X.509 Certificate Policy

For The

E-Governance Certification Authorities

Version 2.0

September 9, 2011

Signature Page

DEBORAH GALLAGHER

Digitally signed by DEBORAH GALLAGHER
DN: c=US, o=U.S. Government, ou=General Services Administration, cn=DEBORAH GALLAGHER, 0.9.2342.19200300.100.1.1=47001001545490
Date: 2011.10.27 11:50:29 -04'00'

October 27, 2011

Chair, Federal Public Key Infrastructure Policy Authority — DATE

Revision History

Document Version	Document Date	Revision Details
		Text changes are specified in the following EGCA CP Change Proposals (**change proposal number**, title, date):
Release Candidate 2.0	9 September 2011	This E-Governance CA CP updates and replaces Version 1.5, dated 16 August 2010. This version of the EGCA CP reflects a major overhaul of the CP that 1) converted the format from RFC 2527 to RFC 3647, 2) included modifications to support the EGTS and 3) included modifications to align with the Common and FBCA CPs where appropriate (e.g., physical and environmental security requirements).
1.5	16 August 2010	This E-Governance CA CP updates and replaces Version 1.4, dated 16 August 2007. **2010-01,** Bring into alignment with recent operational changes to the FBCA CP, 5 August 2010
1.4	16 August 2007	This E-Governance CA CP updates and replaces Version 1.3, dated 9 November 2005. **2007-01**, Alignment of Cryptographic Algorithm Requirements with SP 800-78-1, 17 July 2007

1.3	9 November 2005	This E-Governance CA CP updates and replaces Version 1.2, dated 3 October 2005. **2005-03**, Modify the E-Governance CA CP to permit additional attributes to appear in subscriber distinguished names, 22 September 2005
1.2	3 October 2005	This E-Governance CA CP updates and replaces Version 1.1, dated 13 September 2005. **2005-02**, Modify the E-Governance CA CP to permit centrally generated key pairs for agency application servers, 20 September 2005
1.1	13 September 2005	This E-Governance CA CP updates and replaces Version 1.0, dated 29 September 2004. **2005-01**, Change in Certificate Profile specified for Self-Signed Certificates, 22 June 2005
1.0	29 September 2004	This E-Governance CA CP updates and replaces Version 0.9, dated 23 July 2004. **2004-01**, Change in responsible party for certificate dispute resolution, 29 September 2004 **2004-02**, Deletion of Standard Operating Procedure (SOP) references, 29 September 2004

Table of Contents

1. INTRODUCTION

In September 2004, three E-Governance Certification Authorities (EGCA) were established to support the government-wide E-Authentication Federation.

In September 2008, the Identity, Credential, and Access Management Subcommittee (ICAMSC) was established under the Federal CIO Council's Information Security & Identity Management Committee. The ICAMSC is tasked with aligning the identity management activities of the Federal Government, which includes the former E-Authentication Program and its supporting EGCA.

Identity Credential and Access Management's (ICAM) open approach creates many new uses for the EGCA that are not addressed by the original EGCA design and corresponding EGCA Certificate Policy (CP). Examples of new uses include, but are not limited to:

1. Providing an infrastructure for Backend Attribute Exchange (BAE); and
2. Facilitating trusted metadata (e.g., signing of metadata by IdPs, Trust Framework Providers, and Relying Parties).

The Legacy E-Authentication Federation and the new uses described above are collectively known as the E-Governance Trust Services (EGTS) and facilitate the use of federated identity in a trusted manner throughout the Federal Government, and between the Federal Government and its partners (i.e., other governments, citizens, businesses, and other entities).

This document defines a suite of policies that apply to the management of the E-Governance Certification Authorities in support of the EGTS.

Two specific certificate policies support the Legacy E-Authentication Federation and are designed to recognize Credential Service Providers (CSPs) that have been certified as meeting E-Authentication assurance requirements at Level 2[1], as defined in [M-04-04], and agency application servers participating in the E-Authentication program (http://www.cio.gov/eauthentication/). In these policies, certificates either:

- Identify a Level 2 CSP (as a network device) named in the certificate and binds that CSP to a particular public/private key pair, or
- Identify a federal agency server (a network device) supporting one or more E-Authentication applications, and binds that server to a particular public/private key pair.

[1] Version 2.0 of the EGCA removed references to the Level 1 CSP because the Level 1 CSP was not in use and therefore decommissioned in the second quarter of FY-2011.

Eight policies support new services defined under the EGTS:

- Four certificate policies support Level 1-4 Identity Providers (IdPs) aligned with the four discussed in National Institute of Standards and Technology (NIST) Special Publication 800-63 [SP 800-63]. IdPs are a new version of a CSP previously defined in the Legacy E-Authentication Federation
- One policy supports Backend Attribute Exchange (BAE). BAE is a standard mechanism for Relying Parties (RPs) to obtain Attributes directly from an authoritative source or Attribute Authority (AA).
- One policy supports RPs that exchange information with IdPs and BAE Brokers. RPs are a new version of an Agency Application previously defined in the Legacy E-Authentication Federation
- Two policies support MetaData Signers. Digitally signed metadata is used to convey trust between ICAM and its members, including individual agencies, ICAM-approved Trust Framework Providers (TFPs) and other Federations.

Unless otherwise noted, stipulations in this document (henceforth referred to as "this CP") apply to all policies. As specified in this CP, the E-Governance CAs (EGCAs) will provide the following security management services:

- CA key generation/storage;
- Certificate generation, update, renewal, rekey, and distribution;
- Certificate revocation list (CRL) generation and distribution;
- Directory management of certificate related items; and
- System management functions (e.g., security audit, configuration management, archive).

This policy requires use of FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys by both the E-Governance CAs and their subscribers.

Under this policy, the E-Governance CAs will not issue certificates to other CAs. Self-issued certificates to manage transitions (e.g., to new CA key pairs) are permitted. Only the E- Governance CAs are permitted to assert these policies in certificates.

This policy also establishes requirements for the secure distribution of the E-Governance CAs' self-signed certificates. This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) request for comments (RFC) 3647, CP and Certification Practice Statement Framework.

1.1 OVERVIEW

Certificates issued under this policy contain a 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.

This CP states what assurance can be placed in a certificate issued by the EGCA. The Certificate Practice Statement (CPS) states how the EGCA establishes that assurance. The EGCA shall have a corresponding CPS.

This CP applies to certificates issued by E-Governance CAs to CSPs, agency application servers, Level 1-4 IdPs, Relying Parties, BAE Brokers, and MetaData Signers.

1.1.1 Certificate Policy (CP)

Certificates issued under this policy contain a 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.

1.1.2 Relationship between the EGCA CP & the EGCA CPS

This CP states what assurance can be placed in a certificate issued by the EGCA. The certification practice statement (CPS) states how the EGCA establishes that assurance.

1.1.3 Scope

This CP applies to certificates issued to devices that are represented by human sponsors. This CP does not apply to certificates issued to human subscribers.

1.2 DOCUMENT IDENTIFICATION

This CP provides substantial assurance concerning identity of certificate subjects. Certificates issued in accordance with this CP shall assert at least one of the following OIDs in the certificate policy extension:

Table 1 - id-fpki-eGov Policy OIDs

id-eGov-Level2	::= {2 16 840 1 101 3 2 1 3 10}
id-eGov-Applications	::= {2 16 840 1 101 3 2 1 3 11}
id-eGov-Level1-IdP	::= {2.16.840.1.101.3.2.1.3.28}
id-eGov-Level2-IdP	::= {2.16.840.1.101.3.2.1.3.29}
id-eGov-Level3-IdP	::= {2.16.840.1.101.3.2.1.3.30}
id-eGov-Level4-IdP	::= {2.16.840.1.101.3.2.1.3.31}
id-eGov-BAE-Broker	::= {2.16.840.1.101.3.2.1.3.32}
id-eGov-RelyingParty	::= {2.16.840.1.101.3.2.1.3.33}
id-eGov-MetaSigner	::= {2.16.840.1.101.3.2.1.3.34}
id-eGov-MetaSigner-Hardware	::= {2.16.840.1.101.3.2.1.3.35}

Certificates issued to CSPs under this policy shall contain the id-eGov-Level2 OID.

Certificates issued to agency application servers under this policy shall contain the id-eGov-Applications OID.

The EGCAs issue certificates to Level 1 IdPs under the EGCA CP that contain the id-eGov-Level1-IdP OID.

The EGCAs issue certificates to Level 2 IdPs under the EGCA CP that contain the id-eGov-Level2-IdP OID.

The EGCAs issue certificates to Level 3 IdPs under the EGCA CP that contain the id-eGov-Level3-IdP OID.

The EGCAs issue certificates to Level 4 IdPs under the EGCA CP that contain the id-eGov-Level4-IdP OID.

The EGCAs issue certificates to BAE Brokers under the EGCA CP that contain the id-eGov-BAE-Broker OID.

The EGCAs issue certificates to Relying Parties under the EGCA CP that contain the id-eGov-RelyingParty OID.

The EGCAs issue certificates to Metadata Signers under the EGCA CP that contain either the id-eGov-MetaSigner or id-eGov-MetaSigner-Hardware OIDs.

Certificates issued to devices shall only assert one of these certificate policy OIDs.

1.3 PKI ENTITIES

Certificates issued under this policy support distribution of authentication information to Federal Government relying parties, exchange of authentication information between IdPs and RPs, exchange of attribute information, and exchange of MetaData.

1.3.1 PKI Authorities

1.3.1.1 Federal PKI Policy Authority (FPKIPA)

The Federal PKI Policy Authority (FPKIPA) is comprised of U.S. Federal Government Agencies (including cabinet-level Departments) participating in the Federal PKI and was established by the Federal CIO Council.

The E-Authentication Authorizing Official (EAO) will provide the FPKIPA with status of the periodic compliance audits from the operating entity to demonstrate that the EGCAs are operating in compliance with the approved CPSs.

1.3.1.2 FPKI Management Authority (FPKIMA)

The FPKIMA is the organization that operates and maintains the EGCA on behalf of the U.S. Government, subject to the direction of the EAO.

1.3.1.3 Certification Authority (CA)

The EGCA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. The EGCA is responsible for the issuing and managing certificates including but not limited to:

- The certificate manufacturing process;
- Publication of certificates;
- Revocation of certificates;
- Generation and destruction of EGCA signing keys; and
- Ensuring that all aspects of the EGCA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.4 E-Authentication Authorizing Official

The E-Authentication Authorizing Official (EAO) is responsible for the decision to issue a certificate to particular CSPs, Agency Application servers, Level 1-4 IdPs, Relying Parties, BAE Brokers, or MetaData Signers. The EAO shall:

- Approve the CPS for each EGCA that issues certificates under this policy;
- Revise this CP to maintain operational practicality and consistency with the Medium level of assurance at the FBCA;
- Approve the compliance audit report for each EGCA issuing certificates under this policy;
- Authorize issuance of certificates to CSPs;
- Authorize issuance of certificates to Federal Agency application servers;
- Authorize issuance of certificates to IdPs;
- Authorize issuance of certificates to Relying Parties;
- Authorize issuance of certificates to BAE Brokers;
- Authorize issuance of certificates to MetaData Signers; and
- Revise this CP as needed to enable the support of additional services as required.

1.3.2 Subscribers

A subscriber is the entity whose name appears as the subject in a certificate. For this policy, subscribers are limited to devices and services, which include but are not limited to:

- CSPs;
- Agency Application Servers;
- IdPs (Levels 1-4);
- BAE Brokers;
- Relying Parties; and
- Metadata Signers (Medium and Hardware).

CSPs provide SAML assertions to agency application servers. Subscribers will use these certificates to establish mutually authenticated TLS connections to provide authentication, integrity, and confidentiality to the transmission of these SAML assertions.

1.3.3 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. For this certificate policy, the relying party may be any entity that wishes to validate the binding of a public key to CSPs, agency application servers, Level 1-4 IdPs, Relying Parties, BAE Brokers, and MetaData Signers.

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate based on the assurance provided by the process used to vet the identity of certificate sponsors (see section 3.2.3.1). The relying party decides, pursuant to its own policies, which steps to take. The EGCA merely provides the tools (i.e., certificates and CRLs) needed to validate certificates that the relying party may wish to employ.

1.3.4 Other Participants

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

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Certificates issued under these policies may be used to establish mutually authenticated TLS connections to provide authentication, integrity, and confidentiality to the transmission of SAML assertions; support the exchange of authentication information between IdPs and RPs; support exchange of attribute information; or support exchange of MetaData.

1.4.2 Prohibited Certificate Uses

Certificates are prohibited from being used for a human entity.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

The EAO is responsible for all aspects of this CP.

1.5.2 Contact Person

Questions regarding this CP shall be directed to the EAO at fpki.webmaster@gsa.gov.

1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

The EAO shall approve the CPS for each EGCA that issues certificates under this policy.

1.5.4 CPS Approval Procedures

The EAO shall make the determination that a CPS complies with this policy. The EGCA must meet all requirements of an approved CPS before commencing operations. The EAO will make this determination based on the nature of the system function, the type of communications, or the operating environment.

1.6 DEFINITIONS AND ACRONYMS

See Sections 11 and 12.

2. PUBLICATION & REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

2.1.1 Repository Obligations

All EGCAs that issue certificates under this policy are obligated to post all EGCA certificates and all CRLs in a directory that is publicly accessible through the Hypertext Transport Protocol (HTTP). EGCAs may optionally post subscriber certificates in this directory in accordance with agency policy. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent modification or deletion of information.

Posted certificates and CRLs may be replicated in additional repositories for performance enhancement. Such repositories may be operated by the EGCA or other parties (e.g., Federal agencies).

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

Certificates and CRLs shall be published as specified in Section 2. No stipulation regarding publication of additional EGCA information.

For the EGCA, mechanisms and procedures shall be designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually.

2.3 FREQUENCY OF PUBLICATION

Certificates are published following subscriber acceptance as specified in Section 4.4 and proof of possession of private key as specified in Section 3.2.1. The CRL is published as specified in Section 4.9.7. All information to be published in the repository shall be published promptly after such information becomes available to the EGCA. The EGCA shall specify in its CPS time limits within which it will publish various types of information.

This CP and any subsequent changes shall be made publicly available within 1 week of approval.

2.4 ACCESS CONTROLS ON REPOSITORIES

The EGCA shall protect information not intended for public dissemination or modification. EGCA certificates and CRLs in the repository shall be publicly available through the Internet. Access to other information in the EGCA repositories shall be determined by agencies pursuant to their authorizing and controlling statutes.

3. IDENTIFICATION & AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

Names assigned to E-Governance CAs shall be in the following form:

- C=US, o=U.S. Government, ou=FPKI, cn=*CAname*

The common name should be descriptive and must include the authentication level supported by the EGCA.

CSP subscriber names assigned by E-Governance CAs shall be in the following form:

- C=US, o=*Organization*, [ou=*major unit*], [ou=*minor unit*], cn=*CSP name*

The ou attributes are optional. The common name may be descriptive, or may be the Internet domain name of the CSP. That is, the common name may be "Acme Corporation" or "csp2.acme.com". The naming attributes identified in [RFC 5280] may also be included in CSP subscriber distinguished names.

CSP subscriber certificates shall also include the CSP's Internet domain name in the subject alternative name extension and an email address for a human point of contact.

Agency application server subscriber names assigned by the E-Governance CAs shall be in the following form:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], cn=*Agency Server name*

The organizational units department and agency appear when applicable and are used to specify the federal entity that employs the subscriber. At least one organizational unit must appear in the DN. The common name may be descriptive, or may be the Internet domain name of the server supporting the application. That is, the common name may be "Big Agency Grants Server" or "grants1.bigagency.gov". The naming attributes identified in [RFC 3280] may also be included in agency application server subscriber distinguished names.

Agency application server certificates shall also include the server's Internet domain name in the subject alternative name extension and may include an email address for a human point of contact.

For certificates issued under Level 1 IdP, Level 2 IdP, Level 3 IdP, Level 4 IdP, BAE Broker, Relying Party, Metadata Signer (Medium), Metadata Signer (Hardware) policies, the EGCA shall include X.501 distinguished names in certificates according to the distinguished name information provided in the certificate request. These distinguished names shall be a geo-political name.

Device names shall take one of the following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=*structural_container*], cn=*device name*
- C=US, o=*Organization*, [ou=*major unit*], [ou=*minor unit*], cn=*device name*

where *device name* may be descriptive or may be the Internet domain name of the device.

3.1.2 Need for Names to Be Meaningful

The subscriber 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 in a meaningful way the subscriber to which they are assigned.

3.1.3 Anonymity or Pseudonymity of Subscribers

The EGCA shall not issue anonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.5 Uniqueness of Names

The EAO is responsible for name space control procedures.

The EAO will establish name space control procedures for names assigned to subscriber CSPs, agency application servers, Level 1-4 IdPs, Relying Parties, BAE Brokers, and MetaData Signers to ensure name collisions do not occur.

This policy depends upon established name space control procedures for Internet Domain Names to avoid name collisions in the subject alternative name extension or the common name attribute.

The EAO shall resolve any name collisions brought to its attention.

3.1.6 Recognition, Authentication, & Role of Trademarks

No stipulation.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

The subscriber shall be required to prove possession of the private key that corresponds to the public key in the certificate request. This may be done by the entity using its private key to sign the public key in a certificate request. The EAO may allow other mechanisms that are at least as secure as those cited here.

3.2.2 Authentication of Organization Identity

The EAO shall comply with processes established to verify that sponsors of device certificates are affiliated with and authorized to act on behalf of the organization who submitted the request for the certificate. Information about the organization shall be verified to ensure the content of the E-Governance Certificate Issuance Authorization Letter issued by the EAO to the EGCA is accurate.

3.2.3 Authentication of Individual Identity

Computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects and shall have a human sponsor. The identity of the human sponsor shall be verified in accordance with section 3.2.3.1, Authentication of Devices.

3.2.3.1 Authentication of Devices

Computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects and shall have a human sponsor.

The identity of the sponsor shall be authenticated by:

- Verification of digitally signed messages sent from the sponsor; or
- Receipt of a signed E-Governance Certificate Issuance Authorization Letter issued by the EAO. The content of the Authorization Letter shall be verified by processes established by the EAO to verify that the sponsor is affiliated with and authorized to act on behalf of the organization who submitted the request for the certificate.

The issuing EGCA shall verify the identity information, in addition to the authenticity of the requester. The EGCA shall verify that the requester is listed as a POC on the E-Governance Certificate Issuance Authorization Letter issued by the EAO.

Requests for certificates issued under the Agency application server CSP, and Level 1 IdP policies shall include:

- Equipment identification (i.e., DNS name); and
- Equipment public keys.

For certificates issued under the Level 2 IdP, Level 3 IdP, Level 4 IdP, BAE Broker, Relying Party, Metadata Signer (Medium), Metadata Signer (Hardware) policies, the sponsor is 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); and
- Contact information to enable the EGCA to communicate with the sponsor when required.

3.2.4 Non-verified Subscriber Information

Non-verified subscriber information shall not be included in certificates.

3.2.5 Validation of Authority

No stipulation.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

The procedures for accomplishing the Certificate Renewal, Update, and Routine Re-Key specified in this CP will be detailed in the EGCA's CPS.

3.3.2 Identification and Authentication for Re-key after Revocation

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.1.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using the digital signature of the sponsor for that certificate or other authorized party for that certificate or the digital signature of the EAO.

4. CERTIFICATE LIFE-CYCLE

4.1 APPLICATION

Application for certificates shall be made to the EAO. All certificates issued by the EGCA shall be issued exclusively to non-person end entities (devices) which are represented by a human sponsor.

4.1.1 Submission of Certificate Application

An application for a device certificate shall be submitted by the human sponsor of the device.

4.1.2 Enrollment Process and Responsibilities

All communications supporting the certificate application and issuance process shall be authenticated and protected from modification. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications protect the confidentiality and integrity of the data.

Sponsors of certificates issued under EGCA certificate policies are responsible for providing accurate information on their certificate applications.

4.2 CERTIFICATE APPLICATION PROCESSING

This policy allows a certificate to be issued only to a single subscriber. Certificates shall not be issued that contain a public key whose associated private key is shared by multiple subscribers.

[Practice Note: Where multiple devices assert the same DNS name, (e.g., load balanced authentication servers), they are considered a single subscriber and may share the private key corresponding to a certificate issued under this policy.]

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in sections 3.2 and 3.3 of this CP.

4.2.2 Approval or Rejection of Certificate Applications

No stipulation.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

Upon receiving the certificate request, the EGCAs will:

- Verify the identity of the requestor;

- Verify the authority of the requestor and the integrity of the information in the certificate request;
- Build and sign a certificate if all certificate requirements have been met; and
- Make the certificate available to the subscriber.

The certificate request may already contain a certificate built by either the EGCA or the subscriber. This certificate will not be signed until all verifications and modifications, if any, have been completed to the EGCA's satisfaction.

All authorization and other attribute information received from a prospective subscriber shall be verified against the E-Governance Certificate Issuance Authorization Letter before inclusion in a certificate. The EAO is responsible for verifying prospective subscriber data before issuing the authorization letter.

4.3.2 Notification to Subscriber of Certificate Issuance

CAs operating under this policy shall inform the human sponsor of the creation of a certificate and make the certificate available to the sponsor.

4.4 CERTIFICATE ACCEPTANCE

Before a subscriber can make effective use of its private key, the EAO shall:

- Explain to the human sponsor of device certificates its responsibilities as defined in Section 9.6.3; and
- Inform the human sponsor of device certificates of the creation of a certificate and the contents of the certificate.

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

Certificates and CRLs shall be published as specified in Section 2. No stipulation regarding publication of additional EGCA information.

4.4.3 Notification of Certificate Issuance by the CA to other entities

The FPKI Management Authority shall inform the EAO and FPKIPA of any certificate issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

No stipulation.

4.5.2 Relying Party Public key and Certificate Usage

CAs shall issue CRLs covering all unexpired certificates issued under this policy

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 with a new, extended validity period and a new serial number. Subscriber certificates issued under this policy shall not be renewed, except during recovery from EGCA key compromise (see Section 5.7.3). Subscriber requests for renewal shall be treated as a request for a new certificate.

The procedures for accomplishing the Certificate Renewal specified in this CP will be detailed in the EGCA's CPS.

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 obtain new keys. (Section 6.3.2 establishes usage periods for private keys for both EGCAs and subscribers.) 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. Subscriber requests for re-key shall be treated as a request for a new certificate.

The procedures for accomplishing the Certificate Re-Key specified in this CP will be detailed in the EGCA's CPS.

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 differs in one or more other fields from the old certificate. Subscriber requests for modification shall be treated as a request for a new certificate.

The procedures for accomplishing the Certificate Modification specified in this CP will be detailed in the EGCA's CPS.

4.9 CERTIFICATE REVOCATION & SUSPENSION

4.9.1 Circumstances for Revocation

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. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Privilege attributes asserted in the subscriber's certificate are reduced.
- The stipulations of the subscriber agreement have been violated.
- There is reason to believe the private key has been compromised.
- The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, 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.

Re-issuance of certificates, as specified in Section 3.1, shall be performed as quickly as possible except where it would adversely affect the integrity and trust of the system.

4.9.2 Who Can Request Revocation

The EGCA may summarily revoke certificates it issued to maintain the integrity of the system. A written notice and brief explanation for the revocation shall subsequently be provided to the subscriber.

The CA or EAO can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in the CPS. A human sponsor may request that the certificate he represents be revoked. Other authorized agency officials may request revocation as described in the CPS.

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 signed). The steps involved in the process of requesting a certification revocation are detailed in the CPS.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this policy.

4.9.5 Time within which CA must Process the Revocation Request

The EGCA will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall 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 shall be processed before the following CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

4.9.7 CRL Issuance Frequency

CRLs shall be issued at least once every 18 hours.

4.9.8 Maximum Latency of CRLs

If the EGCA cannot issue a CRL within 36 hours after the time specified in the next update field of its currently valid CRL, the FPKIPA shall be informed.

4.9.9 On-line Revocation/Status Checking Availability

If on-line revocation/status checking is supported EGCA, the latency of certificate status information distributed on-line by Entity CAs or their delegated status responders must meet or exceed the requirements for CRL issuance stated in 4.9.7.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

None.

4.9.12 Special Requirements Related To Key Compromise

In the event of an EGCA private key compromise, the following operations must be performed:

- Generate a new signing key pair and corresponding Root Certificate;
- Initiate procedures to notify subscribers of the compromise;
- Securely distribute the Root Certificate;
- Revoke the compromised certificate; and
- Optionally, the EGCA may renew current certificates under the new signing key. (see Section 4.6).

4.9.13 Circumstances for Suspension

Certificate suspension is not allowed by this policy.

4.9.14 Who can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 CERTIFICATE STATUS SERVICES

No stipulation.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW & RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

Under no circumstances shall a subscriber signature key be held in trust by a third party.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY MANAGEMENT & OPERATIONS CONTROLS

5.1 PHYSICAL CONTROLS

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

All the physical control requirements specified below apply equally to the EGCA, and any remote workstations used to administer the EGCA except where specifically noted.

5.1.1 Site Location & Construction

The location and construction of the facility housing the EGCA 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 EGCA equipment and records.

5.1.2 Physical Access

At a minimum, the physical access controls should:

- Ensure that no unauthorized access to the hardware is permitted;
- Ensure that 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; and
- Require two-person physical access control to both the cryptographic module and computer system.

5.1.2.1 Physical Access for CA Equipment

Removable cryptographic modules shall be inactivated before storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and EGCA equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and it shall not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the EGCA (See section 5.2 for procedures for accessing system components).

A security check of the facility housing the EGCA 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”;

- 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.

5.1.3 Power and Air Conditioning

The EGCA shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. The directories (containing EGCA-issued certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

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).

Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention & Protection

No stipulation.

5.1.6 Media Storage

Media shall be stored so as to protect them from accidental damage (e.g., water, fire, or electromagnetic). Media that contain audit, archive, or backup information shall be duplicated and stored in locations separate from the EGCAs.

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed in the disposal process. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 Off-Site backup

Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the EGCA's CPS. Backups are to be performed and stored offsite not less than once per week. At least one full backup copy shall be stored at an offsite location (separate from EGCA 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 EGCA.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible, or the integrity of the EGCA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The primary trusted roles defined this policy are Administrator, Officer, Auditor, and Operator. These roles will be employed at both EGCA locations as appropriate.

5.2.1.1 Administrator

The Administrator role is responsible for:

- Installation, configuration, and maintenance of the EGCA hardware and software;
- Establishing and maintaining EGCA system accounts;
- Configuring certificate profiles or templates and audit parameters; and
- Generating and backing up EGCA keys.

Administrators do not issue certificates to subscribers.

5.2.1.2 Officer

The Officer's role and the corresponding procedures shall be defined in the EGCA's CPS. The Officer's responsibility is to ensure the following functions occur according to the stipulations of this policy, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and the accuracy of information included in certificates;
- Executing the issuance of certificates; and
- Requesting, approving, and executing the revocation of certificates.

5.2.1.3 Auditor

The Auditor role is responsible for:

- Reviewing, maintaining, and archiving audit logs; and
- Performing or overseeing internal compliance audits to ensure that the EGCA are operating in accordance with its CPS.

5.2.1.4 Operator

The Operator role is responsible for the routine operation of the EGCA equipment and operations such as system backups and recovery, or changing recording media.

5.2.2 Number of Persons Required per Task

Two or more persons are required for the following tasks:

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

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants must 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 trusted role.

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.

5.2.4 Roles Requiring Separation of Duties

Individual EGCA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The EGCA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both the Administrator and Officer roles, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual shall have more than one identity.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the EGCA shall be set forth in the EGCA's CPS.

5.3.2 Background Check Procedures

Background check procedures shall be described in the EGCA's CPS and shall demonstrate that requirements set forth in Section 5.3.1 are met.

5.3.3 Training Requirements

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

- CA security principles and mechanisms;
- All PKI software versions in use on the EGCA system;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and

- Stipulations of this policy.

5.3.4 Retraining Frequency & Requirements

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

5.3.5 Job Rotation Frequency & Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The EAO shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the EGCA that are not authorized in this CP, the corresponding CPS, or other published procedures.

5.3.7 Independent Contractor Requirements

See Section 5.3.1. PKI vendors who provide any services shall establish procedures to ensure that any subcontractors perform in accordance with the CPS and this policy.

5.3.8 Documentation Supplied To Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to access, security and activities (e.g. configuration management) of the EGCA. 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.

5.4.1 Types of Events Recorded

All security auditing capabilities of EGCA operating system and PKI EGCA applications shall be enabled during installation. 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;
- A success or failure indicator when executing the EGCA's signing process;
- A success or failure indicator when performing certificate revocation; and
- The identity of the entity and/or Operator that caused the event.

A message from any source requesting an action by the EGCA is an auditable event; the message must include message date and time, source, destination, and contents.

The EGCA shall record the events identified in the list below. Where these events cannot be electronically logged, the EGCA shall supplement electronic audit logs with physical logs as necessary.

- SECURITY AUDIT:
  - Any changes to the Audit parameters, e.g., audit frequency, type of event audited
  - Any attempt to delete or modify the Audit logs
  - Obtaining a third-party time-stamp
- IDENTIFICATION AND AUTHENTICATION:
  - Successful and unsuccessful attempts to assume a role
  - The value of maximum authentication attempts is changed
  - Maximum authentication attempts, unsuccessful authentication attempts which occur during user login
  - An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
  - An Administrator changes the type of authenticator, (e.g., from password to biometrics)
- LOCAL DATA ENTRY:
  - All security-relevant data that is entered in the system
- REMOTE DATA ENTRY:
  - All security-relevant messages that are received by the system
- DATA EXPORT AND OUTPUT:
  - All successful and unsuccessful requests for confidential and security-relevant information
- KEY GENERATION:
  - Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
- PRIVATE KEY LOAD AND STORAGE:
  - The loading of Component private keys
  - All access to certificate subject private keys retained within the CA for key recovery purposes
- TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:
  - All changes to the trusted public keys, including additions and deletions
- SECRET KEY STORAGE:
  - The manual entry of secret keys used for authentication
- PRIVATE AND SECRET KEY EXPORT:
  - The export of private and secret keys (keys used for a single session or message are excluded)
- CERTIFICATE REGISTRATION:
  - All certificate requests
- CERTIFICATE REVOCATION:
  - All certificate revocation requests
- CERTIFICATE STATUS CHANGE APPROVAL:
  - The approval or rejection of a certificate status change request
- CA CONFIGURATION:
  - Any security-relevant changes to the configuration of the CA
- ACCOUNT ADMINISTRATION:
  - Roles and users are added or deleted
  - The access control privileges of a user account or a role are modified
- CERTIFICATE PROFILE MANAGEMENT

    - All changes to the certificate profile
- REVOCATION PROFILE MANAGEMENT
    - All changes to the revocation profile
- CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
    - All changes to the certificate revocation list profile
- MISCELLANEOUS
    - Appointment of an individual to a Trusted Role
    - Designation of personnel for multiparty control
    - Installation of the Operating System
    - Installation of the CA
    - Installing hardware cryptographic modules
    - Removing hardware cryptographic modules
    - Destruction of cryptographic modules
    - System Startup
    - Logon Attempts to CA Apps
    - Receipt of Hardware / Software
    - Attempts to set passwords
    - Attempts to modify passwords
    - Backing up the CA internal database
    - Restoring the CA internal database
    - File manipulation (e.g., creation, renaming, moving)
    - Posting of any material to a repository
    - Access to the CA internal database
    - All certificate compromise notification requests
    - Loading tokens with certificates or Shipment of Tokens
    - Zeroizing tokens
    - Rekey of the CA
    - Configuration changes to the CA server involving:
        - Hardware
        - Software
        - Operating System Patches
        - Security Profiles
- PHYSICAL ACCESS / SITE SECURITY
    - Personnel Access to the room housing the CA
    - Access to the CA server
    - Known or suspected violations of physical security
- ANOMALIES
    - Software Error conditions
    - Software check integrity failures
    - Receipt of improper messages
    - Misrouted messages
    - Network attacks (suspected or confirmed)
    - Equipment failure o Electrical power outages
    - Uninterruptible Power Supply (UPS) failure
    - Obvious and significant network service or access failures
    - Violations of Certificate Policy
    - Violations of Certification Practice Statement
    - Resetting Operating System clock

5.4.2 Frequency of Processing Log

Review of the audit log shall be required at least once every two months. All significant events shall be explained in an audit log summary. A statistically significant portion of the security audit data generated by the EGCA since the last review shall be examined. This amount will be described in the CPS. Such reviews involve verifying that the log has not been tampered with 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 2 months in addition to being retained in the manner described below. The individual who removes audit logs from the EGCA system shall be an official different from the individuals who, in combination, command the EGCA signature key.

5.4.4 Protection of Audit Logs

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. EGCA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent offsite in accordance with the CPS, on a monthly basis.

5.4.6 Audit Collection System (internal vs. external)

The audit log collection system may or may not be external to the EGCA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application 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, operations shall be suspended until the problem has been remedied. The EAO shall determine when to resume operations.

5.4.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

5.4.8 Vulnerability Assessments

The EGCA will perform routine self-assessments of security controls.

5.5 RECORDS ARCHIVAL

The EGCAs must follow either the General Records Schedules established by the National Archives and Records Administration (NARA) or an agency-specific schedule as applicable.

5.5.1 Types of Events Archived

CA archive records shall be sufficiently detailed to determine the proper operation of the EGCA and the validity of any certificate (including those revoked or expired) issued by the EGCA. At a minimum, the following data shall be recorded for archive:

- CA accreditation (if applicable)
- Certificate Policy
- Certification Practice Statement
- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Record of Re-key
- Revocation requests
- Subscriber identity Authentication data as per Section 3.2.2
- Documentation of receipt and acceptance of certificates (if applicable)
- Subscriber agreements
- Documentation of receipt of tokens
- All CRLs issued and/or published
- Other data or applications to verify archive contents
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys)
- All access to certificate subject private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- The export of private and secret keys (keys used for a single session or message are excluded)
- The approval or rejection of a certificate status change request
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

5.5.2 Retention Period for Archive

The archive records must be kept for a minimum of 10 years and 6 months without any loss of data.

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the EGCA, archived records may be moved to another medium. The contents of the archive shall not be released except (1) in accordance with agency policy, or (2) as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the EGCA.

5.5.4 Archive Backup Procedures

No stipulation.

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.

5.5.7 Procedures to Obtain & Verify Archive Information

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

5.6 KEY CHANGEOVER

To minimize risk from compromise of an EGCA's private signing key, that key may be changed often. From that time on, only the new key will be used for certificate signing purposes. The older, but still valid, public key will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, the old key must be retained and protected.

The EGCA's signing key shall have a validity period as described in Section 6.3.2.

5.7 COMPROMISE & DISASTER RECOVERY

The EGCA and directory system shall be deployed so as to provide 24-hour, 365-day availability. The EGCA shall implement features to provide high levels of reliability. The following subsections outline the policy for instances that may prevent such maintenance of reliability.

The FPKI Management Authority shall operate a hot backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary site. The EGCA

operations shall be designed to restore full service within six (6) hours of primary system failure.

5.7.1 Incident and Compromise Handling Procedures

No stipulation.

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

If the EGCA equipment is damaged or rendered inoperative, but the EGCA signature keys are not destroyed, EGCA operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information. The FPKIPA shall be notified as soon as possible.

5.7.3 Entity (CA) Private Key Compromise Procedures

In case of an EGCA key compromise, the FPKIPA and EAO shall be immediately informed, as well as any subscribers. Subsequently, the EGCA installation shall be reestablished. If the EGCA distributes a Root Certificate for use as a trust anchor, the new self-signed certificate must be distributed via secure out-of-band mechanisms. The CPS shall detail the secure out-of-band mechanisms.

Subscriber certificates may be renewed automatically by the EGCA under the new key pair, or the EGCA may require subscribers to repeat the initial certificate application process.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby the EGCA installation is physically damaged and all copies of the EGCA signature key are destroyed as a result, the FPKIPA and EAO shall be notified at the earliest feasible time, and the EAO shall take whatever action it deems appropriate.

Relying parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of EGCA operation with new keys and certificates.

5.8 CA & RA TERMINATION

In the event of termination of the EGCA operation, certificates signed by the EGCA shall be revoked. Prior to EGCA termination, the EGCA shall provide archived data to an archive facility as specified in the CPS. As soon as possible, the EGCA will advise all other organizations to which it has issued certificates of the EGCA termination, using an agreed-upon method of communication specified in the CPS.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION & INSTALLATION

6.1.1 Key Pair Generation

Validated software or hardware cryptographic modules shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.

A private key will be generated within the boundary of a cryptographic module, as described in Section 6.2.6. The owner of the cryptographic token will always generate the key, so there is no need to deliver the private key. Where private keys corresponding to certificates issued under this policy are shared by multiple devices asserting the same DNS name (e.g., load balanced authentication servers), the private key shall be delivered in a secure manner to prevent disclosure.

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used by EGCAs to sign certificates, CRLs or status information shall be generated in FIPS 140 validated cryptographic modules. The module(s) shall meet or exceed Security Level 2. Multiparty control is required for EGCA key pair generation, as specified in Section 5.2.2.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The audit trail must identify and document any failures or anomalies in the key generation process, and any corrective actions taken. For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used.

6.1.1.2 Subscriber Key Pair Generation

Subscribers shall perform their own key pair generation.

Key generation shall be performed using a FIPS-approved method.

For certificates issued under the Level 1 IdP, Level 2 IdP, Level 3 IdP, Level 4 IdP, BAE Broker, Relying Party, Metadata Signer (Medium), Metadata Signer (Hardware) policies, subscriber key pair generation shall be performed by the subscriber. Validated software or hardware cryptographic modules shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation.

For certificates issued under the Level 3 IdP, Level 4 IdP, BAE Broker, Relying Party, Metadata Signer (Medium), Metadata Signer (Hardware) policies, subscriber key pairs shall be generated at a minimum in FIPS 140 Level 2 hardware cryptographic modules. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method.

For certificates issued under the Level 1 IdP, Level 2 IdP policies, subscriber key pairs shall be generated at a minimum in FIPS 140 Level 1 hardware cryptographic modules. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method.

6.1.2 Private Key Delivery to Subscriber

Subscribers generate their own key pairs; therefore delivery of subscriber private keys is not necessary.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys must be delivered for certificate issuance in a way that binds the applicant principal's verified identification to the public key. This binding may be accomplished using cryptography. If cryptography is used it must be at least as strong as that employed at certificate issuance. This binding may be accomplished using non-cryptographic physical and procedural mechanisms. Regardless of the method selected, the mechanism used for public key delivery shall be set forth in the EGCA's CPS.

The public key and the Subscriber's identity must be delivered securely to the EGCA 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 must be at least as strong as the EGCA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

When an EGCA updates its signature key pair, the EGCA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate or in a key rollover certificate. Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods for self-signed certificate delivery are:

- The EGCA loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms;
- Secure distribution of self-signed certificates through secure out-of-band mechanisms;
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

[Practice Note: Other methods that preclude substitution attacks may be considered acceptable.]

Key rollover certificates are signed with the EGCA's current private key, so secure distribution is not required.

[Practice Note: To ensure the availability of the new public key, the key rollover certificates should be distributed using directories and other repositories.]

The public key of the EGCA must be available for certification trust paths to be created and verified. In general, EGCA certificates are published in the public repository (see Section 2), and the verification of public keys is performed using X.509 path validation.

Where users rely on the EGCA's public key as a trust anchor, the EGCA must ensure that its users have obtained a self-signed EGCA certificate through trusted procedural mechanisms. Such a self-signed EGCA certificate is sometimes called a Self-signed Root Certificate. This document will use the term Root Certificate.

Acceptable methods for Root Certificate delivery include but are not limited to:

- The EGCA loading a Root Certificate onto tokens delivered to relying parties via secure mechanisms, such as loading the Root Certificate onto the token during the subscriber's appearance at the EGCA;
- Distribution of Root Certificates through secure out-of-band mechanisms;
- Comparison of certificate hashes or fingerprints against Root Certificate hashes or fingerprints 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 certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

CAs that distribute Root Certificates will create key rollover certificates as a consequence of EGCA re-key. The new EGCA keys may be used securely (through the X.509 path validation algorithm) without explicit delivery of the public key to subscribers.

6.1.5 Key Sizes

This CP requires use of RSA PKCS#1 signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA public keys.

[Practice Note: Future versions of this policy may specify additional FIPS-approved signature algorithms.]

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 2048 bit keys.

CAs that generate certificates and CRLs under this policy shall use SHA-256 hash algorithm when generating digital signatures. Signatures on certificates and CRLs shall be generated using SHA-256.

End entity certificates shall contain RSA public keys that are at least 2048 bits.

Certificates issued that expire after December 31, 2030 shall contain RSA public keys that are 3072 bits or elliptic curve keys that are 256 or 384 bits.

Use of TLS or another protocol providing similar security to accomplish certificate issuance or any of the requirements of this CP shall require (1) AES for the symmetric key and (2) at least 2048 bit RSA or 224 bit elliptic curve keys.

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 186-2.

Public key parameters shall always be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186-2.

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

The use of a specific key is constrained by the key usage extension in the X.509 certificate.

Public keys that are bound into subscriber certificates shall assert the *digitalSignature* bit and/or the *keyEncipherment* bit.

Public keys that are bound into EGCA certificates shall be used only for signing certificates and status information (e.g., CRLs). EGCA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. EGCA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. If the EGCA certificate is to be used to verify both certificate and CRLs, both the *keyCertSign* and *cRLSign* bits shall be asserted.

Certificates to be used for digital signatures shall assert the *digitalSignature* bit. Certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. Certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit. Certificates to be used for both digital signatures and key management shall assert the *digitalSignature* bit and either the *keyEncipherment* (for RSA) or *keyAgreement* (for elliptic curve) bit. Certificates shall not assert the *nonRepudiation* bit.

Certificates issued under the Level 1 IdP, Level 2 IdP, Level 3 IdP, Level 4 IdP policies shall assert the *claimSigner* OID in the extended key usage extension. Asserting the *claimSigner* OID in a certificate indicates that the keys associated with that certificate are used for signing claims. A claim is a signed object that binds some set of attributes to a given subject (i.e., a subject/attribute pair) where the Signer is asserting the binding. Certificates issued under these policies shall be used for digitally signing authentication claims that bind identity attributes to subjects.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards & Controls

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [FIPS 140-2]. Cryptographic modules shall be validated to a FIPS 140 level identified in this section.

The EGCA shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module.

For certificates issued under the Level 1 IdP, Level 2 IdP, CSP, and Agency Application policies, FIPS 140 Level 1 or higher validated cryptographic module shall be used for all cryptographic operations.

For certificates issued under the Level 3 IdP, Level 4 IdP, BAE Broker, Relying Party, Metadata Signer (Medium), Metadata Signer (Hardware) policies, FIPS 140 Level 2 or higher validated cryptographic module shall be used for all cryptographic operations.

6.2.2 Private Key Multi-Person Control

A single person shall not be permitted to invoke the complete EGCA signature process or access any cryptomodule containing the complete EGCA private signing key. EGCAsignature keys may be backed up only under two-person control. Access to EGCA signing keys backed up for disaster recovery shall be under at least two-person control. The names of the parties used for two- person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

CA private keys are never escrowed. Private keys are generated by the subscriber or device.

6.2.4 Private Key Backup

6.2.4.1 Backup of EGCA & Entity CA Private Signature Key

The EGCA private signature keys shall be backed up under the same multi-person control as the original signature key. Such backup shall create only a single copy of the signature key at the EGCA location; a second copy may be kept at the EGCA backup location. Backup procedures shall be included in the EGCA's CPS.

6.2.4.2 Backup of subscriber private signature key

Subscriber private keys whose corresponding public key is contained in a certificate may be backed up or copied, but must be held in the subscriber's control. Backed up subscriber private keys must be encrypted using a symmetric algorithm of consistent strength or stored in a cryptographic module validated at FIPS 140 Level 2.

6.2.5 Private Key Archival

CA and subscriber private keys shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Subscriber keys shall be generated by and in a cryptographic module. 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 from outside the cryptographic token 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

No stipulation beyond that specified in FIPS-140.

6.2.8 Method of Activating Private Keys

The subscriber must be authenticated to the cryptographic token before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. 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 Keys

Cryptographic modules that have been activated shall not be 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. EGCA Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 Method of Destroying Private Keys

Private keys shall be destroyed when they are no longer needed or when the certificates to which they correspond expire or are revoked. This may be performed by executing a "zeroize" command. Physical destruction of hardware is not required.

6.2.11 Cryptographic Module Rating

Requirements for cryptographic modules are as stated above in Section 6.2.

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

The usage period for an EGCA key pair is a maximum of six years. The EGCA private key may be used to generate certificates for the first half of the usage period (3 years), and the public key may be used to validate certificates for the entire usage period. If the EGCA private key is used to sign CRLs, it may be used to sign CRLs for the entire usage period.

Subscriber public keys have a maximum usage period of one half the EGCA key pair usage period (3 years). Subscriber private keys have the same usage period as their corresponding public key.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation & Installation

CA activation data may be user-selected (by each of the multiple parties holding that activation data). 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.

Subscriber activation data may be user-selected. 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.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should be either biometric in nature or memorized (not written down). If written down, activation data shall be physically secured or encrypted under a FIPS approved cryptographic algorithm, and shall not be stored with the cryptographic module.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

Computer security controls are required to ensure EGCA operations are performed as specified in this policy. The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards:

- Require authenticated logins;
- Provide Discretionary Access Control;
- Provide a security audit capability;
- Restrict access control to EGCA services and PKI roles;
- Enforce separation of duties for PKI roles;
- Require identification and authentication of PKI roles and associated identities;
- Prohibit object reuse or require separation for random access memory;
- Require use of cryptography for session communication and database security;
- Archive EGCA history and audit data;
- Require self-test security-related EGCA services;
- Require a trusted path for identification of PKI roles and associated identities;
- Require a recovery mechanism for keys and the EGCA system; and
- Enforce domain integrity boundaries for security-critical processes.

For remote workstations used to administer the EGCAs, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Generate and archive audit records for all transactions (see Section 5.4);
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

All communications between any PKI trusted role and the EGCA shall be authenticated and protected from modification.

6.5.1 Specific Computer Security Technical Requirements

No stipulation.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 System Development Controls

The System Development Controls for the EGCA are as follows:

- The EGCA shall use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured to operate the EGCA 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 specifically for the EGCA 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.
- The EGCA hardware and software shall be dedicated to performing one task: the EGCA. There shall be no other applications, hardware devices, network connections, or component software installed that are not parts of the EGCA operation. Where the EGCA operation supports multiple EGCAs, the hardware platform can support multiple CAs.
- Proper care shall be taken to prevent malicious software from being loaded onto the EGCA equipment. Only applications required to perform the operation of the EGCA shall be obtained from sources authorized by local policy. EGCA hardware and software shall 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 shall be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the EGCA system, in addition to any modifications and upgrades, shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the software or configuration. The EGCA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The EGCA shall periodically verify the integrity of the software as specified in the CPS.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

A network guard, firewall, or filtering router must protect network access to EGCA equipment. The network guard, firewall, or filtering router shall limit services allowed to and from the EGCA equipment to those required to perform EGCA functions.

Protection of EGCA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the EGCA equipment shall be necessary to the functioning of the EGCA application.

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.

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

6.8 TIME STAMPING

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, see Section 5.4.1.

7. CERTIFICATE, CRL, AND OCSP PROFILES FORMAT

7.1 CERTIFICATE PROFILE

Certificates issued by an EGCA under this policy shall conform to the X.509 Certificate and CRL Extensions Profile for the EGCA [EGCA-PROF].

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in [EGCA-PROF].

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}

Certificates issued under this CP shall use the following OID to identify the algorithm associated with the subject key:

RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name Forms

The subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by Section 3.1.1.

Subscriber certificates shall contain Internet Domain Names, as specified in Section 3.1.1.

7.1.5 Name Constraints

Certificates issued under this CP shall not contain name constraints.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert one of the following OIDs in the certificate policies extension, as appropriate:

Table 2 - id-fpki-eGov Policy OIDs

id-eGov-Level2	::= {2 16 840 1 101 3 2 1 3 10}
id-eGov-Applications	::= {2 16 840 1 101 3 2 1 3 11}

id-eGov-Level1-IdP	::= {2.16.840.1.101.3.2.1.3.28}
id-eGov-Level2-IdP	::= {2.16.840.1.101.3.2.1.3.29}
id-eGov-Level3-IdP	::= {2.16.840.1.101.3.2.1.3.30}
id-eGov-Level4-IdP	::= {2.16.840.1.101.3.2.1.3.31}
id-eGov-BAE-Broker	::= {2.16.840.1.101.3.2.1.3.32}
id-eGov-RelyingParty	::= {2.16.840.1.101.3.2.1.3.33}
id-eGov-MetaSigner	::= {2.16.840.1.101.3.2.1.3.34}
id-eGov-MetaSigner-Hardware	::= {2.16.840.1.101.3.2.1.3.35}

7.1.7 Usage of Policy Constraints Extension

Certificates issued under this CP shall not contain policy constraints.

7.1.8 Policy Qualifiers Syntax & Semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Certificates issued under this policy shall not contain a critical certificate policy extension.

7.2 CRL PROFILE

CRLs issued by an EGCA under this policy shall conform to the CRL Profile specified in [EGCA- PROF].

7.2.1 Version Numbers

The EGCAs shall issue X.509 Version two (2) CRLs.

7.2.2 CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension are specified in [EGCA-PROF].

7.3 OCSP PROFILE

If implemented, Certificate Status Servers (CSS) shall sign responses using algorithms designated for CRL signing.

8. COMPLIANCE AUDIT & OTHER ASSESSMENTS

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

CAs operating under this policy shall conduct a compliance audit no less than once every year. As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of EGCAs may be carried out in accordance with the requirements as specified in the Triennial Audit Guidance document located at http://www.idmanagement.gov/fpkipa/.

Additionally, the EAO has the right to require aperiodic inspections of EGCAs to validate that the EGCA is operating in accordance with their CPS.

8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR

The Auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the EGCA's CPS and this CP.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance Auditor either shall be a private firm, which is independent from the entities (EGCA) being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. The EAO 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 an EGCA comply with all the requirements of the current versions of this CP and the EGCA's CPS. All aspects of the EGCA operation shall be subject to compliance audit inspections. The process used by the EAO to determine if a certificate should be issued to CSPs, agency application servers, Level 1-4 IdPs, Relying Parties, BAE Brokers, and MetaData Signers is out of scope for the compliance audit.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the compliance Auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions shall be performed:

- The compliance Auditor shall note the discrepancy;
- The compliance Auditor shall notify the parties identified in Section 8.6 of the discrepancy; and
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the EAO who will notify the FPKI PA as appropriate.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may decide to temporarily halt operation of the EGCA or take

other actions it deems appropriate. The FPKIPA will develop procedures for making and implementing such determinations.

8.6 COMMUNICATION OF RESULTS

An Audit Compliance Report shall be provided to the EGCA. After 30 days, the Audit Compliance Report and identification of corrective measures taken or being taken by the EGCA shall be provided to the EAO. Status updates will be provided to the FPKI PA as appropriate for continued trust. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

9. OTHER BUSINESS & LEGAL MATTERS

9.1 FEES

No stipulation.

9.1.1 Certificate Issuance/Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fee

No stipulation.

9.1.4 Fees for other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

This CP contains no limits on the use of certificates issued by EGCAs under this policy.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

EGCA information not requiring protection shall be made publicly available. Public access to organizational information shall be determined by the respective organization.

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information not within the scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 PRIVACY OF PERSONAL INFORMATION

No stipulation.

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information treated as Private

No stipulation.

9.4.3 Information not deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

No stipulation.

9.4.5 Notice and Consent to use Private Information

No stipulation.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

No stipulation.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

No stipulation.

9.6 REPRESENTATIONS & WARRANTIES

No stipulation.

9.6.1 CA Representations and Warranties

No stipulation.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

A subscriber (i.e., human sponsors of device certificates) shall be required to sign a document containing the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

The subscriber agreement shall require subscribers to:

- Accurately represent themselves in all communications with the PKI authorities and other subscribers;

- Protect their private key(s) at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures;
- Promptly notify the appropriate EGCA that issued their certificates of suspicion that their private keys are compromised or lost. Such notification shall be made directly or indirectly through mechanisms consistent with the EGCA's CPS; and
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).

In addition to the above requirements, subscriber agreements shall include the following additional stipulations per the table below.

Table 9-1: Additional Subscriber Agreement Stipulations by Policy

Policy	Subscriber Agreement Stipulations
Level 1 IdP Level 2 IdP Relying Party BAE Broker (without HSMs) Metadata Signer (Medium)	▪ No additional requirements
Level 3 IdP Level 4 IdP BAE Broker (using HSMs) Metadata Signer (Hardware)	▪ Only a defined list of people who have trusted roles shall be able to physically or logically access the Hardware Security Module (HSM) device. ▪ Backup keys shall always be under two person control. ▪ Any physical move or removal of the HSM shall be under two person control.

9.6.4 Relying Parties Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Affiliated Organizations

No stipulation.

9.6.6 Representations and Warranties of other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

No stipulation.

9.8 LIMITATIONS OF LIABILITY

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

9.9 INDEMNITIES

No stipulation.

9.10 TERM & TERMINATION

No stipulation.

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

The E-Authentication Authorizing Official (EAO) shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy.

9.12 AMENDMENTS

The EAO shall review this CP at least once every year. Corrections, updates, or suggested changes to this CP shall be publicly available. Suggested changes to this CP shall be communicated to the contact in Section 1.5; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.1 Procedure for Amendment

No stipulation.

9.12.2 Notification Mechanism and Period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 DISPUTE RESOLUTION PROVISIONS

No stipulation.

9.14 GOVERNING LAW

No stipulation.

9.15 COMPLIANCE WITH APPLICABLE LAW

All CAs operating under this policy are required to comply with applicable law.

9.16 MISCELLANEOUS PROVISIONS

The terms and provisions of this Certificate Policy shall be interpreted under and governed by applicable Federal law.

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in Section 9.12.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

The EAO will not issue waivers; EGCAs issuing under this policy are required to meet all facets of the policy.

10. BIBLIOGRAPHY

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

ABADSG	Digital Signature Guidelines, 1996-08-01 http://www.abanet.org/scitech/ec/isc/dsgfree.html
CAF	E-Authentication Interim Credential Assessment Framework (CAF), 12/19/2003 release 1.3.0. http://www.eapartnership.org/docs/CAF_CAFv1-3.doc
EGCA-PROF	X.509 Certificate and CRL Extensions Profile for EGCA, March 2, 2004.
FIPS 140-2	Security Requirements for Cryptographic Modules, 1994-02 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186	Digital Signature Standard, 1994-05-19 http://csrc.nist.gov/fips/fips186.pdf
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 2000.
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996 http://www4.law.cornell.edu/uscode/40/1452.html
M-04-04	E-Authentication Guidance for Federal Agencies, December 16, 2003.
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999
PKCS#1	RSA Cryptography Standard, Technical Note, Version 2.1. 14 June 2002. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf
RFC 2527	Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999
RFC 3280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Housley et al., April 2002.
SP 800-63	Electronic Authentication Guideline, Burr, Polk, and Dodson.
USGold	GOVERNMENTWIDE DIRECTORY SUPPORT 2 TECHNICAL SERIES: The Updated USGold Schema, July 14, 1997. http://csrc.nist.gov/pki/twg/directory_references.htm

11. ACRONYMS & ABBREVIATIONS

AES	Advanced Encryption Standard
CA	Certification Authority
CAF	Credential Assessment Framework
EGCA-Prof	X.509 Certificate and CRL Extensions Profile for the E-Governance Certification Authorities
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Credential Service Provider
DN	Distinguished Name
DNS	Domain Naming System
DSS	Digital Signature Standard
EAO	E-Authentication Authorizing Official
FIPS	(U.S.) Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
FPKIPA	Federal PKI Policy Authority
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
OID	Object Identifier
OMB	Office of Management and Budget
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509

POC	Point of Contact
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SAML	Security Assertion Markup Language
SHA-1	Secure Hash Algorithm, Version 1
SHA-256	Secure Hash Algorithm, 256-bit version
TLS	Transport Layer Security
U.S.C.	United States Code
WWW	World Wide Web

12. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to IS resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a CA 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. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009audit trail]
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. [NS4009]

Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical characteristic of a human being, including a photograph for visual identification. For the purposes of this document, biometrics do not include handwritten signatures.
CA Facility	The collection of equipment, personnel, procedures, and structures that are used by a CA to perform certificate issuance and revocation.
Certificate	A digital representation of information which at least (1) identifies the CA 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 CA 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.
Certificate Policy (CP)	A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A CP addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a CP can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certificate Revocation List (CRL)	A list maintained by a CA of the certificates it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides online verification to a relying party of a subject certificate's trustworthiness and may also provide additional attribute information for the subject certificate.
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. A CA managing certificates may use this information.

Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
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).
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.
Component Private Key	Private key associated with a function of the certificate-issuing equipment, as opposed to being associated with an Operator or administrator.
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. [NS4009]
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Credential Service Provider	An organization that offers one or more credential services.
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. [FIPS 1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
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.
Discretionary Access Control	Means of restricting access to objects based on user identity.
E-Commerce	The use of network technology (especially the Internet) to buy or sell goods and services.
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.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. 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.
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 (2) even knowing one key, it is computationally infeasible to discover the other key.
Mutual Authentication	Authentication when parties at both ends of a communication activity authenticate each other (see "Authentication").
Naming Authority	An organizational entity responsible for assigning DNs and for assuring that each DN is meaningful and unique within its domain.
Nonrepudiation	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. [NS4009]. Technical nonrepudiation 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 nonrepudiation 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. In the federal government PKI OIDs are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties using 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).
Privacy	Restricting access to subscriber or relying party information in accordance with Federal law and Agency 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 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 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 does not sign or issue certificates (i.e., an RA 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 Agency 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.
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.
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.
Secret Key	A “shared secret” used in symmetric cryptography, wherein users are authenticated based on a password, PIN, or other information shared between the user and the remote host or server. A single key is shared between two parties: the

	sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.
Server	A system entity that provides a service in response to requests from clients.
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.
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
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. [NS4009]
Trust List	Collection of Root Certificates used by relying parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Agency in confirming subscriber identification during the registration process. Trusted Agents do not have automated interfaces with CAs.
Root Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in Root 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. [NS4009]
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.
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. [FIPS 1401]

13. ACKNOWLEDGEMENTS

The Certificate Policy Working Group developed this CP based on RFC 3647 and the original EGCA Certificate Policy.