For emergency revocation, CAs shall follow the notification procedures in Section 5.7.

4.9.1 Circumstance for Revocation of a Certificate

A certificate shall be revoked when the binding between the subject and the subject’s public key defined within a certificate is no longer considered valid. For certificates that express an organizational affiliation, organizations shall inform the CA of any changes in the subscriber affiliation. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate become invalid;
- Privilege attributes asserted in the Subject's certificate are reduced;
- The Subject can be shown to have violated the stipulations of its agreement;
- The private key is suspected of compromise; or
- The Subject or other authorized party (as defined in the applicable CPS) asks for his/her certificate to be revoked.

Where subscribers use hardware tokens, revocation is optional if all of the following conditions are met:

- the revocation request was not for key compromise;
- the hardware token does not permit the user to export the signature private key;
- the Subscriber surrendered the token to the PKI;
- the token was zeroized or destroyed promptly upon surrender;
- the token has been protected from malicious use between surrender and zeroization or destruction.

In all other cases, revocation of the certificates is mandatory.

Whenever a revocation occurs, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation of a Certificate

A certificate subject, human supervisor of a human subject, human resources (HR) person for a human subject, PKI Sponsor for a sponsored component, issuing CA, or RA may request revocation of a certificate.

In the case of certificates issued by an Exostar CA, the Exostar PMA may request revocation of a certificate.

For CA certificates, authorized individuals representing the CA operations may request revocation of certificates.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).
Any CA may unilaterally revoke another CA certificate it has issued. Generally, a CA certificate will be revoked based on a subject request, authorized representative of subject request, or Exostar PMA request.

Upon receipt of a revocation request, a CA shall authenticate the request and then revoke the certificate.

In the case of a CA certificate issued by an Exostar CA, the Operational Authority shall seek approval from the Exostar PMA before revocation of the certificate, and all cross-certified entities shall be notified at least two weeks prior whenever possible, except when the Exostar PMA is not available and there is an emergency situation such as:

- Request from the subject CA for reason of key compromise;
- Determination by the Operational Authority that a subject CA key is compromised; or
- Determination by the Operational Authority that a subject CA is in violation of the CP, CPS, or MOA to a degree that threatens the integrity of the Exostar FIS PKI.

If it is determined subsequent to issuance of new certificates that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, all certificates authorized by directly or indirectly chaining back to that compromised key shall be revoked.
At the Medium Hardware assurance levels, a Subscriber ceasing its relationship with an organization that sponsored the certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

If it is determined that a private key used to authorize the issuance of one or more certificates may have been compromised, all certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise shall be revoked or shall be verified as appropriately issued.

If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then all Subscriber certificates associated with the un-retrieved tokens shall be immediately revoked for the reason of key compromise.

4.9.4 Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

4.9.5 Time within which CA must Process the Revocation Request

Exostar CAs shall process all revocation requests within 18 hours of receipt of request.

Entity CAs will revoke subscriber certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests must be processed before the next CRL is published, excepting those requests validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance must be processed before the following CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party and the system accreditor. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. A CA shall ensure that superseded certificate status information is removed from the PKI Repository upon posting of the latest certificate status information.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation. PKI participants shall coordinate with the PKI Repositories to which they post certificate status information to reduce latency between creation and availability.

The following table provides CRL issuance frequency requirements.

	CRL Issuance Frequency
Routine	At least once every 31 days for Offline Roots; At Least Once every 24 hours for all others, including Signing CAs
Loss or Compromise of Private Key	Within 18 Hours of Notification
CA Compromise	Immediately, but no later than 18 hours after notification

The CAs that issue routine CRLs less frequently that the requirement for Emergency CRL issuance (i.e., CRL issuance for loss or compromise of key or for compromise of CA) shall meet the requirements specified above for issuing Emergency CRLs. Such CAs shall also be required to notify the Exostar Operational Authority upon Emergency CRL issuance. This requirement shall be included in the MOA between the Exostar and the Entity.

For off line Root and Bridge CAs that do not issue end-entity certificates except for internal operations, the *nextUpdate* shall be less than or equal to *thisUpdate* plus 32 days +/- 20 minutes.

For all other CAs, the *nextUpdate* shall be less than or equal to *thisUpdate* plus 24 hours +/- 20 minutes.

4.9.8 Maximum Latency for CRLs

CRLs shall be published within four hours of generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

The maximum delay between the time a Subscriber certificate revocation request is received by a CA and the time that this revocation information is available to Relying Parties shall be no greater than 24 hours.

4.9.9 Online Revocation Checking Availability

In addition to CRLs, CAs and Relying Party client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

If on-line revocation/status checking is supported by a CA, the latency of certificate status information distributed on-line by the CA or its delegated status responders shall meet or exceed the requirements for CRL issuance stated in 4.9.7.

4.9.10 Online Revocation Checking Requirements

OCSP support is optional. When implemented, the PKI shall implement Delegated Trust Model (DTM) OCSP Responders, and shall at least provide pre-signed responses..

4.9.11 Other Forms of Revocation Advertisements Available

Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and on-line revocation and status checking.

The alternative method must be described in the CA's approved CPS, and must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.

4.9.11.1 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.9.12 Special Requirements Related To Key Compromise

None beyond those stipulated in Section 4.9.7.

4.9.13 Circumstances for Suspension

Suspension shall be permitted for certificates issued under the Medium Hardware policy only, in the event that a user's token is temporarily unavailable to them.

4.9.14 Who can Request Suspension

A human subscriber, human supervisor of a human subscriber, HR person for the human subscriber, issuing CA, or RA may request suspension of a certificate.

4.9.15 Procedure for Suspension Request

A request to suspend a certificate shall identify the certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated (e.g., digitally or manually signed).

The reason code CRL entry extension shall be populated with “certificateHold”. The Hold Instruction Code CRL entry extension shall be either absent or contain the OID for id-holdinstruction-reject per RFC 5280.

4.9.16 Limits on Suspension Period

A certificate may only be suspended for up to 14 days. If the subscriber has not removed their certificate from hold (suspension) within that period, the certificate shall be revoked for reason of “Key Compromise”.

In order to mitigate the threat of unauthorized person removing the certificate from hold, the subscriber identity shall be authenticated in person using initial identity proofing process described in Section 3.2.3 or using Human Subscriber Re-Authentication process described in Section 3.2.3.2.

4.10 Certificate Status Services

The Exostar PKI and cross-certified PKIs are not required to support certificate status services such as SCVP.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

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

4.10.3 Optional Features

No stipulation.

4.11 End Of Subscription

Certificates that have expired prior to or upon end of subscription are not required to be revoked. Unexpired CA certificates shall always be revoked at the end of subscription.

4.12 Key Escrow and Recovery

If escrow is supported, subscriber private keys (i.e., decryption private keys) associated with a key management certificate must be securely escrowed.

Subscriber private keys must be protected during transit and storage using cryptography at least as strong as the key being escrowed.

Subscribers must be notified that the private keys associated with their encryption certificates will be escrowed.

Communications between the various key recovery components must be secured from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols must be equal to or greater than that of the keys they protect.

During delivery, escrowed keys must be protected against disclosure to any party except the Requestor.

Subscribers may use electronic or manual means to request their own escrowed keys. Subscriber must authenticate them selves and perform self recovery. If the request is made electronically, the subscriber must authenticate to a recovery service using an associated authentication or signature certificate with an assurance level equal to or greater than that of the escrowed key. Manual requests must be made in person, and include proper identity verification.

A current Subscriber's escrowed keys may be provided directly to the Subscriber without imposition of two-person control requirements. The KED must only provide escrowed keys to current Subscribers without two-person control upon:

- Verifying that the authenticated identity of the Requestor is the same as the Subscriber associated with the escrowed keys being requested;
- Sending notification to the Subscriber of all attempts (successful or unsuccessful) to recover the Subscriber's escrowed keys that are made by entities claiming to be the subscriber. If the KED does not have information (e.g., an e-mail address) necessary to send notification to the Subscriber of a key recovery request, then the KED must not provide the Subscriber with the requested key material using the automated recovery process

- Ensuring that the escrowed keys are being sent only to the authenticated Subscriber associated with the escrowed keys; and
- Ensuring that the escrowed keys are encrypted during transmission using cryptography of equal or greater strength than provided by the escrowed keys.
- Current Subscribers are authorized to recover their own escrowed key material.

4.12.1 Key Escrow and Recovery Policy and Practices

Under no circumstances shall a CA or an end entity signature key be escrowed.

The Exostar FIS PKI may escrow Subscriber encryption private keys.

Eoxstar only supports self-recovery.

Subscribers may request recovery of their own escrowed keys by authenticating as described in 3.5.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

This CP neither requires nor prohibits the Exostar to have the capability of recovering session keys.

5 Facility Management & Operational Controls

5.1 Physical Controls

5.1.1 Site Location & Construction

The location and construction of the facility housing CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

5.1.2.1 CA Physical Access

CA and CSA equipment shall always be protected from unauthorized access. The physical security requirements pertaining to CA and CSA equipment are:

- Ensure no unauthorized access to the hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers
- Be manually or electronically monitored for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Provide at least three layers of increasing security such as perimeter, building, and CA room
- Require two person physical access control to both the cryptographic module and computer system

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules shall be placed in secure containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the CA equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”);
- For off-line CAs, all equipment other than the PKI Repository is shut down;
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 RA Equipment Physical Access

RA equipment shall be protected from unauthorized access while the RA cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

5.1.3 Power and Air Conditioning

CAs shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power, to support continuity of operations.

5.1.4 Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

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

5.1.5 Fire Prevention & Protection

The CA must comply with local commercial building codes for fire prevention and protection.

5.1.6 Media Storage

CA media shall be stored so as to protect it from unauthorized physical access.

CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the CA location.

5.1.7 Waste Disposal

Sensitive waste material (including hard drives, removable storage, tape media, and paper) shall be disposed of using a process that is aligned with the US NIST Special Publication 800-88 Moderate controls baseline.

a. Paper format:

i. Shredding.

ii. Burning.

iii. Pulping.

iv. Pulverizing.

v. Rendered unreadable, and unable to be reconstructed

b. Electronic format:

i. Clearing i.e. using software or hardware products to overwrite media with nonsensitive data.

ii. Purging i.e. degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains.

iii. Destroying i.e. disintegration, pulverization, melting, incinerating, or shredding.

5.1.8 Off-Site backup

Full system backups of the CAs, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS.   Backups shall be performed and stored off-site not less than once every 7 days. At least one full backup copy shall be stored at an offsite location (at a location separate from the CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role (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 extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. An auditable record must be created identifying when personnel are added or removed from a trusted role, as well as who added or removed them from the role. The individual who authorized the role assignment, or any series of role assignments over a given period of time, must also be traceable via audit and archive records. Trusted Role appointments must be documented and archived as defined in Section 5.4 and Section 5.5.

The requirements of this policy are drawn in terms of four roles (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile):

1. *Administrator* – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
2. *Officer* – authorized to request or approve certificates or certificate revocations.
3. *Audit Administrator* – authorized to view and maintain audit logs.
4. *Operator* – authorized to perform system backup and recovery.

The following sections define these and other Trusted Roles.

5.2.1.1 Administrator

- The administrator shall be responsible for:
- Installation, configuration, and maintenance of the CA;

- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.
- Administrators shall not issue certificates to subscribers.

5.2.1.2 Officer

- The officer shall be responsible for issuing certificates, that is:
- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates, and;
- Requesting, approving and executing the revocation of certificates.

5.2.1.3 Audit Administrator

- The Audit Administrator shall be responsible for:
- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS;

5.2.1.4 Operator

The operator shall be responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.5 Registration Authority

An RA's responsibilities are:

- Verifying identity, pursuant to section 3.2;
- Entering Subscriber information, and verifying correctness;
- Securely communicating requests to and responses from the CA;
- Receiving and distributing Subscriber certificates.

The RA role is highly dependent on public key infrastructure implementations and local requirements. The responsibilities and controls for RAs shall be explicitly described in the CPS of a CA if the CA uses an RA.

5.2.1.6 CSA Roles

A CSA shall have at least the following roles.

- The CSA administrator shall be responsible for:
- Installation, configuration, and maintenance of the CSA;
- Establishing and maintaining CSA system accounts;
- Configuring CSA application and audit parameters, and;
- Generating and backing up CSA keys.
- The CSA Audit Administrator shall be responsible for:
- Reviewing, maintaining, and archiving audit logs;

- Performing or overseeing internal compliance audits to ensure that the CSA is operating in accordance with its CPS;

The operator shall be responsible for the routine operation of the CSA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.7 [Reserved]

5.2.1.8 Trusted Agent

A Trusted Agent is responsible for:

- Verifying identity, pursuant to section 3.2; and
- Securely communicating subscriber information to the RA.

A Trusted Agent need **not** be a Trusted Role.

5.2.2 Number of Persons Required per Task

Two or more persons shall be required to perform the following tasks:

- CA and CSA key generation;
- CA and CSA signing key activation;
- CA and CSA private key backup.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a Trusted Role as defined in Section 5.2.1.

Multiparty control shall not be achieved using personnel that serve in the Auditor Administrator Role.

All roles are recommended to have multiple persons in order to support continuity of operations.

5.2.3 Identification and Authentication for Each Role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

An individual in a trusted role shall authenticated to remote components of the PKI using a method commensurate with the strength of the PKI.

5.2.4 Roles Requiring Separation of Duties

Role separation, when required as set forth below, may be enforced either by the CA equipment (using hardware or software), or procedurally, or by both means.

Individual CA, CSA and CMS personnel shall be specifically designated to the four roles defined in Section 5.2.1 above, as applicable. Individuals may assume more than one role, except:

- Individuals who assume an Officer role may not assume an Administrator or Audit Administrator role;
- Individuals who assume an Audit Administrator shall not assume any other role; and

- Under no circumstances shall any of the four roles perform its own compliance auditor function.

No individual shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

A group of individuals responsible and accountable for the operation of each CA and CSA shall be identified. The Trusted Roles of these individuals per Section 5.2.1 shall be identified.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation. Personnel appointed to Trusted Roles (including CA trusted roles, CSA trusted roles, and RA role) shall:

- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere or conflict with their duties for the trusted role;
- Have not been previously relieved of duties for reasons of negligence or non-performance of duties;
- Have not been denied a security clearance, or had a security clearance revoked for cause[3];
- Have not been convicted of a felony offense; and
- Be appointed in writing by an approving authority.

For PKIs operated at Basic, Medium Software, and Medium Hardware, each person filling a Trusted Role shall satisfy at least one of the following requirements:

- The person shall be a citizen of the country where the CA is located; or
- For PKIs operated on behalf of multinational governmental organizations, the person shall be a citizen of one of the member countries; or
- For PKIs located within the European Union, the person shall be a citizen of one of the member states of the European Union; or
- The person shall have a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32; or
- For RAs and personnel appointed to the trusted roles for the CSAs, in addition to the above, the person may be a citizen of the country where the function is located.

[3] Practice Note: In order to make the determination if a person was denied clearance or had clearance revoked for cause, it is sufficient to rely on the local Facility Security Officer (FSO) database, Joint Personnel Adjudication System (JPAS), and assertions by the person on security clearance forms.

5.3.2 Background Check Procedures

All persons filling Trusted Roles (including CA trusted roles, CSA trusted roles, and RA role), shall have completed a favorable background investigation. The scope of the background check shall include the following areas covering the past five years, excepting the residence check which shall cover at least the past three years:

- Employment[4];
- Education (Regardless of the date of award, the highest educational degree shall be verified);
- Place of residence (3 years);
- Law Enforcement; and
- References

Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with United States Executive Order 12968 August 1995, or equivalent.

The results of these checks shall not be released except as required in Sections 9.3 and 9.4

Background check procedures shall be described in the CPS.

If a formal clearance or other check is the basis for background check, the background refresh shall be in accordance with the corresponding formal clearance or other check. Otherwise, the background check shall be refreshed every ten years.

One way to meet these requirements of this section is to have a national agency security clearance that is based on a five year background investigation. As an example, a successfully adjudicated United States National Agency Check with Written Inquires (NACI) or United States National Agency Check with Law Enforcement Check (NACLC) on record is deemed to have met the requirements of this section.

Practice Note: The qualifications of the adjudication authority and procedures utilized to satisfy these requirements must be demonstrated before cross certification with the Exostar FISRCA.

Practice Note: Interim clearance may be acceptable. However, if the final adjudication is not favorable, all certificates issued while the person had a trusted role may require re-evaluation and possibly revocation.

5.3.3 Training Requirements

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

- CA/CSA/RA security principles and mechanisms
- All PKI software versions in use on the CA system
- All PKI duties they are expected to perform

[4] If the person has been in the work-force for less than five years, the employment verification shall consist of the periods during which the person has been in the work-force.

- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles shall be aware of changes in the CA, CSA, or RA operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, RA software upgrades, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The Exostar PMA shall take appropriate administrative and disciplinary actions against personnel who violate this policy.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to CA, CSA, or RA operations shall meet applicable requirements set forth in this CP (e.g., all requirements of Section 5.3).

5.3.8 Documentation Supplied To Personnel

The CA and CSA shall make available to its personnel the certificate policies they support, the CPS, and any relevant statutes, policies or contracts. Other technical, operations and administrative documents (e.g., Administrator Manual, User Manual, etc.) shall be provided in order for the trusted personnel to perform their duties.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CAs, CSAs, and RAs. For CAs operated in a virtual machine environment (VME), audit logs shall be generated for all applicable events on both the virtual machine (VM) and isolation kernel (i.e. hypervisor).

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. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 5.5.2.

5.4.1 Types of Events Recorded

All security auditing capabilities of the CA, CSA, and RA operating system and the CA, CSA, and RA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,

- The date and time the event occurred,
- Outcome of the event to include success or failure;
- Identity of any individuals, subjects, or objects/entities associated with the event,
- A message from any source requesting an action by a CA is an auditable event. The message must include message date and time, source, destination and contents.

The following events shall be audited:

Auditable Event	CA	CSA	RA
SECURITY AUDIT			
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X
Obtaining a third-party time-stamp	X	X	X
IDENTIFICATION AND AUTHENTICATION			
Successful and unsuccessful attempts to assume a role	X	X	X
The value of *maximum number of authentication attempts* is changed	X	X	X
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	X	X
LOCAL DATA ENTRY			
All security-relevant data that is entered in the system	X	X	X
REMOTE DATA ENTRY			
All security-relevant messages that are received by the system	X	X	X
DATA EXPORT AND OUTPUT			
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X
KEY GENERATION			
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	X	X
PRIVATE KEY LOAD AND STORAGE			
The loading of Component private keys	X	X	X
All access to certificate subject Private Keys retained within the CA for key recovery purposes	X	N/A	N/A

Auditable Event	CA	CSA	RA
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE			
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X
SECRET KEY STORAGE			
The manual entry of secret keys used for authentication	X	X	X
PRIVATE AND SECRET KEY EXPORT			
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X
CERTIFICATE REGISTRATION			
All certificate requests	X	N/A	X
CERTIFICATE REVOCATION			
All certificate revocation requests	X	N/A	X
CERTIFICATE STATUS CHANGE APPROVAL			
The approval or rejection of a certificate status change request	X	N/A	N/A
CA CONFIGURATION			
Any security-relevant changes to the configuration of the Component	X	X	X
ACCOUNT ADMINISTRATION			
Roles and users are added or deleted	X	-	-
The access control privileges of a user account or a role are modified	X	-	-
CERTIFICATE PROFILE MANAGEMENT			
All changes to the certificate profile	X	N/A	N/A
CERTIFICATE STATUS AUTHORITY MANAGEMENT			
All changes to the CSA profile (e.g. OCSP profile)	N/A	X	N/A
REVOCATION PROFILE MANAGEMENT			
All changes to the revocation profile	X	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT			
All changes to the certificate revocation list profile	X	N/A	N/A
MISCELLANEOUS			
Appointment of an individual to a Trusted Role	X	X	X
Designation of personnel for multiparty control	X	-	N/A
Installation of the Operating System	X	X	X
Installation of the PKI Application	X	X	X
Installation of hardware cryptographic modules	X	X	X

Auditable Event	CA	CSA	RA
Removal of hardware cryptographic modules	X	X	X
Destruction of cryptographic modules	X	X	X
System Startup	X	X	X
Logon attempts to PKI Application	X	X	X
Receipt of hardware / software	X	X	X
Attempts to set passwords	X	X	X
Attempts to modify passwords	X	X	X
Back up of the internal CA database	X	-	-
Restoration from back up of the internal CA database	X	-	-
File manipulation (e.g., creation, renaming, moving)	X	-	-
Posting of any material to a PKI Repository	X	-	-
Access to the internal CA database	X	X	-
All certificate compromise notification requests	X	N/A	X
Loading tokens with certificates	X	N/A	X
Shipment of Tokens	X	N/A	X
Zeroizing Tokens	X	N/A	X
Re-key of the Component	X	X	X
CONFIGURATION CHANGES			
Hardware	X	X	-
Software	X	X	X
Operating System	X	X	X
Patches	X	X	-
Security Profiles	X	X	X
PHYSICAL ACCESS / SITE SECURITY			
Personnel Access to room housing Component	X	-	-
Access to the Component	X	X	-
Known or suspected violations of physical security	X	X	X
ANOMALIES			
Software error conditions	X	X	X
Software check integrity failures	X	X	X
Receipt of improper messages	X	X	X
Misrouted messages	X	X	X
Network attacks (suspected or confirmed)	X	X	X
Equipment failure	X	-	-

Auditable Event	CA	CSA	RA
Electrical power outages	X	-	-
Uninterruptible Power Supply (UPS) failure	X	-	-
Obvious and significant network service or access failures	X	-	-
Violations of Certificate Policy	X	X	X
Violations of Certification Practice Statement	X	X	X
Resetting Operating System clock	X	X	X

5.4.2 Frequency of Processing Audit Logs

Audit logs shall be reviewed at least once every 30 days. Statistically significant sample of security audit data generated by the CA, CSA, or RA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. The Audit Administrator shall explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained onsite for at least sixty days as well as being retained in the manner described below. For the CA and CSA, Audit Administrator shall be the only person responsible to manage the audit log (e.g., review, backup, rotate, delete, etc.). For the RA, a system administrator other than the RA shall be responsible for managing the audit log.

5.4.4 Protection of Audit Logs

System configuration and procedures shall be implemented together to ensure that:

- Only authorized people[5] have read access to the logs;
- Only authorized people may archive audit logs; and,
- Audit logs are not modified.

The person performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access). Audit logs shall be moved to a safe, secure storage location separate from the CA equipment.

[5] For the CA and CSA, the authorized individual shall be the Audit Administrator. For RA, the authorized individual shall be a system administrator other than the RA.

The individual who supervises the removal of audit logs from the CA system and controls the removed audit logs shall be an official different from the individuals who, in combination, command the CA signature key.

It is acceptable for the system to over-write audit logs after they have been backed up and archived.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least once every 30 days. A copy of the audit log shall be sent off-site in accordance with the CPS every 30 days.

The process for transferring the audit records to the backup environment must be documented.

5.4.6 Audit Collection System (internal vs. external)

The audit log collection system may or may not be external to the CA, CSA, or RA. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the CA shall determine whether to suspend CA operation until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

No stipulations beyond Section 5.4.2

5.5 Records Archival

5.5.1 Types of Records Archived

CA, CSA, and RA archive records shall be sufficiently detailed to establish the proper operation of the component or the validity of any certificate (including those revoked or expired) issued by the CA.

Data To Be Archived	CA	CSA	RA
Certification Practice Statement	X	X	X
Contractual obligations	X	X	X
System and equipment configuration	X	X	-
Modifications and updates to system or configuration	X	X	-
Certificate requests	X	-	-
Revocation requests	X	-	-
Subscriber identity authentication data as per Section 3.2.3	X	N/A	X
Documentation of receipt and acceptance of certificates, including Subscriber Agreements	X	N/A	X

Data To Be Archived	CA	CSA	RA
Documentation of receipt of Tokens	X	N/A	X
All certificates issued or published	X	N/A	N/A
Record of Component CA Re-key	X	X	X
All CRLs and CRLs issued and/or published	X	N/A	N/A
All Audit Logs	X	X	X
Other data or applications to verify archive contents	X	X	X
Documentation required by compliance auditors	X	X	X

5.5.2 Retention Period for Archive

The minimum retention periods for archive data is 10 years and 6 months.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archive data shall also be maintained for the minimum retention period specified above.

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CA and CSA, the authorized individuals are Audit Administrators. For the RA, authorized individuals are someone other than the RA (e.g., Information Assurance Officer or IAO). The contents of the archive shall not be released except as determined by the Exostar PMA for the Exostar PKI, or as required by law. Records of individual transactions may be released upon request of any Subscriber involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the component (CA, CSA, or RA) with physical and procedural security controls equivalent or better than those for component.

5.5.4 Archive Backup Procedures

The applicable CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for Time-Stamping of Records

CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (internal or external)

Archive data may be collected in any expedient manner, but must be documented in the associated CPS.

5.5.7 Procedures to Obtain & Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store archive information shall be described in the applicable CPS.

5.6 Key Changeover

Each CA’s signing key must have a validity period as described in Section 6.3.2.

Prior to the end of a CA’s signing key validity period, a new CA must be established or a re-key on the existing CA must be performed. This is referred to as key changeover. From that time on, only the new key is used to sign CA and Subscriber certificates. The old private key may continue to be used to sign CRLs. If the old private key is used to sign CRLs that cover certificates signed with that key, the old key must be retained and protected.

After all certificates signed with the old key have expired or been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates. This final CRL must be available for all relying parties until the validity period of all issued certificates has passed. Once the last CRL has been issued, the old private signing key of the CA may be destroyed.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Exostar shall have a formal disaster recovery plan.

If a CA or CSA detects a potential hacking attempt or other form of compromise, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA or CSA key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA or CSA needs to be rebuilt, only some certificates need to be revoked, and/or the CA or CSA key needs to be declared compromised.

The Exostar PMA shall be notified by the Exostar OA if any of the following cases occur:

- suspected or detected compromise of an Exostar CA system;
- physical or electronic attempts to penetrate an Exostar CA system;
- denial of service attacks on an Exostar CA component; or
- any incident preventing an Exostar CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL; or
- A CA certificate revocation is planned.

In the event of an incident as described above, the Exostar PMA shall notify cross-certified entities within 24 hours of incident discovery, along with preliminary remediation analysis.

Within 10 business days of incident resolution, Exostar shall post a notice on its public web page identifying the incident and provide notification to the FPKIPA. The public notice shall include the following:

1. Which CA components were affected by the incident
2. The CA's interpretation of the incident.
3. Who is impacted by the incident

4. When the incident was discovered
5. A complete list of all certificates that were either issued erroneously or not compliant with the CP/CPS as a result of the incident
6. A statement that the incident has been fully remediated

Appropriate incident notification provided directly to the FPKIPA shall also include detailed measures taken to remediate the incident.

The above measures will allow member entities to protect their interests as Relying Parties.

A CA Operational Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the respective CPS.

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

If a CA or CSA equipment is damaged or rendered inoperative, but the signature keys are not destroyed**;** the operation shall be re-established as quickly as possible, giving priority to the ability to generate certificate status information. Before returning to operation, Exostar shall ensure that the system's integrity has been restored.

If a CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs that have been issued certificates by the CA shall be securely[6] notified at the earliest feasible time. This will allow other CAs to protect their subscribers' interests as Relying Parties. The CA shall re-establish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. If revocation capability cannot be established in a reasonable timeframe, the CA shall determine whether to request revocation of its certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all subscribers that use the CA as a trust anchor to delete the trust anchor.

In the event of an incident as described above, the Exostar shall post a notice on its web page(https://www.myexostar.com/?ht_kb=policy-and-compliance) identifying the incident and provide notification to the FPKIPA and cross-certified entities. See Section 5.7.1 for contents of the notice.

5.7.3 Private Key Compromise Procedures

If the FBCA signature keys are compromised or lost (such that compromise is possible even though not certain):

- The FPKIPA and all of its member entities shall be notified so that entities may issue CRLs revoking any cross-certificates issued to the compromised CA;

- A new FBCA key pair shall be generated by the FBCA in accordance with procedures set forth in the FBCA CPS; and

[6] With confidentiality, source authentication, and integrity security services applied.

- New FBCA certificates shall be issued to Entities also in accordance with the FBCA.

If the CA distributes its key in a self-signed certificate, the new self-signed certificate shall be distributed as specified in Section 6.1.4.

The FPKIMA shall also investigate and report to the FPKIPA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request that its certificates be revoked. The CA shall follow steps outlined in Section 5.7.3.

The PKI Repositories containing certificates and certificate status information shall be deployed so as to provide 24 hour per day/365 day per year availability. Exostar shall implement features to provide high levels of PKI Repository reliability (99.9% availability or better).

5.8 CA, CSA, and RA Termination

In the event of termination of a CA, the CA shall request all certificates issued to it be revoked. Any certificates issued by the terminated CA that have not expired, shall be revoked and a final long term CRL with a *nextUpdate* time past the validity period of all issued certificates shall be generated. This final CRL shall be available for all relying parties until the validity period of all issued certificates has past. Once the last CRL has been issued, the private signing key(s) of the terminated CA will be destroyed.

In the event of a CA termination, the Entity responsible shall provide notice to all cross-certified CAs prior to the termination. Additionally, in the case of an Exostar CA termination, Entities will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought. For emergency termination, CAs shall follow the notification procedures in Section 5.7.

A CA, CSA, and RA shall archive all audit logs and other records prior to termination.

A CA, CSA, and RA shall destroy all its private keys upon termination.

CA, CSA, and RA archive records shall be transferred an appropriate authority such as the PMA responsible for the entity.

If a Root CA is terminated, the Root CA shall use secure means to notify the subscribers to delete all trust anchors representing the CA.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The following table provides the requirements for key pair generation for the various entities.

Entity	FIPS 140-1/2 Level	Hardware or Software
CA	3	Hardware
RA	2	Hardware
OCSP Responder	2	Hardware
SCVP Server	2	Hardware
Code Signing	2	Hardware
End Entity Signature or Authentication (Basic)	1	Hardware or Software
End Entity Encryption (Basic)	1	Hardware or Software
End Entity Signature or Authentication (Medium Software)	1	Software
End Entity Encryption (Medium Software)	1	Software
End Entity Signature or Authentication (Medium Hardware)	2	Hardware
End Entity Encryption (Medium Hardware)	2	Hardware
Device (Basic)	1	Hardware or Software
Device (Medium Software)	1	Software
Device (Medium Hardware)	2	Hardware

Where a FIPS-validated module is used, key generation shall be performed using a FIPS approved method or equivalent international standard.

Random numbers for Medium Hardware assurance level keys shall be generated in FIPS 140 Level 2 validated hardware cryptographic modules.

When private keys are not generated on the token to be used, originally generated private keys shall be destroyed after they have been transferred to the token. This does not prohibit the key generating modules to act as the key escrow module also.

Multiparty control shall be used CA key pair generation, as specified in Section 5.2.2.

CA key pair generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used.

For Medium assurance levels, an independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.2 Private Key Delivery to Subscriber

The CA shall generate their own key pair and therefore do not need private key delivery.

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the Subscriber, then the private key shall be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements shall be met:

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber.
- The private key shall be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
    - For hardware modules, accountability for the location and state of the module shall be maintained until the Subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

The CA or the RA shall maintain a record of the subscriber acknowledgement of receipt of the token.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber’s identity shall be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the Subscriber’s verified identity to the public key. If cryptography is used to achieve this binding, it shall be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of a trust anchor shall be provided to the subscribers acting as relying parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution. Acceptable methods for delivery of trust anchor include but are not limited to:

- The CA loading a trust anchor onto tokens delivered to subscribers via secure mechanisms;
- Secure distribution of a trust anchor through secure out-of-band mechanisms;
- Comparison of certificate hash (fingerprint) against trust anchor hash made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); or
- Loading trust anchor from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded and the trust anchor is not in the certification chain for the Web site certificate.

6.1.5 Key Sizes

If the Exostar PMA determines that the security of a particular algorithm may be compromised**,** it may require the CAs to revoke the affected certificates. All certificates and Transport Layer Security (TLS) protocols shall use the following algorithm suites.

Cryptographic Function	**Expire after 12/31/2010 and before 12/31/2030**	**Expire after 12/31/2030**
Public keys in CA, Identity, Authentication, and Digital Signature Certificates; CRL Signatures; and OCSP Response Signatures (FIPS 186-4)	2048 bit RSA, 224 bit prime field, or 233 bit binary field	3072 bit RSA, 256 bit ECDSA in prime field, or 283 bit ECDSA in binary field
Public Keys in Encryption Certificates (PKCS 1 for RSA and NIST SP 800-56A for ECDH)	2048 bit RSA, 224 bit prime field or 233 bit binary field	3072 bit RSA, 256 bit ECDSA in prime field, or 283 bit ECDSA in binary field
Symmetric Encryption	3 Key TDES or AES	AES

	Exostar SHA-2 PKI
	All Dates
Hashing Algorithm for Certificates	SHA-256
Hashing Algorithm for CRLs	SHA-256

Regardless, all CAs shall use 2048 bit RSA or stronger.

CSAs shall use the same signature algorithms, key sizes, and hash algorithms as used by the CA to sign the CRL.

Only SHA-2 may be used for certificates and CRLs under the “id-basic-sha2”, “id-mediumSoftware-sha2”, “id-mediumHardware-sha2”, and “id-basic-sha2” OIDs after 12/31/2010.

An Exostar CA which possesses an “id-basic-sha2”, “id-mediumSoftware-sha2”, or “id-mediumHardware-sha2”, or issues certificates at those levels, shall not issue any certificates using the SHA-1 hashing algorithm.

6.1.6 Public Key Parameters Generation and Quality Checking

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186-4.

Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186-4.

ECDSA and ECDH keys shall be generated in accordance with FIPS 186-4. Curves from FIPS 186-4 shall be used.

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

The use of a specific key is determined by the key usage and extended key usage extensions in the X.509 certificate.

- Certificates to be used for authentication shall set the *digitalsignature* bit only.
- Certificates to be used for digital signatures shall set the *digitalsignature* and *nonrepudiation* bits.
- Certificates that have the *nonrepudiation* bit set, shall not have *keyEncipherment* bit or *keyAgreement* bit set.
- Certificates to be used for encryption shall set the *keyEncipherment* bit.
- Certificates to be used for key agreement shall set the *keyAgreement* bit.
- CA certificates shall set *cRLSign* and *keyCertSign* bits.

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using key management certificates and require setting both digitalsignature and keyEncipherment bits.

For End Entity certificates, the Extended Key Usage extension shall always be present and shall not contain anyExtendedKeyUsage {2.5.29.37.0}.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*. Cryptographic modules shall be validated to the FIPS 140-2 level identified in this section. Additionally, the Exostar PMA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the CAs.

Practice Note: The Exostar PMA may determine that other comparable validation, certification, or verification standards are sufficient when cross-certifying with non-U.S. government PKIs.

The table in Section 6.1.1 summarizes the minimum requirements for cryptographic modules; higher levels may be used. In addition, private keys shall not exist outside the cryptographic module in plaintext form.

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location. When a collection of private keys for Subscriber certificates are held in a single location, there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber.

Cryptographic modules for Custodial Subscriber Key Stores at the Rudimentary Assurance Level shall be no less than FIPS 140 Level 1 (Hardware or Software). For all other levels, the cryptographic module shall be no less than FIPS 140 Level 2 Hardware.

Practice Note: The Exostar PMA may determine that other comparable validation, certification, or verification standards are sufficient when cross-certifying with non-U.S. government PKIs.

In addition, authentication to the Cryptographic Device in order to activate the private key associated with a given certificate shall require authentication commensurate with the assurance level of the certificate.

6.2.2 Private Key Multi-Person Control

Use of a CA or CSA private signing key shall require action by at least two persons.

6.2.3 Private Key Escrow

CA private keys are never escrowed.

Human Subscriber key management keys may be escrowed to provide key recovery as described in Section 4.12.1.

Subscriber private signature keys shall not be escrowed.

The end entity private keys used solely for decryption shall be escrowed prior to the generation of the corresponding certificates.

Subscriber private dual use keys must not be escrowed. If a device has a separate key management key certificate, the key management private key may be escrowed.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multi-person control as the original signature key. A single backup copy of the signature key shall be stored at or near the CA location. A second backup copy shall be kept at the CA backup location. Procedures for CA private signature key backup shall be included in the appropriate CPS and shall meet the multiparty control requirement of Section 5.2.2.

6.2.4.2 Backup of Subscriber Private Signature Key

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting Basic or Medium Software may be backed up or copied, but must be held in the Subscriber's control. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the Medium Hardware may not be backed up or copied.

Backed up subscriber private signature keys shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.4.3 CSA Private Key Backup

If backed up, the CSA private signature keys shall be backed up under the same multi-person control as the signature key is invoked, and all copies shall be accounted for and protected in the same manner as the original. A single backup copy of the signature key may be stored at or near the CSA location. A second backup copy may be kept at the CSA backup location. Procedures for CSA private signature key backup shall be included in the appropriate CPS.

6.2.4.4 Backup of Device Private Keys

Device private keys may be backed up or copied, but must be held under the control of the device's human sponsor or other authorized administrator. Backed up device private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the device's cryptographic module.

6.2.5 Private Key Archival

Private signature keys shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA and CSA private keys shall be generated by and remain in a cryptographic module. The CA and CSA private keys may be backed up in accordance with Section 6.2.4.1.

In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

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

6.2.7 Private Key Storage on Cryptographic Module

The cryptographic module may store private keys in any form as long as the keys are not accessible without authentication mechanism that is in compliance with FIPS 140-1/2 rating of the cryptographic module.

6.2.8 Method of Activating Private Key

The user must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. When passphrases or PINs are used, they shall be a minimum of six (6) characters. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Methods of Deactivating Private Key

The cryptographic modules that have been activated shall not be available to unauthorized access.

If cryptographic modules are used to store Subscriber Private Keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 Method of Destroying Private Key

Individuals in trusted roles must destroy the private signature keys when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a “zeroize” command. Physical destruction of hardware should not be required.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects Of Key Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods/Key Usage Periods

CAs must not issue subscriber certificates that extend beyond the expiration date of their own certificates and public keys.

The validity period of the subscriber certificate must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1

Also see Section 5.6.

A CA private key may be used to sign CRLs for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair’s usage period. The following table provides the life times for the private keys and certificates issued to the owner of that private key.

Key	1024 Bits		2048 Bit Keys	
	Private Key	Certificate	Private Key	Certificate
Root CA	5 years	5 years	20 years	20 years

Cross Certified CA	N/A	N/A	20 years	20 years
Signing CA	5 years	5 years	6 years	10 years
Subscriber Identity or Signature	3 years	3 years	3 years	3 years
Subscriber Encryption	No Limit	3 years	No Limit	3 years
Code Signer	3 years	3 years	3 years	8 years
OCSP Responder	3 years	1 month	3 years	1 month
SCVP Server	3 years	3 years[7]	3 years	3 years
Server	3 years	3 years	3 years	3 years

2048-bit RSA certificates, including self-signed certificates shall not be issued with validity beyond December 31, 2030.

6.3.3 Subscriber Private Key Usage Environment

Subscribers shall use their private keys only from machines that are protected and managed using commercial best practices for computer security and network security controls.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptomodule used to store the keys. Subscriber activation data may be user selected. For CAs, it shall either entail the use of biometric data or satisfy the policy-enforced at/by the cryptographic module. 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.

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

6.4.2 Activation Data Protection

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

[7] SCVP Server certificate shall be self-signed since the SCVP Servers are considered to provide certificate validation services.

6.4.3 Other Aspects of Activation Data

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

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA, CSA and RA shall include the following functionality (in a VME these functions are applicable to both the VM and hypervisor):

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability (see Sections 5.4 and 5.5)
- Prohibit object re-use
- Require use of cryptography for session communication and database security
- Require a trusted path for identification and authentication
- Provide domain isolation for process
- Provide self-protection for the operating system
- Require self-test security related CA services (e.g., check the integrity of the audit logs)
- Support recovery from key or system failure

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

The computer system shall be configured with a minimum of required accounts, network services, and no remote login.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the CA and CSA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Hardware and software developed shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- The hardware and software, including the VME hypervisor, shall be dedicated to operating and supporting the CA (i.e. the systems and services dedicated to the issuance and management of certificates). There shall be no other applications, hardware devices, network connections, or component software installed which are not part of the PKI operation. In a VME, a single hypervisor may support multiple CAs and their supporting systemsm, provided all systems have comparable security controls and are dedicated to the support of the CA.
- In a VME, all VM systems must operate in the same security zone as the CA.
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the PKI operations shall be obtained from sources authorized by local policy. CA, CSA, and RA hardware and software shall be scanned for malicious code on first use and periodically thereafter. Except for Offline CAs, CA and RA hardware and software must be scanned for malicious code on first use and periodically thereafter.
- 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.

6.6.2 Security Management Controls

The configuration of the CA and CSA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CA and CSA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the CA system. The CA and CSA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. For the Exostar CA, the integrity of the software shall be verified by the Exostar Operational Authority at least once every 7 days for online CAs (e.g., in conjunction with CRL publication) and at least once every 30 days for offline CAs.

In addition, only applications needed to perform the organization's mission shall be loaded on the RA Workstation, and all such software shall be obtained from sources authorized by local policy.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

CAs, CSAs, and RAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the CA.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Time Stamping

All CA and CSA components shall regularly synchronize with a time service such as National Institute of Standards and Technology (NIST) Atomic Clock or NIST Network Time Protocol (NTP) Service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's certificate
- Revocation of a Subscriber's certificate
- Posting of CRL updates

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as listed in Section 5.4.1.

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version Numbers

The CAs shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

Critical private extensions shall be interoperable in their intended community of use.

CA certificates shall not include critical private extensions.

CA and Subscriber certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP. Section 10 contains the certificate formats.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha256(2)}

Certificates under this CP shall use the following OID for identifying the subject public key information:

rSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) public-key-type(2) 1}

7.1.4 Name Forms

The subject and issuer fields of the certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by RFC5280. Certificates exhibiting ETSI QC Public OIDs shall be further constrained by RFC 3739, ETSI TS 101 456, and ETSI TS 101 862.

Subject and issuer fields shall include attributes as detailed in the table below.

Subject Name Form (CAs)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Recommended	CN	0…1	Descriptive name for CA, e.g., “CN=XYZ Inc CA”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Certification Authorities” or similar text
	Required	O	1	Issuer name, e.g., “O=XYZ Inc”
	Required	C	1	Country name, e.g., “C=US”
2	Recommended	CN	0…1	Descriptive name for CA, e.g., “CN=XYZ Inc CA”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Certification Authorities” or similar text
	Optional	O	0…1	Issuer name, e.g., “O=XYZ Inc”

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
	Optional	C	0…1	Country name, e.g., “C=US”
	Required	DC	1	Domain name, e.g., “DC=xyzinc”
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or, “DC=com, DC=au”, etc.

Subject Name Form (Non-CAs)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See right	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email, etc.
	Optional	OU	0…N	As needed
	Required	O	1	Issuer name, e.g., “O=XYZ Inc” exactly as it appears in the CA certificate(s)
	Required	C	1	Country name, e.g., “C=US” exactly as it appears in the CA certificate(s)
2	Required	See right	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email, etc.
	Optional	OU	0…N	As needed
	Optional	O	0…1	Issuer name, e.g., “O=XYZ Inc”
	Required	DC	1	Domain name, e.g., “DC=xyzinc” exactly as it appears in the CA certificate(s)
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or, “DC=com, DC=au”, etc. exactly as it appears in the CA certificate(s)

When multiple values exist for an attribute in a DN, the DN shall be encoded so that each attribute value is encoded in a separate relative distinguished name.

7.1.5 Name Constraints

Principal CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats in Section 10 subject to the requirements above.

A CA may obscure a Subscriber Subject name to meet local privacy regulations as long as such name is unique and traceable to a corresponding unobscured name. Issuer names may not be obscured. A CA may assert critical or non-critical name constraints beyond those specified in the Certificate Formats.

7.1.6 Certificate Policy Object Identifier

CA and Subscriber Certificates issued under this CP shall assert a id-basic, id-mediumSoftware, id-mediumHardware, qcp-public, and/or qcp-public+sscd certificate policy OID. This policy document assumes a strict ordering among these policies, with id-mediumHardware, and qcp-public+sscd being the highest assurance. When a CA asserts a policy OID, it shall also assert all lower assurance policy OIDs for which it has been certified. Thus:

- If a CA issues an id-mediumHardware certificate, it shall assert id-mediumHardware, id-mediumSoftware, and id-basic OIDs.
- If a CA issues an id-mediumSoftware certificate, it shall assert id-mediumSoftware and id-basic OIDs.

7.1.7 Usage of Policy Constraints Extension

The CAs may assert policy constraints in CA certificates. When this extension appears, at least one of requireExplicitPolicy or inhibitPolicyMapping must be present. When present, this extension should be marked as noncritical, to support legacy applications that cannot process policyConstraints. For Subordinate CA certificates inhibitPolicyMappings, skip certs will be set to 0. For cross-certificates inhibitPolicyMappings, skip certs will be set to 1.When requireExplicitPolicy is included skip certs will be set to 0.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under the Exostar CP may contain policy qualifiers such as user notice, policy name, and CP and CPS pointers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension shall conform to X.509 certification path processing rules.

7.1.10 Inhibit Any Policy Extension

The CAs may assert InhibitAnyPolicy in CA certificates. When present, this extension should be marked as noncritical*, to support legacy applications that cannot process InhibitAnyPolicy. Skip Certs shall be set to 0.

*Note: The recommended criticality setting is different from RFC 5280

7.2 CRL Profile

7.2.1 Version Numbers

CAs shall issue X.509 version two (v2) CRLs (populate version field with integer "1").

7.2.2 CRL and CRL Entry Extensions

Critical private extensions shall be interoperable in their intended community of use.

Section 10 contains the CRL formats.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS and the provisions of the MOA are being implemented and enforced.

8.1 Frequency or Circumstances of Assessments

All CAs, RAs and CSAs shall be subject to a periodic compliance audit at least once per year.

8.2 Identity and Qualifications of Assessor

The compliance auditor shall demonstrate competence in the field of compliance audits, and shall be thoroughly familiar with requirements of the CP. The compliance auditor must perform such compliance audits as a primary responsibility. The applicable CPS shall identify the compliance auditor and justify the compliance auditor's qualifications.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor shall be a firm, which is independent from the entity being audited. The Exostar PMA shall determine whether a compliance auditor meets this requirement.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a component operates in accordance with the applicable CP, the component CPS, and the applicable MOAs between Exostar and other Entities. Additionally, audits of FIS CA include assessment of the technical and operational aspects of Exostar's PKI as required by Directive 1999/93/EC, ETSI TS 101 456, *tScheme*, and ISO 27001.

8.5 Actions Taken as a Result of Deficiency

The Exostar PMA may determine that a CA is not complying with its obligations set forth in this CP or the respective MOA. When such a determination is made, the Exostar PMA may suspend operation of a noncompliant CA it controls, or may direct the Exostar Operational Authority to cease interoperating with the affected CA (e.g., by revoking the certificate that the FISRCA had issued to the CA), or may direct that other corrective actions be taken which allow interoperation to continue. When the compliance auditor finds a discrepancy between how an Exostar CA is designed or is being operated or maintained, and the requirements of this CP, the MOA, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the Exostar PMA of the discrepancy;
- The Exostar PMA shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the MOA, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Exostar PMA may decide to halt temporarily operation of an Exostar CA, to revoke a certificate issued by the Exostar CA, or take other actions it deems appropriate. The Exostar PMA shall develop procedures for making and implementing such determinations.

8.6 Communication of Results

9 On an annual basis, the Exostar must submit an annual review package to the FPKIPA. This package must be prepared in accordance with the *FPKI Annual Review Requirements* document and includes an assertion that all PKI components have been audited - including any components that may be separately managed and operated. The package must identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results must be communicated as set forth in Section 8.5 above.

OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance and Renewal Fees

Unless (a) otherwise restricted by separate agreement or (b) prohibited by applicable law or any cross-certified authorities, Exostar may set any reasonable certificate issuance and renewal fees.

9.1.2 Certificate Access Fees

Exostar CAs may not charge for access to any certificates.

9.1.3 Revocation or Status Information Access Fees

Exostar CAs may not charge for access to any revocation or status information.

9.1.4 Fees for Other Services

Unless (a) otherwise restricted by separate agreement or (b) prohibited by applicable law or any cross-certified authorities, Exostar may set any reasonable fees for any other services that Exostar may offer.

9.1.5 Refund Policy

CAs may, but are not required to, have a documented refund process.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Exostar maintains reasonable levels of insurance coverage to address foreseeable liability obligations to PKI Participants.

9.2.2 Other Assets

Exostar maintains sufficient financial resources to maintain operations and fulfill duties. CAs shall also maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to participants in the Exostar PKI.

9.2.3 Insurance or Warranty Coverage for End-Entities

CAs may, but are not required to, offer protection to end entities that extends beyond the protections provided in this CP. Any such protection shall be offered at commercially reasonable rates.

9.3 Confidentiality of Business Information

CAs shall maintain the confidentiality of confidential business information that is clearly marked or labeled as confidential, or by its nature should reasonably be understood to be confidential, and shall treat such information with the same degree of care and security as the CA treats its own most confidential information.

9.4 Privacy of Personal Information

An Exostar CA collects, stores, processes and discloses personally identifiable information in accordance with the Exostar Privacy Policy.

Each cross-certified CA may store, process, and disclose personally identifiable information in accordance with the privacy policy of that CA.

9.5 Intellectual Property Rights

The Exostar Operational Authority or the operational authority of a cross-certified PKI shall not knowingly violate any intellectual property rights held by others.

9.5.1 Property Rights in Certificates and Revocation Information

Subject to any agreements between a CA and its customers, the CA shall retain all Intellectual Property Rights in and to the certificates and revocation information that they issue. For any certificates issued, the PKI shall grant permission to reproduce and distribute certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of certificates is subject to a Memorandum of Agreement (or equivalent contractual mechanism) with the relevant CA. A CA shall grant permission to use revocation information to perform Relying Party functions, subject to applicable contractual agreements.

9.5.2 Property Rights in the CPS

All Intellectual Property Rights in this CP are owned by Exostar and/or its licensors. All Intellectual Property Rights in any CP or CPS are owned by the CA and/or its licensors.

9.5.3 Property Rights in Names

The Certificate Applicant retains all rights, if any, in any trademark, service mark, or trade name of the Certificate Applicant contained in any Customer Application.

9.5.4 Property Rights in Keys

Subject to any agreements between a CA and its customers, ownership of and property rights in key pairs corresponding to certificates of the CA, and Subscribers shall be specified in the applicable CPS regardless of the physical medium within which they are stored and protected. Such persons retain all Intellectual Property Rights in and to these key pairs. Notwithstanding the foregoing, Exostar's CA, CSA, and RA public keys and the certificates containing them are the property of Exostar.

9.6 Representations and Warranties

Representations and warranties between Exostar, its Subscribers, and other involved parties are contained in the following documents:

- Cross Certification Agreements
- Memoranda of Agreement
- Subscriber Agreements

9.6.1 CA Representations and Warranties

CAs operating under this policy shall warrant that their procedures are implemented in accordance with this CP, and that any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this policy.

A CA that issues certificates that assert a policy defined in this document shall conform to the stipulations of this document, including—

Providing to the Exostar PMA a CPS, as well as any subsequent changes, for conformance assessment.

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3.
- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.

9.6.2 RA Representations and Warranties

An RA that performs registration functions as described in this policy shall comply with the stipulations of this policy, and comply with a CPS approved by the Exostar PMA for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy shall conform to the stipulations of this document, including—

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
- Ensuring that obligations are imposed on subscribers in accordance with section 9.6.3, and that subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber

A Subscriber shall be required to sign a document (e.g., a subscriber agreement) containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

In signing or electronically agreeing to the document described above, each Subscriber shall agree to the following:

- Subscriber shall accurately represent itself in all communications with the PKI authorities.
- Subscriber shall protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures; and
- Subscriber shall promptly notify the appropriate CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the CA’s CPS.
- Subscriber shall abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.

If the human sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device's private key and ensure that the device's certificate is only used for authorized purposes, the device sponsor may delegate these responsibilities to an authorized administrator for the device.

The delegation shall be documented and signed by both the device sponsor and the authorized administrator for the device. Delegation does not relieve the device sponsor of his or her accountability for these responsibilities.

9.6.4 Relying Party

Parties who rely upon the certificates issued under a policy defined in this document shall:

- use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- check each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;
- establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment;
- preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades will often invalidate digital signatures and shall be avoided.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, Policy Mapping Agreements, Memorandums of Agreement, and any other related agreements may contain disclaimers of all warranties (other than any express warranties contained in such agreements or set forth in this CP).

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CAS MAY DISCLAIM ANY EXPRESS OR IMPLIED WARRANTIES, OTHER THAN THOSE EXPRESS WARRANTIES CONTAINED IN THIS CP.

EXCEPT FOR THE EXPLICIT REPRESENTATIONS, WARRANTIES, AND CONDITIONS PROVIDED IN THIS CP OR THOSE BETWEEN EXOSTAR AND ITS CUSTOMERS UNDER SEPARATE AGREEMENTS, (A) CERTIFICATES ISSUED BY EXOSTAR AND THE EXOSTAR PKI ARE PROVIDED "AS IS", AND EXOSTAR, ITS EMPLOYEES, OFFICERS, AGENTS, REPRESENTATIVES, AND DIRECTORS DISCLAIM ALL OTHER WARRANTIES, CONDITIONS AND OBLIGATIONS OF EVERY TYPE (INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SECURITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE, OR ACCURACY OF INFORMATION PROVIDED), AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE, FAILURE TO WARN, OR LACK OF REASONABLE CARE AND

(B) THE ENTIRE RISK OF THE USE OF ANY EXOSTAR CERTIFICATES, ANY SERVICES PROVIDED BY EXOSTAR, OR THE VALIDATION OF ANY DIGITAL SIGNATURES LIES WITH THE APPLICABLE PARTICIPANT.

9.8 Limitations of Liabilities

The liability (and/or limitation thereof) of Exostar to CAs to which Exostar issues certificates shall be set forth in the applicable agreements.

OTHER THAN THE ABOVE DESCRIBED LIMITATIONS OF LIABILITY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EXOSTAR BE LIABLE FOR ANY INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CP, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE TOTAL, AGGREGATE LIABILITY OF EACH EXOSTAR CA ARISING OUT OF OR RELATED TO IMPROPER ACTIONS BY THE EXOSTAR CA SHALL BE LIMITED TO ONE THOUSAND DOLLARS ($1,000 USD) PER TRANSACTION AND ONE MILLION DOLLARS ($1 MILLION USD) PER INCIDENT).

9.9 Indemnities

The indemnity requirement of 9.9.1 and 9.9.2 shall not apply when the entity/relying party is an instrumentality of the US Government. Recourse against the United States shall proceed under the Contract Disputes Act or Federal Tort Claims Act as applicable.

9.9.1 Indemnification by Entity CAs

No Stipulation.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, each Relying Party shall indemnify Exostar and its contractors, agents, assigns, employees, officers, and directors from and against any third party claims, liabilities, damages, costs and expenses (including reasonable attorney’s fees), relating to or arising out of use of or reliance by Relying Party on any certificates issued by Exostar, including, without limitation, for:

- The Relying Party’s improper, illegal, or unauthorized use of a certificate (including use of any expired, revoked, or unvalidated certificate);
- The Relying Party’s unreasonable reliance on a certificate, under the circumstances, or
- The Relying Party’s failure to check the status of a certificate on which it relies to determine if the certificate is expired or revoked.

Any applicable contractual agreement between Exostar and a Relying Party within the Exostar PKI may include additional indemnity obligations, but these would not apply to relying parties that are not customers of Exostar.

9.10 Term and Termination

9.10.1 Term

The CP becomes effective upon ratification by the Exostar PMA and publication in the Exostar Repository as a PDF document. Amendments to this CP become effective upon ratification by the Exostar PMA and publication at http://www.myexostar.com/Exostar_FIS_Certificate_Policy.pdf

There is no specified term for this CP.

9.10.2 Termination

While this CP may be amended from time to time, it shall remain in force until replaced by a newer version or explicitly terminated by a resolution of the Exostar PMA. For purposes of clarity, termination of any Memoranda of Agreement shall not operate as a termination of this CP unless this CP is explicitly terminated by a separate resolution of the Exostar PMA.

9.10.3 Effect of Termination and Survival

Upon termination of this CP, all CAs are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates. The following sections of this CP shall survive any termination or expiration of this CP: 2.1.1, 2.2, 5.4, 5.5, 6.2-6.4, 6.8, 9.2-9.4, 9.7-9.10, 9.13-9.16.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, all parties shall use commercially reasonable methods to communicate, taking into account the criticality and subject matter of the communication.

Any planned change to the infrastructure that has the potential to affect the FPKI operational environment shall be communicated to the FPKIPA at least two weeks prior to implementation, and all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

9.12 Amendments

9.12.1 Procedure for Amendment

The Exostar PMA shall review the CP and CPS at least once every year. Additional reviews may be enacted at any time at the discretion of the Exostar PMA.

If the Exostar PMA wishes to recommend amendments or corrections to the CP or CPS, such modifications shall be circulated to appropriate parties identified by the Exostar PMA. Comments from such parties will be collected by the Exostar PMA in a fashion prescribed by the Exostar PMA.

If the Exostar PMA believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of Exostar, Exostar shall be entitled to make amendments effective immediately upon publication in the Repository.

9.12.2 Notification Mechanism and Period

The most up to date copy of the CP can be found at
https://www.myexostar.com/?ht_kb=policy-and-compliance

This CP and any subsequent changes shall be made publicly available within seven days of approval.

9.12.3 Circumstances under Which OID Must be Changed

Certificate Policy OIDs shall be changed if the Exostar PMA determines that a change in the CP reduces the level of assurance provided.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among Exostar and Customers

Provisions for resolving disputes between Exostar and its Customers shall be set forth in the applicable agreements between the parties.

9.13.2 Alternate Dispute Resolution Provisions

Except as otherwise agreed (e.g., under an agreement under Section 9.13.1 above), any dispute under this CP shall be resolved by binding arbitration in accordance with the commercial rules (or international rules, if the other party to the dispute is a non-US entity) of the American Arbitration Association then in effect. The arbitration panel shall consist of one (1) neutral arbitrator if the amount in controversy is less than $10,000, otherwise the panel shall consist of three (3) neutral arbitrators, each an attorney with five (5) or more years of experience in computer and technology law and/or the primary area of law as to which the dispute relates. The arbitrator(s) shall have never been employed (either as an employee or as an independent consultant) by either of the Parties, or any parent, subsidiary or affiliate thereof. The Parties shall have the right to take discovery of the other Party by any or all methods provided in the Federal Rules of Civil Procedure. The arbitrator(s) may upon request exclude from being used in the arbitration proceeding any evidence not made available to the other Party pursuant to a proper discovery request. The arbitrator(s) shall apply federal law of the United States and/or the law of the State of New York, and the arbitration proceeding shall be held in New York City, New York, USA or in such other location as is mutually agreed upon. The cost of the arbitration shall be borne equally by the Parties, unless the arbitrator(s) awards costs and attorneys fees to the prevailing Party. Notwithstanding the choice of law provision in this Agreement, the Federal Arbitration Act, except as modified herein, shall govern the interpretation and enforcement of this provision. All arbitration proceedings shall be conducted in English. Any claim, dispute and controversy shall be arbitrated on an individual basis and not aggregated with the claims of any third party class action arbitration is prohibited. The arbitrator(s) shall have no discretion to award punitive damages._Notwithstanding the foregoing dispute resolution procedures, either Party may apply to any court having jurisdiction to (i) enforce the agreement to arbitrate, (ii) seek provisional injunctive relief so as to maintain the status quo until the arbitration award is rendered or the dispute in otherwise resolved, or to otherwise prevent irreparable harm, (iii) avoid the expiration of any applicable limitation period, (iv) preserve a superior position with respect to creditors, or (v) challenge or vacate any final decision or award of the arbitration panel that does not comport with the express provisions of CP.

9.14 Governing Law

Subject to any limits appearing in applicable law, the federal laws of the United States and/or the laws State of New York, shall govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in the State of New York. This choice of law is made to ensure uniform procedures and interpretation for all Exostar Customers no matter where they are located.

This governing law provision applies only to this CP. Agreements incorporating the CP by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the terms of such other agreements, subject to any limitations appearing in applicable law.

9.15 Compliance with Applicable Law

This CP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No Stipulation

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the other party (such consent not to be unreasonably withheld), except that Exostar may assign and delegate this CP to any party of its choosing.

9.16.3 Severability

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

9.16.4 Waiver of Rights

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

9.16.5 Force Majeure

Exostar shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action. EXOSTAR HAS NO LIABILITY FOR ANY DELAYS, NON-DELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD PARTY ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO EXOSTAR.

9.17 Other Provisions

No stipulation.

10 CERTIFICATE, CRL, AND OCSP FORMATS

This section contains the formats for the various PKI objects such as certificates, CRLs, and OCSP requests and responses. The section only contains certificate profiles based on RSA. For algorithm identifiers, parameter encoding, public key encoding, and signature encoding for ECDSA and ECDH, RFC3279 shall be used.

Certificates and CRLs issued under a policy OID of this CP shall not contain any critical extensions not listed in the profiles in this section. Certificates and CRLs issued under a policy OID of this CP may contain non-critical extensions not listed in the profiles in this section only upon Exostar PMA approval.

First entries in the caIssuers field of the AIA extension and CRL DP shall point to a resource that is publicly available using HTTP. If LDAP pointers are used, they shall appear only after the HTTP pointers.

For attribute values other than dc and e-mail address[8]: All CA Distinguished Names (in various fields such as Issuer, Subject, Subject Alternative Name, Name constraints, etc.) shall be encoded as printable string. All subscriber DN portions that name constraints apply to, shall be encoded as printable string. Other portions of the subscriber DN shall be encoded as printable string if possible. If a portion cannot be encoded as printable string, then and only then shall it be encoded using a different format and that format shall be UTF8.

For dc and e-mail address attribute values: All dc attribute values shall be encoded as IA5 string.

CAs may issue partitioned CRL as long as the CRLs are not indirect CRL, are not partitioned by reason code, and CRL DP and Issuing Distribution Point do not assert name relative to issuer. If Exostar provides OCSP services for a CA, that CA must also issue a full and complete CRL (i.e., a CRL without Issuing Distribution Point extension) for the use by the OCSP Responder.

[8] Note that Exostar does not recommend using e-mail address in a DN.

10.1 FISRCA → Cross-Certified CA Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	cn=Exostar Federated Identity Service Root CA {1…n}, ou=Certification Authorities, o=Exostar LLC, c=us
Validity Period	Expressed in UTCTime for dates until 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PKCS-10 request from the FISRCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the PCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature (optional) , nonrepudiation (optional)
Certificate Policies	c=no; all or a subset of the following, using Exostar SHA-2 OIDs as appropriate to the FISRCA instance and CA infrastructure: {id-basic}, {id-mediumSoftware}, {id-mediumHardware}
Policy Mapping	c=no; all or a subset of the following, using Exostar SHA-2 OIDs as appropriate to the FISRCA instance and CA infrastructure: [{id-basic} {PCA's CP id-rudimentary}], [{id-mediumSoftware} {PCA's CP id-mediumSoftware}], [{id-mediumHardware} {PCA's CP id-mediumHardware}],
Basic Constraints	c=yes; cA=True; path length constraint optional[9]
Name Constraints	c=yes; optional: Name forms as determined by the Exostar PMA
Policy Constraints	c=no; (optional) as specified in Section 7.1.7 of this CP
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA or details of the CA that is cross certified; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder (present if OCSP is supported by the Issuing CA);
CRL Distribution Points[10]	c=no;

[9] Path length constraint should be present where possible.

[10] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://…) and/or HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer)

Field	Value
Inhibit anyPolicy	c=no; (optional) as specified in Section 7.1.10 of this CP

10.2 Cross-Certified CA → FISRCA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	Expressed in UTCTime for dates until 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	cn=Exostar Federated Identity Service Root CA {1…n}, ou=Certification Authorities, o=Exostar LLC, c=us
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request to the FISRCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the FISRCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature (optional), nonrepudiation (optional)
Certificate Policies	c=no; all or a subset of the following, using Exostar ~~SHA-1 or~~ SHA-2 OIDs as appropriate to the FISRCA instance and CA infrastructure: {CA's CP id-basic}, {CA's CP id-mediumSoftware}, {CA's CP id-mediumHardware}
Policy Mapping	c=no; all or a subset of the following, using Exostar ~~SHA-1 or~~ SHA-2 OIDs as appropriate to the FISRCA instance and CA infrastructure: [{PCA's CP id-rudimentary} {id-basic}], [{PCA's CP id-mediumSoftware} {id-mediumSoftware }], [{PCA's CP id-mediumHardware} {id-mediumHardware}]
Basic Constraints	c=yes; cA=True; path length = 1
Name Constraints	c=yes; optional: Name forms as determined by the Issuing CA
Policy Constraints	c=no; (optional) as specified in Section 7.1.7 of this CP
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing certificates issued to the PCA or LDAP URL pointer to the caCertificate attribute of the PCA PKI Repository entry; id-ad-ocsp access method entry contains HTTP URL for the PCA OCSP Responder (present if OCSP is supported by the Issuing CA)
CRL Distribution Points[11]	c = no;

[11] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://…) and/or HTTP (i.e., of the form

Field	Value
Inhibit anyPolicy	c=no; (optional) as specified in Section 7.1.10 of this CP

10.3 FISRCA (also called Trust Anchor)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	cn=Exostar Federated Identity Service Root CA {1…n}, ou=Certification Authorities, o=Exostar LLC, c=us
Validity Period	Up to 12/31/2030 for 2048 bit RSA, not to exceed 20 year validity; expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	cn=Exostar Federated Identity Service Root CA {1…n}, ou=Certification Authorities, o=Exostar LLC, c=us
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; keyCertSign, cRLSign, offlineCRLSigning, DigitalSignature, nonRepudiation
Basic Constraints	c=yes; cA=True; path length constraint absent

http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.4 Signing CA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	Up to 12/31/2030 for 2048 bit RSA, not to exceed 20 year validity; expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 Subject CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subject CA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation, (offline CRL sign (optional))
Certificate Policies	c=no; all or a subset of the following, using Exostar ~~SHA-1 or~~ SHA-2 OIDs as appropriate to the Signing CA instance and CA infrastructure: {id-basic}, {id-mediumSoftware}, {id-mediumHardware}, {id-QCP-Public}, {id-QCP-Public+SSCD}
Basic Constraints	c=yes; cA=True; path length=0
Policy Constraints	c=no; (optional) as specified in Section 7.1.7 of this CP
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA or details of the CA that is cross certified; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder (present if OCSP is supported by the Issuing CA);
CRL Distribution Points[12]	c = no;
inhibitAnyPolicy	c=no; (optional) as specified in Section 7.1.10 of this CP

[12] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://…) and/or HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.5 FIS Subscriber Identity Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue; expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 5280 method 1 or other method)
Key Usage	c=yes; digitalSignature (always present), nonRepudiation (optional)

Extended Key Usage	c=no;
	After June 30, 2012: id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}; and id-pkinit-KPClientAuth {1 3 6 1 5 2 3 4}
	Please Note: smartCard Logon and id-pkinit-KPClientAuth in id-mediumHardware only

Certificate Policies	c=no; a subset of the following, within parameters described in Section 1.2 and using Exostar SHA-2 OIDs as appropriate to the Signing CA instance and CA infrastructure: {id-basic}, {id-mediumSoftware}, {id-mediumHardware}
Subject Alternative Name	c=no; optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA or details of the CA that is cross certified; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder (present if OCSP is supported by the Issuing CA);
CRL Distribution Points[13]	c = no;

[13] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://…) and/or HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.6 FIS Subscriber Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue; expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature, nonRepudiation

Extended Key Usage	c-no;
	After June 30, 2012: id-kp-emailProtection {{1.3.6.1.5.5.7.3.4}; Microsoft Document Signing {1.3.6.1.4.1.311.10.3.12}; and Adobe Certified Document Signing {1.2.840.113583.1.1.5}

Certificate Policies	c=no; a subset of the following, within parameters described in Section 1.2 and using Exostar SHA-2 OIDs as appropriate to the Signing CA instance and CA infrastructure: {id-basic}, {id-mediumSoftware}, {id-mediumHardware}
Subject Alternative Name	c=no; RFC822 email address (required); others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA or details of the CA that is cross certified; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder (present if OCSP is supported by the Issuing CA);
CRL Distribution Points[14]	c = no;

10.7 FIS Subscriber Encryption Certificate

Field	Value
Version	V3 (2)

[14] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://…) and/or HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

Field	**Value**
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue; expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption
Issuer's Signature	sha256WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment (required), dataEncipherment (optional)
Extended Key Usage	**c=no;** id-kp-emailProtection {1.3.6.1.5.5.7.3.4}; Encrypting File System {1.3.6.1.4.1.311.10.3.4}
Certificate Policies[15]	c=no; a subset of the following, within parameters described in Section 1.2 and using Exostar SHA-2 OIDs as appropriate to the Signing CA instance and CA infrastructure: {id-basic}, {id-mediumSoftware}, {id-mediumHardware}
Subject Alternative Name	c=no; RFC822 email address (required); others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA or details of the CA that is cross certified; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder (present if OCSP is supported by the Issuing CA)
CRL Distribution Points[16]	c = no;

[15] Only software OID asserted to support key recovery to software tokens

[16] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://…) and/or HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.8 FIS Code Signing Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue; expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; nonRepudiation, digitalSignature

Extended key usage	c=yes; { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-kp(3) id-kp-codesigning (3) };
	Lifetime Signing {1.3.6.1.4.1.311.10.3.13}

Certificate Policies[17]	c=no; a subset of the following, within parameters described in Section 1.2 and using Exostar SHA-2 OIDs as appropriate to the Signing CA instance and CA infrastructure: {id-basic}, {id-mediumSoftware}, {id-mediumHardware}
Subject Alternative Name	DN of the person controlling the code signing private key
CRL Distribution Points[18]	c = no;
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA or details of the CA that is cross certified; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder (present if OCSP is supported by the Issuing CA)

[17] As Code Signing certificates require FIPS 140-1/2 Level 2 or higher, a hardware OID will be present in certificates issued under this profile.

[18] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://…) and/or HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.9 FIS Device or Server Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue; expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment, digitalSignature
Extended key usage	c=no; at least one EKU OID is present: serverAuthentication (optional), clientAuthentication (optional), anyExtendedKeyUsage is not permitted
Certificate Policies	c=no; a subset of the following, within parameters described in Section 1.2 and using Exostar SHA-2 OIDs as appropriate to the Signing CA instance and CA infrastructure: **After October 1, 2016:** {id-mediumSoftware-device-sha2}, {id-mediumHardware-device-sha2}
Subject Alternative Name	c=no; always present, Host URL | IP Address | Host Name
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA or details of the CA that is cross certified; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder (present if OCSP is supported by the Issuing CA)
CRL Distribution Points[19]	c = no; always present

[19] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://…) and/or HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.10 OCSP Responder Certificate

The following table contains the OCSP Responder certificate profile assuming that the OCSP Responder certificate is issued by the same CA using the same key as the Subscriber Certificate. Alternative trust models such as OCSP Responder as trust anchor may be acceptable to the Exostar PMA.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than one month from date of issue; expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 OCSP Responder (subject) DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Certificate Policies[20]	c=no, all or a subset of the following, using Exostar ~~SHA-1 or~~ SHA-2 OIDs as appropriate to the Signing CA instance and CA infrastructure; {id-basic}, {id-mediumSoftware}, {id-mediumHardware} If required by a particular PKI bridge, Policy Qualifier shall be present and express a userNotice conforming to the following format, where [Entity] represents a PKI that is cross-certified with Exostar and such notice is contractually required: userNotice = "OCSP RESPONSE SUBJECT TO LIMITED LIABILITY/for [Entity] use see [Entity] CP at [Entity URL]; other use see Exostar CP at [Exostar URL]/CPs incorporated by reference."
Subject Alternative Name	HTTP URL for the OCSP Responder
No Check id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}	c=no; Null

[20] Technically the Responder certificate need not have a CP OID in it; but, not everyone and every product gets the Gestalt behind PKI. Thus, we include this extension to help product interoperability.

Field	Value
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA

10.11 FIS Role Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue; expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN for role as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=no; id-kp-emailProtection {{1.3.6.1.5.5.7.3.4}; Microsoft Document Signing {1.3.6.1.4.1.311.10.3.12}; and Adobe Certified Document Signing {1.2.840.113583.1.1.5}
Certificate Policies	c=no; a subset of the following, within parameters described in Section 1.2 and using Exostar SHA-2 OIDs as appropriate to the Signing CA instance and CA infrastructure: {id-basic}, {id-mediumSoftware}, {id-mediumHardware}
Subject Alternative Name	c = no; DN of the person controlling the role signing private key; RFC822 email address of role
CRL Distribution Points[21]	c = no;

[21] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://…) and/or HTTP (i.e., of the form http://…) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

Field	Value
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA or details of the CA that is cross certified; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder (present if OCSP is supported by the Issuing CA)

10.12 CRL Format

10.13.1 Full and Complete CRL

If the PKI provides OCSP Responder Services, the PKI shall make a full and complete CRL available to the OCSP Responders as specified below. This CRL may also be provided to the relying parties.

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
thisUpdate	expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
nextUpdate	expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter (>= thisUpdate + CRL issuance frequency)
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter)
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
CRL Extension	**Value**
CRL Number	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA)
CRL Entry Extension	**Value**
Reason Code	c=no; optional, must be included when reason code = key compromise or CA compromise
Hold Instruction	c=no; optional, id-holdinstruction-reject[22]

10.13.2 Distribution Point Based Partitioned CRL

Exostar may make distribution based partitioned CRL available to the relying parties in lieu of or in addition to the full and complete CRL. The distribution point based partition CRL shall adhere to the following profile. Note that the CRL may not be an indirect CRL,

[22] may be present only if reason code = certificateHold

may not partitioned based on reason codes, and may not assert a distribution point that is a nameRelativetoCRLIssuer.

Field	**Value**
Version	V2 (1)
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
thisUpdate	expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
nextUpdate	expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter (>= thisUpdate + CRL issuance frequency)
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter)
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
CRL Extension	**Value**
CRL Number	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA)
Issuing Distribution Point	c=yes; distribution point field must contain a full name (i.e., distribution point field may not contain nameRelativetoCRLIssuer; the following fields must all be absent: onlySomeReasons, indirectCRL, and onlyContainsAttributeCerts
CRL Entry Extension	**Value**
Reason Code	c=no; optional, must be included when reason code = key compromise or CA compromise
Hold Instruction	c=no; optional, id-holdinstruction-reject[23]

[23] may be present only if reason code = certificateHold

10.13 OCSP Request Format

Requests sent to Issuer PKI OCSP Responders are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC2560 for detailed syntax. The following table lists the fields that are expected by the OCSP Responder.

Field	**Value**
Version	V1 (0)
Requester Name	DN of the requestor (required)
Request List	List of certificates as specified in RFC 2560
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

10.14 PKCS 10 Request Format

The following table contains the format for PKCS 10 requests.

Field	**Value**
Version	V1 (0)
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Subject's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension (encoded in extension request attribute)	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; optional; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Basic Constraints	c=yes; optional; cA=True; path length constraint (absent or 1 as appropriate)

11 PKI REPOSITORY INTEROPERABILITY PROFILE

This section provides an overview of the PKI Repository interoperability profiles. The following topics are discussed:

- Protocol
- Authentication
- Naming
- Object Class
- Attributes

Each of these items is described below.

11.1 Protocol

Each Enterprise shall implement a PKI Repository that provides either LDAP or HTTP protocol access to CA certificates and CRLs.

11.2 Authentication

Each PKI Repository shall permit “none” authentication to read CA certificate and CRL information.

Each Enterprise shall be free to implement authentication mechanisms of its choice for browse and list operations.

Any write, update, add entry, delete entry, add attribute, delete attribute, change schema etc., shall require password over SSL or stronger authentication mechanism.

11.3 Naming

This CP has defined the naming convention. Certificates shall be stored in the PKI Repository in the entry that appears in the certificate subject name. issuedByThisCA element of CrossCertificatePair shall contain the certificate(s) issued by a CA whose name the entry represents.

CRLs shall be stored in the PKI Repository in the entry that appears in the CRL issuer name.

11.4 Object Class

Entries that describe CAs shall be defined by organizationUnit structural object class. These entries shall also be a member of pkiCA cpCPS auxiliary object classes.

Entries that describe individuals (human entities) shall be defined by the inetOrgPerson class, which inherits from other classes: person, and organizationalPerson. These entries shall also be a member of pkiUser auxiliary object class.

11.5 Attributes

CA entries shall be populated with the caCertificate, crossCertificatePair, certificateRevocationList, cPCPS attributes, as applicable.

User entries shall be populated with userCertificate attribute containing encryption certificate. Signature certificate need not be published to the PKI Repository.

BIBLIOGRAPHY

The following documents were used in part to develop this CP:

1999/93/EC Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

ABADSG Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html.

ANSI X9.62 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005-03-11

ANSI X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography, 2001-11-20

CHARTER Exostar PMA Charter

ETSI TS 101 456 Electronic Signatures and Information (ESI); Policy Requirements for certification authorities issuing qualified certificates (2007-05)

ETSI TS 101 862 Qualified Certificate profile (2006-01)

FIPS 140-2 Security Requirements for Cryptographic Modules, 1994-01 http://csrc.nist.gov/cryptval/

FIPS 186-4 Digital Signature Standard, July 2013 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

PKCS #12 Personal Information Exchange Syntax Standard, April 1997. Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html

RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 2527 Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999.

RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

RFC 3647 Certificate Policy and Certificate Practices Framework, Chokhani, Ford, Sabett, Merrill, and Wu. November 2003.

RFC 3739 Qualified Certificates Profile, Santesson, Nystrom, and Polk. March 2004.

12 ACRONYMS & ABBREVIATIONS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
C	Country
CA	Certification Authority
FISRCA	Federated Identity Service Root Certification Authority
CBP	Commercial Best Practices
CIMC	Certificate Issuing and Management Components
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DC	Domain Component
DMV	Department of Motor Vehicles
DN	Distinguished Name
DNS	Domain Name Service
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EE	End Entity
ETSI	European Telecommunications Standards Institute
FBCA	Federal Bridge Certification Authority
FIPS	(US) Federal Information Processing Standard

FIPS PUB	(US) Federal Information Processing Standard Publication
FSO	Facility Security Officer
HR	Human Resources
HTTP	Hypertext Transfer Protocol
IAO	Information Assurance Officer
ID	Identifier
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
JPAS	Joint Personnel Adjudication System
LDAP	Lightweight Directory Access Protocol
MOA	Memorandum of Agreement (as used in the context of this CP, between an Entity and the Exostar allowing interoperation between the Exostar CA). Exostar consults Exostar PMA through the Exostar PMA Chair on the MOA
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
O	Organization
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PCA	Principal Certification Authority
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
RA	Registration Authority

RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SCVP	Simple Certificate Validation Protocol
SHA-1	Secure Hash Algorithm, Version 1
SSL	Secure Sockets Layer
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TS	Technical Specification
UPS	Uninterrupted Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VME	Virtual Machine Environment

13 GLOSSARY

Access	Ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Entity	An organization with operational control of a CA that will interoperate with an Exostar CA.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term

“Certificate” refers to certificates that expressly reference the OID of this CP in the “Certificate Policies” field of an X.509 v.3 certificate.

Certification Authority (CA)

An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.

CA Facility

The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certificate

A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it’s Subscriber, (3) contains the Subscriber’s public key, (4) identifies it’s operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]

Certificate Management Authority (CMA)

A Certification Authority or a Registration Authority.

Certification Authority Software

Key Management and cryptographic software used to manage certificates issued to subscribers.

Certificate Policy (CP)

A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practice Statement (CPS)

A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

Certificate-Related Information

Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.

Certificate Revocation List (CRL)

A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.

Certificate Status Authority

A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.

Client (application)

A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.

Common Criteria

A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Compromise

Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Computer Security Objects Registry (CSOR)

Computer Security Objects Registry operated by the National Institute of Standards and Technology.

Confidentiality

Assurance that information is not disclosed to unauthorized entities or processes.

Cross-Certificate

A certificate used to establish a trust relationship between two Certification Authorities.

Cryptographic Module

The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1402]

Customer

Any commercial organization that is a paying member of Exostar.

Cryptoperiod

Time span during which each key setting remains in effect.

Data Integrity

Assurance that the data are unchanged from creation to reception.

Digital Signature

The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.

Dual Use Certificate

A certificate that is intended for use with both digital signature and data encryption services.

Duration

A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue".

E-commerce

The use of network technology (especially the internet) to buy or sell goods and services.

Employee

Any person employed by an Entity as defined above.

Encryption Certificate

A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

End Entity

Relying Parties and Subscribers.

Exostar Operational Authority (Exostar OA)

The Exostar Operational Authority is the organization selected by the Exostar PMA (Exostar PMA) to be responsible for operating the FISRCA.

Exostar Root Certification Authority (FISRCA)

The Exostar Root Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, PKI Repositories, Certificate Policies and Certificate Practice

Statements) that are used to issue certificates to Entity Principal Certification Authorities.

Exostar PMA (Exostar PMA)
The Exostar PMA (Exostar PMA) is a body responsible for setting, implementing, and administering policy decisions regarding PKI interoperability that uses the Exostar.

Firewall
Gateway that limits access between networks in accordance with local security policy.

Hypervisor
Computer software, firmware or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or virtual machine monitor.

Inside threat
An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Integrity
Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Intellectual Property
Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Intermediate CA
A CA that is subordinate to another CA, and has a CA subordinate to itself.

Key Escrow
A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]

Key Exchange
The process of exchanging public keys in order to establish secure communications.

Key Generation Material
Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

Key Pair
Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Local Registration Authority (LRA)
A Registration Authority with responsibility for a local community.

Memorandum of Agreement (MOA)
Agreement between the Exostar PMA and an Entity allowing interoperability between the Entity Principal CA and the Exostar CAs.

Mission Support Information
Information that is important to the support of deployed and contingency forces.

Mutual Authentication
Occurs when parties at both ends of a communication activity authenticate each other (see authentication).

Naming Authority
An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.

Non-Repudiation
Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Object Identifier (OID)
A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.

Out-of-Band
Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).

Outside Threat
An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.

Physically Isolated Network
A network that is not connected to entities or systems outside a physically controlled space.

PKI Repository
See Repository

PKI Sponsor
Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.

Policy Management Authority (PMA)
Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.

Principal CA
The Principal CA is a CA designated by an Entity to interoperate with the Exostar CAs. An Entity may designate multiple Principal CAs to interoperate with the Exostar CAs.

Privacy
Restricting access to subscriber or Relying Party information in accordance with Federal law and Entity policy.

Private Key
(1) The key of a signature key pair used to create a digital signature.

(2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key

(1) The key of a signature key pair used to validate a digital signature.

(2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.

Public Key Infrastructure (PKI)

A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA)

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate)

To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party

A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Renew (a certificate)

The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository

A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory. In this CP, Repository refers to PKI Repository.

Responsible Individual

A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate

To prematurely end the operational period of a certificate effective at a specific date and time.

Risk

An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Risk Tolerance

The level of risk an entity is willing to assume in order to achieve a potential desired result.

Root CA

In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Server

A system entity that provides a service in response to requests from clients.

Signature Certificate

A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subordinate CA

In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).

Subscriber

A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device

Superior CA

In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).

System Equipment Configuration

A comprehensive accounting of all system hardware and software types and settings.

Technical non-repudiation

The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.

Threat

Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Trust List

Collection of trusted certificates used by Relying Parties to authenticate other certificates.

Trusted Agent

Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.

Trusted Certificate

A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

Trusted Timestamp

A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

Trustworthy System

Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

Two-Person Control

Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.

Update (a certificate)

The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.

Update (in reference to significant change)

Alterations to Licensed Software, including code and/or error corrections and minor code enhancements or modifications, that may be developed and generally released from time to time by the Software Vendor and made available to the customer (licensee). Software Updates do not include: (i) Software Upgrades of the Licensed Software that may be developed and generally released from time to time by the software vendor

Upgrade (in reference to significant change)

Enhancements to the Licensed Software providing a new program feature or function that may be developed and generally released from time to time by the software vendor and made available to customer (licensee). Software Upgrades do not include: (i) Software Updates of the Licensed Software that may be developed and generally released from time to time by the software updates

Virtual Machine Environment

An emulation of a computer system (in this case a CA) that provides the functionality of a physical machine in a platform-independent environment. It consists of a host (virtual machine) and isolation kernel (hypervisor) and provides functionality needed to execute entire operating systems. At this time, allowed VMEs are limited to Hypervisor type virtual environments. Other technology, such as Docker Cotainers, is not permitted.

Zeroize

A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1402]