United States Federal PKI

X.509 Certification Practice Statement –

X.509 Certification Practice Statement (CPS) For The

E-Governance Certification Authorities (EGCA)

26 March 2012

Version 4.1
REDACTED

Signature Page

_____ _____

Chair, Federal Public Key Infrastructure Policy Authority DATE

Table of Contents

List of Tables

RECORD OF CHANGES

CHANGE DESCRIPTION	VERSION NUMBER	DATE OF CHANGE	DATE RECEIVED	DATE ENTERED	SIGNATURE OF PERSON ENTERING CHANGE
Updated CPS to RFC 3647 Format.	2.0	2 February 2008			
Updated CPS to reflect new location of FPKI and changes made for deployment of the Target Architecture (planned deployment in September 2010).	3.0	21 May 2010			
Minor updates to CPS to clarify archiving procedures.	3.1	27 May 2010			
Updated to enhance the description of CPS activities to meet policy.	3.2	19 July 2010			
Major revision that includes: (1) modifications to support the EGTS; (2) modifications to align with the Common and FBCA CPSs where appropriate (e.g., physical and environmental security requirements); (3) updates to address annual audit findings; and (4) minor revisions to address new FPKI Trust Infrastructure environment.	4.0	28 November 2011			
Revisions in response to annual PKI audit findings and recommendations. Audit conducted in January 2012.	4.1	26 March 2012			

CHANGE DESCRIPTION	VERSION NUMBER	DATE OF CHANGE	DATE RECEIVED	DATE ENTERED	SIGNATURE OF PERSON ENTERING CHANGE
Removed sensitive information for security purposes and to allow for public dissemination of CPS.	4.1 REDACTED	14 May 2012			

1 EGCA CPS INTRODUCTION

The EGCA Certification Practice Statement (CPS) documents the internal practices and procedures used by the Federal Public Key Infrastructure Management Authority (FPKIMA) by describing the practices concerning certificate lifecycle services including issuance, certificate management (including publication and archiving), revocation, and renewal or re-keying of the E-Governance Certification Authorities (EGCA).

The EGCA CPS covers the operation of systems and the management of facilities which operate in compliance with the *X.509 Certificate Policy for the E-Governance Certification Authorities* [EGCA CP]. The [EGCA CP] includes ten certificate policies and the Federal PKI Trust Infrastructure common repository functionality used to post CRLs and certificates issued by the EGCA.

The EGCA provides certificates to agency application (AA) servers, credential service providers (CSPs), Level 1-4 Identity Providers (IdPs), Relying Parties, Backend Attribute Exchange (BAE) Brokers, and Metadata Signers to support exchange of authentication information between CSPs and AAs, and between IdPs and Relying Parties. It also supports exchange of attribute information and exchange of Metadata for conducting assertion-based authentication transactions.

The EGCA provides the following security management services:

- Certification Authority (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).

The EGCA CPS implements and complies with the requirements established in [EGCA CP] Version 2.0 dated September 9, 2011. Further, this CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework* [RFC 3647].

1.1 OVERVIEW

1.1.1 Certification Practice Statement

This CPS documents the internal practices and procedures used by the FPKIMA. It covers the operation of systems and the management of facilities, which includes EGCA and the Federal PKI common repository functionality, used to post certificates and CRLs issued.

1.1.2 Relationship between the CP and the CPS

[EGCA CP] states what assurance can be placed in a certificate issued by the EGCA.

This CPS states how the EGCA establishes that assurance.

1.1.3 Scope

This CPS implements the E-Governance Certificate Policy that applies to certificates issued by EGCA for devices used as CSPs, AA servers, Level 1-4 IdPs, Relying Parties, BAE Brokers, or Metadata Signers. The EGCA does not issue certificates to human subscribers.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is referred to as the EGCA CPS.

The EGCA CPS provides substantial assurance concerning identity of certificate subjects. The EGCA issues certificates in accordance with [EGCA CP], asserting one and only one (excluding the CA certificates) of the following object identifiers (OIDs) in the certificate policy extension:

Table 1.2-1. 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}

The EGCA issues certificates to CSPs under the [EGCA CP] that contain the id-eGov-Level2 OID.

The EGCA issues certificates to AA servers under the [EGCA CP] that contain the id-eGov-Applications OID.

The EGCA issues certificates to Level 1 IdPs under the [EGCA CP] that contain the id-eGov-Level1-IdP OID.

The EGCA issues certificates to Level 2 IdPs under the [EGCA CP] that contain the id-

eGov-Level2-IdP OID.

The EGCA issues certificates to Level 3 IdPs under the [EGCA CP] that contain the id-eGov-Level3-IdP OID.

The EGCA issues certificates to Level 4 IdPs under the [EGCA CP] that contain the id-eGov-Level4-IdP OID.

The EGCA issues certificates to BAE Brokers under the [EGCA CP] that contain the id-eGov-BAE-Broker OID.

The EGCA issues certificates to Relying Parties under the [EGCA CP] that contain the id-eGov-RelyingParty OID.

The EGCA issues certificates to Metadata Signers under the [EGCA CP] that contain either the id-eGov-MetaSigner or id-eGov-MetaSigner-Hardware 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. Use of these certificates for other purposes, while not prohibited, is outside the scope of the [EGCA CP] and this CPS.

The following are roles relevant to the administration and operation of CAs under the E-Governance Certificate Policy. The responsibilities of each of the Trusted Roles are further defined in Section 5.2.1.

1.3.1 PKI Authorities

The following table summarizes the roles relevant to the administration and operation of the EGCA. These roles are defined in the [EGCA CP].

Table 1.3-1. EGCA Roles

EGCA Role	*Description*
Federal PKI Policy Authority (FPKIPA)	The 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 EGCA is operating in compliance with the approved CPSs.
FPKI Management Authority (FPKIMA)	The FPKIMA is the organization that operates the FPKI CAs in accordance with the practices and procedures identified in this CPS. In particular it operates the EGCA.

EGCA Role	*Description*
FPKIMA Program Manager (PM)	The FPKIMA PM is the individual within the FPKIMA who has principal responsibility for overseeing the proper operation of the EGCA including the EGCA repository and selecting the FPKIMA staff.
FPKIMA Trusted Roles	The Trusted Roles are the individuals within the FPKIMA, selected by the ISSO, who operate the EGCA executing EAO direction to issue EGCA certificates to Subscribers. The roles include FPKIMA Officer, Auditor, Administrator, and Operator, all described in the EGCA CPS, Section 5.2.1.
E-Governance Certification Authorities (EGCA)	The EGCA operated by the FPKIMA is authorized by the EAO. The EGCA includes the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to Subscribers. The EGCA is responsible for issuing and managing certificates including: • The certificate manufacturing process; • Publication of certificates; • Revocation of certificates; • Generation and destruction of EGov CA signing keys; and • Ensuring that all aspects of the EGov CA services, operations, and infrastructure related to certificates issued under the [EGCA CP] are performed in accordance with the requirements, representations, and warranties of the [EGCA CP].
E-Authentication Authorizing Official (EAO)	The E-Authentication Authorizing Official (EAO) is responsible for the decision to issue a certificate to particular CSPs, AA servers, Level 1-4 IdPs, Relying Parties, BAE Brokers, or Metadata Signers.
Certificate Status Servers	Certificate Status Servers are not currently supported.

1.3.2 Registration Authorities

The Registration Authority (RA) is the entity that collects and verifies each Subscriber's identity and information that is to be entered into his or her public key certificate. For the EGCA, the E-Authentication Authorizing Official (EAO) collects the registration information and provides that information to the FPKIMA in a *Letter of Authorization (LOA) for Certificate Issuance*. In this way, the EAO acts as the RA for the EGCA. Trusted Roles (Section 5.2.1) perform the functions related to the issuance of a certificate through the practices and procedures throughout the Certificate Lifecycle.

The EGCA RA performs its function in accordance with the procedures in the *E-Governance Trust Services (EGTS) Certificate and Issuance Process* [EGTS Application and Issuance] approved by the EAO. The RA is responsible for:

- Control over the registration process; and
- The identification and authentication process.

RA duties are performed by the EAO and may also be performed as an additional duty by EGCA personnel. The EAO is responsible for the decision to issue a certificate to a

particular approved Subscriber.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate. All EGCA Subscribers are devices. The EGCA CPS limits Subscribers to CSPs, AA servers, Level 1-4 IdPs, Relying Parties, BAE Brokers, and Metadata Signers.

CSPs provide Security Assertion Markup Language (SAML) assertions to AA servers. Subscribers will use these certificates to establish mutually-authenticated Transport Layer Security (TLS) connections to provide authentication, integrity, and confidentiality to the transmission of these SAML assertions.

IdPs, BAE Brokers, and Metadata Signers exchange authentication, attribute, and metadata information with Relying Parties, respectively.

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. For this certificate policy, the Relying Party may be any entity that wishes to validate the binding of a public key to a CSP, AA server, Level 1-4 IdP, Relying Party, BAE Broker, or Metadata Signer. Although the [EGCA CP] contains some helpful guidance, which Relying Parties may consider in making their decisions, Relying Parties are outside the scope of this CPS and are not controlled by the EAO or the FPKIMA.

1.3.5 Other Participants

The EGCA operating under the [EGCA CP] will require the services of other security, community, and application authorities. The Government Information Systems Security Manager (ISSM) is assigned in writing by the appropriate GSA Designated Approving Authority (DAA) and serves as the focal point for overseeing the implementation of adequate security within the system, including ways to prevent, detect, and recover from security problems. These functions are performed through the certification and accreditation process and delegation of tasks to the Information Systems Security Officer (ISSO) (e.g., day-to-day monitoring of the FPKIMA system security).

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

The FPKIMA operates the EGCA as a key critical infrastructure component. The EGCA is intended to support CSPs, AA servers, Level 1-4 IdPs, Relying Parties, BAE Brokers, and Metadata Signers, which have unclassified information and can include sensitive unclassified data protected pursuant to Federal statutes and regulations. Each Subscriber-specific LOA will identify the certificate policy OIDs associated with that Subscriber.

The sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. Organizations must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to

accept based on the sensitivity or significance of the information. Note that the data in such transactions never traverses the FPKI infrastructure. This evaluation is done by each organization for each application and is not controlled by this CPS.

1.4.2 Prohibited Certificate Uses

EGCA Certificates are issued solely to support distribution of authentication information to Federal Government Relying Parties. EGCA certificates are only issued for devices, not for use by human subscribers.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

The FPKIMA is responsible for maintaining this CPS.

1.5.2 Contact Person

Questions regarding this CPS shall be directed to the FPKIMA PM.

1.5.3 Person Determining CPS Suitability for the Policy

This CPS must conform to the corresponding Certificate Policy. The EAO is responsible for asserting whether the EGCA CPS conforms to the [EGCA CP]. This determination of suitability shall be based on an independent compliance auditor's results and recommendations. See Section 8 for further details of the audit requirements.

1.5.4 CPS Approval Procedures

The FPKIMA submits the EGCA CPS and the results of a compliance analysis study to the EAO for approval. The EAO will accept or reject the CPS and accompanying analysis. If rejected, the FPKIMA PM will task the required FPKIMA resources to resolve the identified discrepancies. When the resolutions are documented, a compliance analysis will be conducted and the results resubmitted to the EAO for review and approval.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

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 or behavioral characteristic of a human being.
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.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.

CA Facility	The collection of equipment, personnel, procedures, and structures that are used by a CA to perform certificate issuance and revocation.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to Subscribers.
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.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a Subscriber's postal address, that is not included in a certificate. A CA managing certificates may use this information.
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 Servers	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.
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]

Cross-Certificate	A certificate used to establish a trust relationship between two CAs.
Cryptographic Module	The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation), and is contained within the cryptographic boundary. [FIPS140-2]
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.
EAO	The E-Authentication Authorizing Official (EAO) is responsible for the decision to issue a certificate to particular CSPs, AA servers, Level 1-4 IdPs, Relying Parties, BAE Brokers, or Metadata Signers.
Employee	Any person employed by an Agency as defined above.
FOS	Full Operational Site
FPKI Management Authority (FPKIMA)	The Federal Public Key Infrastructure Management Authority is the organization responsible for operating the FPKI Trust Infrastructure.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding the FPKI Trust Infrastructure.
FPKI Trust Infrastructure	The Trust Infrastructure consists of a collection of PKI components (Certificate Authorities, Directories, Certificate Policies, and Certificate Practice Statements) that are used to implement the Federal PKI.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Information System Security Officer (ISSO)	Person responsible to the Designated Approving Authority for ensuring the security of an IS throughout its life-cycle, from design through disposal. [NS4009]
Information System Security Manager (ISSM)	Individual responsible for a program, organization, system, or enclave's information assurance program

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 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.
Letter of Authorization	Written instructions signed (manually or digitally) by the EAO to issue a certificate to a Subscriber.
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.
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 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).
PKCS#7	Public Key Certificate Standard Response.
PKCS#10	Public Key Certificate Standard Certificate Request.

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 CPS; 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.

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.
Sponsor	Fills the role of a Subscriber for nonhuman system components that are named as public key certificate subjects and is responsible for meeting the obligations of Subscribers as defined throughout this CPS.
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. All EGCA subscribers are devices.
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]
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."
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.
Validity period	Time span during which each key setting remains in effect.

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 140]

1.6.2 Acronyms

AA	Agency Application
BAE	Backend Attribute Exchange
BMS	Building Management System
CA	Certification Authority
CARL	Certification Authority Revocation List
CD	Compact Disc
CIO	Chief Information Officer
CISA	Certified Information System Auditor
CM	Configuration Management
CP	Certificate Policy
CPS	Certification Practice Statement
CPWG	Certificate Policy Working Group
CRL	Certificate Revocation List
CSP	Credential Service Provider
CSS	Certificate Status Server
DAA	Designated Approving Authority
DISP	Directory Information Shadowing Protocol

DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name System
DOFF	Designated Official For Facilities
DSA	Directory System Agent
EAO	E-Authentication Authorizing Official
EDP	Electronic Data Processing
EGCA	E-Governance Certificate Authority
FBCA	Federal Bridge Certification Authority
FERTL	Facility Emergency Response Team Leader
FIPS	(U.S.) Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FPKI	Federal Public Key Infrastructure
FOS	Full Operational Site
FPKIMA	Federal Public Key Infrastructure Management Authority
FPKIPA	Federal Public Key Infrastructure Policy Authority
FTCA	Federal Tort Claims Act
FTP	File Transfer Protocol
GSA	General Services Administration
GTM	Global Traffic Manger

GUI	Graphic User Interface
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
HVCA	Heating, Ventilation and Air Conditioning
IETF	Internet Engineering Task Force
ICAMSC	Identity, Credential and Access Management Subcommittee
IdP	Identity Provider
IP	Internet Protocol
IS	Information System
ISC	Individual Secure Container
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ISSM	Information Systems Security Manager
LDAP	Lightweight Directory Access Protocol
LOA	Certificate Issuance Authorization Letter, otherwise known as a Letter of Authorization
MOU	Memorandum of Understanding
N/A	Not Applicable
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology

NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OEP	Occupant Emergency Plan
OID	Object Identifier
OJT	On-The-Job-Training
OMB	Office of Management and Budget
OS	Operating System
PACS	Physical Access Control System
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509

[*Redacted for Security Purposes*]

PM	Program Manager
POC	Point of Contact

[*Redacted for Security Purposes*]

RA	Registration Authority
RFC	Request For Comments

RSA	Rivest-Shamir-Adleman (encryption algorithm)
SA	Stand Alone
SAML	Security Assertion Markup Language
SBU	Sensitive But Unclassified
SC	Secure Container
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SHA-256	Secure Hash Algorithm, 256 bit length
SKI	Subject Key Identifier
SOP	Standard Operating Procedures
SSP	System Security Plan
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOC	Trusted Operations Center
UPS	Uninterruptable Power Supply
URI	Uniform Resource Identifier
USB	Universal Serial Bus
U.S.C.	United States Code
USPS	United States Postal Service

WWW	World Wide Web

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

2.1.1 EGCA Repository Obligations

The FPKIMA operates and uses a variety of mechanisms for posting information into a repository as required by the [EGCA CP]. The mechanisms supported and operated include:

- Maintaining an online web server which allows anonymous access and retrieval of certificate information via HTTP, including all EGCA root certificates and CRLs;
- Maintaining an online X.500 Directory Service System supporting Lightweight Directory Access Protocol (LDAP) v3, as directed by the EAO, which allows anonymous access and retrieval of all EGCA certificates and CRLs. This directory may optionally contain Subscriber certificates in accordance with Agency policy; and
- Providing administrative access control mechanisms when needed to protect repository information.

2.2 PUBLICATION OF CA INFORMATION

2.2.1 Publication of Certificates and Certificate Status

The FPKIMA publishes information concerning the EGCA necessary to support its use and operation in the repositories described in section 2.1. This includes

- The CRLs it issues; and
- The Certificate for its certificate signing key.

These repositories are available for anonymous access 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.

The FPKIMA publishes certificates issued by the EGCA, when they are issued, in the EGCA directory entry of the FPKI X.500/LDAP directories.

The FPKI repositories include a web server providing HTTP access to EGCA CA certificates and CRLs.

CRLs are published to both the FPKI X.500/LDAP directories and the FPKI web server when they are issued.

The availability requirements are met by the FPKIMA operating multiple sites with load balanced network traffic between the sites and multiple servers at each site available within the local load balanced pool.

2.2.2 Publication of CA Information

The FPKIMA will deliver the EGCA CPS to the EAO and any relevant authority in the Federal government. It will make a redacted version of the EGCA CPS publicly available on the FPKIPA web site.

Information, clearly "about critical infrastructure that could be used to develop an attack on U.S. assets, disrupt emergency response activities, or otherwise compromise the security of Federal facilities and persons in those facilities"[1] is omitted in the universally available public version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know. The FPKIPA maintains a web server, separate from the repositories maintained by the FPKIMA, to post FPKI-related documentation, including the CP, the redacted CPS, and FPKIPA procedural documents.

2.3 FREQUENCY OF PUBLICATION

Certificates issued to Subscribers are published in the issuing CA directory entry of the FPKI Directory when they are issued. The CRL is published as specified in Sections 4.9.7 and 4.9.12.

Updates to the EGCA CP are made by the EAO and published to the FPKIPA web site. Review and updates, if appropriate, are made to this CPS on an annual basis and are provided to the EAO for approval. After approval, a redacted version of this CPS is provided to the FPKIPA for publication.

2.4 ACCESS CONTROLS ON REPOSITORIES

The FPKI online repositories reside behind a firewall protecting the FPKI from the Internet. Public anonymous read access to the Directory and web Servers is allowed. Only authorized FPKIMA personnel (Trusted Roles) can update the information stored on these servers. Access controls are set by administrative function and assigned roles/responsibilities, and enforced using password-based authenticated subject identity.

The EGCA is enabled to generate periodic CRLs. EGCA CRLs are pushed to the online FPKI directory through the internal one-way firewall. Directories are protected from unauthorized modification, requiring authorized authentication in order to make updates. Anonymous read access is provided via LDAP (port TCP/389) and HTTP (port TCP/80) to the public.

[1] (GSA Order 1800.3b and Draft GSA Order 1800.3c), and in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002) §3544(A)(1)(a)(i), §3544(A)(1)(a)(ii), §3544(A)(2)(a), §3544(A)(2)(b), and §3545(f), as well as GSA Orders 1800.3C (draft) and PBS 3490.1

Table 2.4-1 provides network addresses for the Repository for the FPKI system:

Table 2.4-1 FPKI Repository Addresses

Purpose	Network Address
LDAP v2 or better	LDAP access to repositories is: ldap.fpki.gov (port 389)
EGCA Repository website	HTTP access to repositories begins with: http.fpki.gov (port 80) see http://www.idmanagement.gov/fpkima/documents/fpki_gov_sitemap.pdf for the full URLs for all HTTP access.

Table 2.4-2 lists the FPKIPA website that hosts the EGCA CP, redacted CPS, and Interoperability Guidelines:

Table 2.4-2 FPKIPA Website

Purpose	Network Address
EGCA CPS Website	http://www.idmanagement.gov/fpkipa/
EGCA CP Website	http://www.idmanagement.gov/fpkipa/

Access to the entire CPS is granted only to Entities authorized by the FPKIPA or EAO. The procedure for updating the documents on the web server consists of an out-of-band mechanism.

3 IDENTIFICATION AND AUTHENTICATION

This Section contains the practices the FPKIMA follows in registering, identifying, and authenticating AA Owners and CSPs and Sponsors involved in the certification request process. A Subscriber registration to the EGCA is initiated by an application submitted to the EAO by the Sponsor.

This application is done by following a checklist and completing a form that is sent to the EAO for review, assessment, and evaluation. Among other things, the application contains how the applicant Sponsor proposes to demonstrate compliance with the selected policy requirements along with the required substantiating documentation.

The EAO is responsible for evaluating the application and works with the applicant organization to complete the assessment. Once the assessment and evaluation phase is successfully completed and accepted the EAO will instruct the FPKIMA, by way of an LOA, to create and issue the appropriate certificate(s) to the accepted applicant Subscriber.

3.1 NAMING

3.1.1 Type of Names

The EGCA only generates and signs certificates that contain a non-null subject Distinguished Name (DN).

The EGCA generates and signs certificates where the issuer DN matches the DN of the CA identified in the LOA from the FPKIPA and the subject DN matches both the subject DN identified in the LOA and in the certificate request (PKCS#10) received from the applicant Sponsor. The EGCA shall include X.501, *Information Technology – Open Systems Interconnection – The Directory: Models*, distinguished names in the subject DN of certificates according to the distinguished name information provided in the certificate request. These distinguished names shall be a geo-political name.

Subscriber 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.

Certificates issued by the EGCA will contain one of the following issuer DNs:

- cn=eGovernance App CA,ou=FPKI,o=U.S. Government,c=US
- cn=eGovernance CSP2 CA,ou=FPKI,o=U.S. Government,c=US
- cn= eGovernance Trust Services CA,ou=FPKI,o=U.S. Government,c=US

The LOA provided by the EAO and the PKCS#10 request received from the Sponsor will

contain the name to be used as the subject of the certificate issued by the EGCA and the Trusted Roles will verify that the DN specified in the LOA matches the DN received in the PKCS#10 .

The LOA may additionally specify email addresses, Internet Protocol (IP) Addresses or Uniform Resource Identifiers (URI) to be included as one or more subjectAltNames.

3.1.2 Need for Names to be Meaningful

Names used in the EGCA certificates identify the Subscriber in a meaningful way and are created by the applicant and vetted by the EAO. The Sponsor requests the name in their certificate request, and the EAO states that they are in agreement that the name identifies the Subscriber in a meaningful way, by including it in the LOA issued to the FPKIMA.

3.1.3 Anonymity or Pseudonymity of Subscribers

The EGCA does not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501.

3.1.5 Uniqueness of Names

Sponsors are responsible for creating meaningful names that uniquely identify their Subscribers.

The EAO manages the name uniqueness for certificates issued by the EGCA, by assuring the names provided by the Sponsor appropriately identifies the relationship with the Subscriber.

The EAO establishes name space control procedures for names assigned to Subscribers to ensure name collisions do not occur.

The EGCA 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.

3.1.6 Recognition, Authentication and Role of Trademarks

[EGCA CP] makes no stipulation for trademarks; however, the EGCA will not issue a certificate knowing that it infringes the trademark of another. The EAO resolves any disputes involving names and trademarks.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

The FPKIMA requires that the Subscriber prove possession of the private key that corresponds to the public key in the certificate request. This will be accomplished by the Subscriber using its private key to sign the public key in a certificate request. Alternate methods require approval of the EAO and require that any other mechanisms used are at

least as secure as those cited here. The subject key identifier (SKI) is also supplied by the Sponsor, and the FPKIMA verifies that the supplied SKI matches the one in the certificate request (PKCS#10).

3.2.2 Authentication for Organization Identity

The EGCA issues certificates as authorized by the EAO. The EAO verifies the identity and POC information for the individual(s) identified to be the Sponsor for the device certificate to be issued. This information will be verified with the individual(s) who applied for the certificate and participated in the test phases as described in [EGTS Application and Issuance]. In the case of a request for a new certificate for a device with an existing certificate from the EGCA (e.g. before the existing certificate's expiration, for a rekey), the EAO verifies the POC identity information for the new certificate with the current Sponsor of the existing certificate.

3.2.3 Authentication of Individual Identity

Computing and communications devices (e.g., routers, firewalls, servers) 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

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 LOA issued by the EAO. The content of the LOA shall be verified by the EAO with the individual(s) who participated in the testing phase of the [EGTS Application and Issuance] process, or with the currently-registered Sponsor.

The FPKIMA shall confirm the Sponsor is listed as a point of contact (POC) on the LOA before certificate issuance.

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

- Equipment identification (i.e., DNS name);
- Equipment public keys; and
- Contact information to enable the EGCA to communicate with the Sponsor when required.

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.

Information provided in certificate requests shall be recorded by the FPKIMA if it is not documented in the LOA.

3.2.4 Non-verified Subscriber Information

All information included in certificates issued by the EGCA will be verified against information provided in the LOA, or is received from the Sponsor in the PKCS#10.

3.2.5 Validation of Authority

The EAO validates the individual's authority to act in the name of the organization. The FPKIMA coordinates only with individuals listed as authorized POCs on the LOA when issuing certificates.

3.2.6 Criteria for Interoperation

The EAO determines the interoperability of Subscribers approved for certificate issuance.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

EGCA certificate re-key shall follow the same procedures as initial certificate issuance, described in Section 3.2. However, if the device is the same, testing may not be required and the EAO will verify authorized individuals with the current Sponsor.

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.

3.3.2 Identification and Authentication for Re-Key after Revocation

EGCA requires an initial registration process as defined in Section 3.2 in the event of issuing a certificate after revocation of a certificate for the same Subscriber.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The EGCA will revoke certificates issued to Subscribers only upon explicit request from the FPKIPA, the Sponsor of the certificate, or EAO. The [EGCA CP] requires that revocation requests be authenticated. Digitally-signed revocation requests that can be authenticated are accepted.

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. Revocation requests can also be authenticated by the FPKIMA contacting the authorized POC for the Subscriber using other contact information from the LOA that authorized the certificate in question.

4 CERTIFICATE LIFE-CYCLE MANAGEMENT REQUIREMENTS

4.1 CERTIFICATE APPLICATION

An applicant requesting a certificate from the EGCA submits an application to the EAO in accordance with the [EGTS Application and Issuance]. If the applicant successfully passes the required processes, the EAO authorizes the FPKIMA to issue a certificate to the applicant by issuing a signed LOA. Prior to issuing a certificate from the EGCA, the FPKIMA Administrator will have:

- A completed and signed LOA from the EAO indicating the applicant has been authorized to receive a certificate. The LOA will provide authorized point of contact information for individuals authorized to represent the Subscriber; and
- Received a PKCS#10 (certificate request from an authorized Sponsor.)

All communications between trusted roles and the applicant Sponsor supporting the certificate application and issuance process is via an out-of-band secure mechanism such as FedEx, Secure File Transfer Protocol (SFTP) or by digitally-signed email or digitally-signed PDF documents. When FedEx or other physical means of transit are used, tracking numbers are exchanged via email or telephone.

4.1.1 Submission of Certificate Application

The representative identified in the LOA applies for certificates to the EAO.

4.1.2 Enrollment Process and Responsibilities

All communications supporting the certificate application and issuance process is authenticated and protected from modification. Any electronic transmission of shared secrets shall be protected. Communications may be via digitally signed email, SFTP, or out-of-band.

Sponsors are responsible for providing accurate information on their certificate applications.

4.2 CERTIFICATE APPLICATION PROCESSING

EGCA will only issue a certificate to a single Subscriber. Certificates shall not be issued that contain a public key whose associated private key is shared by multiple Subscribers. Where multiple Subscribers 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.

All authorization and other attribute information received from an applicant Sponsor shall be verified against the LOA before inclusion in a certificate. The EAO is responsible for verifying prospective Subscriber data with the authorized POC before issuing the LOA.

4.2.1 Performing Identification and Authentication Functions

The EAO performs the identification and authentication of the applicant while evaluating the applicant's business case to determine if the certificate request is in the interest of the Federal Government. The EAO provides an LOA to the FPKIMA containing POC information for the applicant Sponsor and other authorized individuals. The FPKIMA only corresponds with those individuals listed on the LOA using POC information obtained from the EAO.

4.2.2 Approval or Rejection of Certificate Applications

The EAO may approve or reject a certificate application, following the procedures in [EGTS Application and Issuance]. If the application is accepted, the EAO works with the individual(s) from the applicant organization who participated in the application and issuance process to obtain the correct POC information (to include an LOA and to identify the individual who is named the Sponsor for the requested device certificate). The EAO informs the applicant Sponsor of their responsibilities and obtains a signed subscriber agreement from the Sponsor.

4.2.3 Time to Process Certificate Applications

The EGCA will process and issue certificate within 30 days of identity verification and the receipt of an LOA from the EAO.

4.3 ISSUANCE

4.3.1 EGCA Actions during Certificate Issuance

Upon receipt of a request, the FPKIMA issues certificates by the following procedure:

1. Subscriber public keys are delivered to the FPKIMA electronically in a digitally-signed certificate request (i.e., using PKCS#10) message to the FPKIMA via secure non-electronic means (e.g., CD delivered by registered mail or courier) or via digitally-signed email or SFTP.
2. The identity of the requestor is verified against the POC information in the LOA.
3. The integrity of the information in the certificate request is verified by comparing it with the information specified in the LOA.
4. Proof of possession of the private key is accomplished when the EGCA software verifies the signature on the PKCS#10 and the SKI in the PKCS#10 is compared to the SKI provided by the Sponsor.
5. If all certificate requirements have been met, a certificate is built and signed.
6. The certificate issued by the EGCA will be delivered to the requestor in a signed response message (PKCS#7), via secure non-electronic means (e.g., CD delivered by registered mail or courier) or via SFTP or digitally-signed email.

The EGCA will not issue certificates to other CAs. Self-issued certificates to manage transitions (e.g., to new CA key pairs) are permitted. Only the EGCA is permitted to assert these policies in certificates.

4.3.2 Notification to Subscriber of Issuance of Certificate

The FPKIMA delivers the EGCA Root Certificate to the Subscriber along with the newly-issued certificate via out-of-band courier mechanism or via SFTP or digitally-signed email.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct constituting Certificate Acceptance

For the EGCA, failure to object to the requested certificate or its contents constitutes acceptance of the certificate.

4.4.2 Publication of Certificate by EGCA

Certificates issued by the EGCA are published in repositories, unless the Subscriber requests their certificates be excluded from publication.

4.4.3 Notification of Certificate Issuance to Other Entities

The FPKIMA notifies the EAO by email whenever a certificate is issued.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key is specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2 Relying Party Public Key and Certificate Usage

The EGCA issues CRLs specifying the current status of all unexpired certificates.
The public key of the CA must be available for certification trust paths to be created and verified. In general, CA certificates are published in the public repository and the verification of public keys is performed using X.509 path validation.

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

4.6 CERTIFICATE RENEWAL

Certificate renewal consists of issuing a new certificate with a new validity period and serial number. Subscriber certificates issued by EGCA are only renewed during recovery from CA key compromise.

4.6.1 Circumstance for Certificate Renewal

The EGCA will not renew Subscriber certificates except during recovery from CA key compromise. In such cases, the renewed certificate shall expire as specified in the original Subscriber certificate.

The EGCA may automatically renew certificates during recovery from key compromise.

4.6.2 Who may request Certificate Renewal

EGCA certificates may not be renewed except as specified in Section 4.6.1.

4.6.3 Processing Certificate Renewal Requests

The EGCA processes the renewal requests only during recovery from CA key compromise. A PKCS#10 certificate request for a certificate renewal from a Sponsor must be accompanied by a new LOA from the EAO and will be treated as a request for a new certificate.

4.6.4 Notification of new Certificate Issuance to Subscriber

The EGCA informs the Sponsor of the issuance of a new certificate by sending them the certificate using secure means such as FedEx or secure mail.

4.6.5 Conduct constituting acceptance of a Renewal Certificate

For certificates issued by the EGCA, failure to object to the renewal of the certificate or its contents constitutes acceptance of the certificate.

4.6.6 Publication of the Renewal Certificate by EGCA

The EGCA publishes certificates in repositories as specified in Section 4.4.2.

4.6.7 Notification of Certificate Issuance by EGCA to other entities

The EGCA notifies the EAO whenever a certificate is issued. The new certificate is sent to the Sponsor in the same manner as with the issuance of a new certificate.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificates with a different public key and serial number while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. After certificate re-key, the old certificate is revoked.

A request for a certificate due to a re-key is treated as a request for a new certificate and must be accompanied by an LOA.

4.7.1 Circumstance for 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, and perform the initial registration identification process defined in Section 3.1.

4.7.2 Who may request certification of a new public key

The EGCA considers requests for certification of a new public key as follows:

- For Subscriber certificates, the human Sponsor may request certification of a new public key.

4.7.3 Processing Certificate Re-key Requests

Subscriber re-key requests shall be processed using the same process used for initial certificate issuance, described in Section 4.3.

4.7.4 Notification of new Certificate Issuance to Subscriber

The new certificate is sent to the Sponsor in the same manner as with the issuance of a new certificate.

4.7.5 Conduct constituting acceptance of a Re-keyed Certificate

For certificates issued by the EGCA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.7.6 Publication of the Re-keyed Certificate by EGCA

The EGCA publishes re-keyed certificates in a repository as specified in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by EGCA to other entities

The EGCA notifies the EAO whenever a certificate is issued. The new certificate is sent to the Sponsor in the same manner as with the issuance of a new certificate.

4.8 MODIFICATION

Modifying 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.

A request for certificate modification is treated as a request for a new certificate and must be accompanied by an LOA, except when the modification is to correct an error in the certificate.

After certificate modification, the old certificate is revoked.

4.8.1 Circumstance for Certificate Modification

EGCA may modify a Subscriber certificate whose characteristics have changed (e.g. assert new subjectAltName) by performing the initial registration identification process defined in Section 3. The new certificate may have the same or a different subject public key.

4.8.2 Who may request Certificate Modification

The human Sponsor may request certificate modification for Subscriber certificates. The FPKIMA may request certificate modification when an error is discovered in a current certificate.

4.8.3 Processing Certificate Modification Requests

Proof of all subject information changes must be provided to the EAO or other designated agent and verified before the modified certificate is issued.

The FPKIMA will verify authorization of the request with the EAO and verify the

certificate information with the information supplied on the LOA.

4.8.4 Notification of new Certificate Issuance to Subscriber

Subscribers are notified of certificate issuance as described in Section 4.3.2.

4.8.5 Conduct constituting acceptance of a Modified Certificate

For certificates issued by the EGCA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.8.6 Publication of the Modified Certificate by EGCA

The FPKIMA publishes modified certificates in a repository as specified in Section 4.4.2.

4.8.7 Notification of Certificate Issuance by EGCA to other entities

The FPKIMA notifies the EAO whenever a certificate is issued.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

EGCA issues CRLs covering all unexpired but revoked certificates issued under this policy.

EGCA certificates contain URLs to find CRLs, which provide revocation information for the certificates they issue. The EGTS Subscriber Agreement states how describes Sponsors can request revocation of certificates. [EGTS Application and Issuance] shall be given to the Sponsor during certificate request or issuance, and shall be readily available to any potential Relying Party.

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

Certificate suspension is not allowed by the EGCA policy.

4.9.1 Circumstance for Revocation

EGCA certificates are 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 include the following:

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

- Certificate superseded.

4.9.2 Who can request Revocation

Under the circumstances described in 4.9.1, the following individuals may authorize immediate certificate revocation:

- The Sponsor or other authorized individuals identified on the LOA for that certificate;
- Chair of the FPKIPA;
- Co-chairs of the ICAMSC;
- FPKIMA PM; and
- The EAO.

The EAO shall review and submit a report to the FPKIPA about the emergency revocation as soon as practical.

4.9.3 Procedure for Revocation Request

When the revocation request is not due to a perceived emergency, the revocation can be at a time mutually-agreed upon by the Sponsor (or authorized official), the EAO, and the FPKIMA.

The FPKIMA will review all revocation requests to ensure that the revocation requests are legitimate and will then revoke the certificate, as follows:

1. An authorized official (listed in Section 4.9.2) sends a written request to revoke a certificate via signed e-mail to FPKIPA-MA@listserv.gsa.gov identifying the certificate to be revoked and explaining the reason for revocation. The individual may notify the FPKIMA Administrative/Help desk via phone as well.
2. Upon receipt of a signed revocation request, the FPKIMA authenticates the request by verifying the digital signature and making direct contact (call back or challenge/response telephone conversation) with the EAO POC.
3. The EAO evaluates and verifies the need for revocation expressed in the authenticated request. If the revocation request appears to be valid, the EAO will direct the FPKIMA to proceed with revocation or designate a time at which the revocation should take place.
4. The FPKIMA revokes the certificate, which automatically generates and adds a CRL entry for that certificate within 6 hours of notification of approval by the EAO or at the designated time.
5. The FPKIMA ensures the new CRL is posted in the FPKI repository within 6 hours of notification of approval by the EAO or of the designated time.

The FPKIMA may revoke a certificate prior to receiving approval from the EAO by following emergency revocation procedures consisting of the following steps:

1. Notify all identified POCs in the emergency list of FPKI (i.e., EAO, FPKIMA POC, affected Subscriber POC). This can be done by either:

- Telephone (using one of call-back or challenge/response protocols);
- Signed FAX; or
- Signed e-mail.

2. Revoke the certificate and post the new CRL.

Once the incident has been investigated and documented, a new certificate to replace the one that has been revoked may be issued, if directed by the EAO.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under the [EGCA CP]. The EGCA will revoke certificates as quickly as practical upon receipt of a proper revocation request or at a specified time agreed to by the FPKIMA, the EAO, and the Sponsor. When the revocation request is due to a compromise, the request will be processed before the next CRL is published, except for those requests received within 2 hours of CRL issuance. Revocation requests for compromise received within 2 hours of CRL issuance are processed before the following CRL is published.

4.9.5 Time within which CA must process Revocation Request

EGCA will revoke certificates as quickly as practical upon receipt of a proper revocation request or at a specified time agreed to by the FPKIMA, the EAO, and the Sponsor. Revocation requests shall be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published. In the case of non-emergency revocation requests, the revocation may take place at an agreed upon time.

4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

When FPKIMA personnel validate digital signatures on emails or PDFs, current CRLs are checked.

4.9.7 CRL Issuance Frequency

CRLs are issued twice daily, even if there are no changes to be made, to ensure timeliness of information. The location of revocation information is found in the crlDistributionPoint extension of every certificate issued from the EGCA to the Subscribers. Certificate status information is posted within 6 hours of notification of approval of revocation (as a result of suspected key compromise) or immediately in accordance with emergency revocation procedures. The previous CRL is removed and replaced with the updated CRL.

The EGCA issues CRLs every 12 hours with an 18 hour nextUpdate field.

4.9.8 Maximum Latency of CRLs

There are automated processes running to post CRLs when generated to the FPKI repositories. CRLs are posted initially to the Master Directory System Agent (DSA) at each Full Operational Site (FOS) and then using X.500 Directory Information Shadowing Protocol (DISP) are shadowed to all publicly-available DSAs. On each public DSA server there is a cron job running that pulls current CRLs from its local DSA and updates the local web server location for HTTP access.

If a security incident has occurred that prevents new CRLs from being published to all repository sites before the nextUpdateTime of the previous CRLs, the FPKIMA will notify the FPKI community by sending a digitally-signed email to the appropriate POCs.

4.9.9 On-Line Revocation/Status Checking Availability

On-line status checking is not supported for the EGCA.

4.9.10 On-Line Revocation Checking Requirements

On-line status checking is not supported for the EGCA.

4.9.11 Other Forms of Revocation Advertisements Available

EGCA does not employ other methods to publicize the certificates it has revoked.

4.9.12 Special Requirements Related to Key Compromise

When an EGCA certificate is revoked or Subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL is issued as soon as possible and always within 18 hours of notification.

If one of the EGCA keys is compromised, the FPKIMA will notify the EAO, the FPKIPA and all EGCA Subscribers. The compromised root certificate will be added to the CRL and a CRL either with no nextUpdateTime or a nextUpdateTime past the expiration time of the certificate will be posted.

If directed by the EAO a replacement CA root certificate and key pair will be generated and all Subscribers of the compromised CA will be issued new certificates. The new root certificate and new Subscriber certificates will be securely distributed to all authorized Sponsors.

4.9.13 Circumstances for Suspension

Certificate suspension is not allowed by the EGCA.

4.10 CERTIFICATE STATUS SERVICES

The FPKIMA does not support Certificate Status Services for the EGCA.

4.11 END OF SUBSCRIPTION

Certificates are removed from the FPKI repository after their expiration date.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

EGCA private keys are never escrowed. The EGCAs do not generate Public/private key pairs on behalf of the subscriber; therefore the EGCA is never in possession of Subscriber private keys.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Subscriber keys are generated by the Subscriber and therefore are never in the possession of the EGCA.

5 FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

The FPKIMA imposes physical security requirements that provide the protections specified below. All physical control requirements apply to the EGCA.

The FOS-W and FOS-E sites both adhere to the [NIST SP 800-53] Physical and Environmental controls commensurate with the impact level of the FPKI Trust Infrastructure, which include control of physical access points to the facility where the information system resides and verifying individual access authorizations before granting access to the facility.

For FOS-E, the facility Network Operations Center (NOC) immediately notifies the FPKIMA team in the event of any incident that could impact facility operations or procedures, or the operation of the FPKI. For FOS-W, the facility management immediately notifies the FPKIMA team in the event of any incident that could impact facility operations or procedures, or the operation of the FPKI.

The CA is protected from unauthorized access while the cryptographic module is installed and activated. The cryptographic module activation information is stored in the Officer's individual secure containers (ISC). By design, all CA equipment stays activated, but is stored in the safe when the equipment is not activated (e.g., when equipment is damaged or inoperable). Inoperable or damaged equipment that cannot be stored in the safe will remain in the locked CA cabinet until it is either restored to operation on site, or sanitized and shipped out for service or disposal.

The EGCA equipment is housed in a locked cabinet located in a locked room. In FOS-W, a video camera records access to the FPKI computer room. The camera is connected to a video recorder located in a locked cabinet. Only an Officer can unlock the cabinet, but an Administrator is required to provide access to the FPKI computer room.

5.1.1 Site Location and Construction

The FPKI FOS-W Site is a [*Redacted for Security Purposes*]. The FOS-W Site is located at:

[*Redacted for Security Purposes*]

GSA issues badges to all FPKIMA personnel, either PIV cards, standard swipe badges [*Redacted for Security Purposes*], or both. FPKI Trusted Roles, the ISSO, and the PM are granted authorization for building access through a dedicated FPKI PACS system. Only FPKI Administrators, the ISSO, and the PM are granted server room access through that same FPKI-controlled PACS system. All other personnel must be accompanied by an Administrator, and must sign a Visitor or Personnel Sign-in Log.

The FPKI FOS-E Site is a [*Redacted for Security Purposes*]. The FOS-E Site is located at:

[*Redacted for Security Purposes*]

At all times, all personnel gaining access to the facility must pass through the building's security checkpoint. FPKIMA personnel receive [*Redacted for Security Purposes*] badges. Only Administrators, the ISSO, and the PM have access to keys for the locked cages housing the FPKI systems.

These sites are consistent with facilities used to house high-value, sensitive information consistent with the required physical access controls described in FPKI Security Controls Profile of Special Publication 800-53, Security Controls in PKI Systems [FPKI Security Profile].

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

The EGCA equipment is always protected from unauthorized access. Physical access controls are implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

Physical and environmental protection policies and procedures have been developed and documented, and are reviewed and updated biennially in accordance with the physical and environmental protection security controls outlined in [NIST SP 800-53]. See the *FPKI Trust Infrastructure System Security Plan* [FPKI SSP], "Physical and Environmental Protection" security control section for more details.

The EGCA is secured in a two-person control manner. A locked cabinet/rack houses the EGCA Server. The two-person control is attained by separation of access responsibilities: An Administrator has access to the room, while an Officer has access to the locked rack. The combination of the two individuals is required to access the critical system, providing two-person control. The Trusted Roles present whenever the CA rack is accessed sign the "secure rack access list" which is checked by the auditor during the weekly audits and retained as part of the logs available during the annual PKI Compliance audit. The keyboard-video-mouse (KVM) that is used to access the EGCA server is also housed in a locked cabinet/rack which requires the same two-person control. [*Redacted for Security Purposes*] Both the Administrator and Officer must remain in the room while access to the CA is unlocked. The Officer is never left in the FPKI Computer Room without an escort.

The Administrator and at least one Officer are required to enable the [*Redacted for Security Purposes*] for use with the CAs, thereby providing multi-person control.

Only designated FPKI roles, such as the ISSO, System Owner, Administrators and Operators have unescorted access to the room. All access into, and out of, the FPKI room is recorded in a manual log. The persons accessing the EGCA record the event in

both the FPKI room access log and in the FPKI rack access log(s). In addition, a digital video recorder at FOS-W will record anyone entering the room. The PACS system at FOS-W logs card swipes for both room entry and exit.

Access to the EGCA and private signing keys requires multi-person access. When not in use, the [*Redacted for Security Purposes*] is stored in an onsite safe. There are three secure containers used in the FPKI operations: the onsite secure container (SC) 1 at the FOS-W facility, the onsite secure container (SC2) at the interim offsite facility, and the onsite secure container (SC3) at the FOS-E facility. Only the Administrator, Operator and the ISSO have access to the secure containers (SC1 and SC3). The combination to the offsite secure container (SC2) at the Interim offsite facility is known only to the FPKIMA Auditor and ISSO.

[*Redacted for Security Purposes*] The ISSO is responsible for assigning ISCs and USB flash drives to the Officers. (See Section 6.4.2)

The FPKIMA Administrator and the Operator have access to the FOS secure containers (SC1 and SC3) for backup tapes and the Administrator secure flashdrive.

SC2 is the short-term archive container that stores audit log files (manual and digital) prior to moving them to long-term archival. Only the FPKIMA Auditor has the combination to secure container SC2, however it is housed in a room only accessible to the FPKIMA Administrators.

Only designated FPKI roles, the Administrators, ISSO and FPKIMA PM have unescorted access to the FPKI computer room. Only the Officers and ISSO have access to the locked cabinet/rack. Therefore, EGCA maintenance is under two-person control (i.e., one unescorted role and one Officer).

The separation of roles and physical allocation is summarized in Table 5.1-1.

Table 5.1-1. EGCA Multiple Person Control Access Matrix

Physical Security						**Electronic Security**	
EGCA Role	**Room Access Onsite & Backup**	**Secured Container Access (SC1, SC2, SC3)**	**CA Locked Rack Access**	**Individual Secured Container Access**		**[*Redacted for Security Purposes*] Account**	**CA Account**
ISSM	Escorted						
ISSO	Unescorted	All three SCs	X	X			
Auditor	Escorted	Interim SC					
Officer	Escorted		X	X			X

Physical Security						Electronic Security	
EGCA Role	**Room Access Onsite & Backup**	**Secured Container Access (SC1, SC2, SC3)**	**CA Locked Rack Access**	**Individual Secured Container Access**		**[*Redacted for Security Purposes*] Account**	**CA Account**
Administrator	Unescorted	FOS SCs				X	
Operator	Unescorted	X				X	

At least two individuals are assigned for each FPKI Trusted Role, Auditor, Officer and Administrator. The Officer is the only FPKI role that has access to the EGCA signing functions, and must be accompanied by an Administrator.

Automatic logs are generated each time the CA is started, an entity connects (or unsuccessfully attempts to connect) to the CA, or the private signing keys are used.

[*Redacted for Security Purposes*]

[*Redacted for Security Purposes*] Normally, all CA equipment stays activated. If the CA equipment must be inactive (e.g., when equipment is damaged, inoperable) it is stored in the safe. Inoperable or damaged equipment that cannot be stored in the safe will remain in the locked CA cabinet until it is either restored to operation on site, or sanitized and shipped out for service or disposal.

The EGCA require M of N authentication to start the software user interface that issues or revokes certificates. The activation data is a [*Redacted for Security Purposes*] token split into multiple parts with the number of parts being greater than the number of Officers. Two (2) parts are required for activation. Each Officer is given one part of the [*Redacted for Security Purposes*], which is stored as a file on Federal Information Processing Standard (FIPS) 140-2 Level 3 validated USB Flash Drives stored in ISCs, which are stored in onsite safes when not in use. The last part is given to the Administrators. Per FPKIMA policy, both an Administrator and an Officer must provide their piece of the [*Redacted for Security Purposes*] and a password for that file in order to activate the user interface to the EGCA user interface (i.e., EGCA [*Redacted for Security Purposes*]).

[*Redacted for Security Purposes*]

Administrators perform a security check of the facility and complete a Facility Exit Checklist, ensuring all systems are operating in the appropriate state, and all sensitive material have been secured appropriately before the last authorized individual leaves the FPKI computer room. The Administrator performing the check signs the Facility Exit Checklist.

5.1.2.2 Physical Access for RA Equipment

The EGCA does not have an RA application.

5.1.2.3 Physical Access for CSS Equipment

The EGCA does not have any CSS Equipment.

5.1.3 Power and Air Conditioning

Both facilities have backup power that will allow the FPKI Trust Infrastructure CAs and Repositories to continue operating in case power to the facility is interrupted. The backup power will keep the FPKI Trust Infrastructure CAs and Repositories functioning until commercial power is restored. If commercial power will be unavailable longer than the backup power capacity, the facility will notify the FPKIMA with enough time to allow trusted roles to travel to the site and affect an orderly shutdown of the equipment.

FOS-W: The facility is connected to multiple Uninterruptable Power Supply (UPS) systems, which protect the servers from power surges, and, in the event of a power outage, keeps the servers powered long enough for the diesel generators to turn on and start supplying power to the server room equipment. The diesel generators should start up within a matter of minutes of a power outage.

The following procedures or controls are in-place to regulate temperature:

- Temperature and humidity are monitored and controlled by four systems each with their own UPS battery backup, and can receive power from the generators;
- All four of the systems have temperature set points of 70° Fahrenheit (° F) with an allowed variance of plus or minus 5° F; and
- All four systems have humidity set points of 40 percent with an allowed variance of plus or minus 5 percent.

All of the temperature and humidity controls are integrated into an OpenView alert system. This alerts facility administrators to shifts in temperature or humidity outside the specified range.

FOS-E: The data center is connected to multiple UPS systems that provide temporary backup power in the event of a power failure at the FOS-E site. UPS systems will keep the servers powered long enough for the local generators to turn on and start supplying power to the server room equipment. There are Service Level Agreements in place to ensure the UPS devices are inspected and maintained on a quarterly, semi-annually and annually by a third party vendor. In addition, there are multiple dedicated fueled electric generators to assist in a power failure. The generators are also inspected weekly by the third party vendor.

The facility has five redundant chilled-water heat exchange systems with 2,000 tons of chilled water to cool the building. Humidity is maintained at 45% - 55%. Temperature and humidity are monitored and maintained at acceptable levels, within the facility where the information system resides. Temperature and humidity is monitored onsite and

offsite. The Building Management System (BMS) is used to monitor any alarms.

5.1.4 Water Exposures

FOS-W: All production servers are located on a raised platform and away from any water. In addition, the water pipes over the server room are dry and are activated only in the event that the fire-suppressant FM200 gas fails. An emergency shutoff-valve is also installed directly behind a door labeled "Sprinkler Room FACP."

FOS-E: All production servers are located on a raised platform and away from water. All productions servers are protected from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel. Leak detection mechanisms are also located on each of the HVAC and Chiller units and under the datacenter floor. Type TC cable is used, which is water resistant.

5.1.5 Fire Prevention and Protection

FOS-W: The server room is protected from fire by an automated fire suppression and detection system based on FM200 gas. After smoke detectors sense the presence of smoke in two zones of the facility, the detection and control panel automatically sounds an alarm, shuts down the air handlers, disconnects power from the protected equipment, and then releases the fire-suppressing agent into the protected area. In the event that the FM200 gas cannot stop the fire, the server room is also equipped with 'dry' sprinkler pipes. All proper personnel, the building manager, and local fire department are notified once the alarm goes off. In addition, the facility is equipped with a fire alarm system that responds to alarm pull boxes as well as fire and smoke detectors. In the event of a fire, the facility is also equipped with fire extinguishers. The facility personnel adhere to GSA's abbreviated Occupant Emergency Plan (OEP), which references the number to call in the event of a fire emergency.

FOS-E: Fire suppression and detection devices/systems that can be activated in the event of a fire are installed. The fire suppression system is zone and pre-action. The fire suppression system is a dry pipe system. There are also handheld fire extinguishers and smoke detectors available.

5.1.6 Media Storage

Media is stored at the FPKI sites or kept under two-party control when transferred between sites to protect it from unauthorized physical access, in accordance with the SOPs. Media is stored in the SC to protect it from accidental damage (water, fire, electromagnetic).

5.1.7 Waste Disposal

The disposal of sensitive or classified information is handled in accordance with the GSA FTS procedures for disposal of such material. Burn bag procedures are in place, which specify the use of a "Sensitive Waste Container" (burn bag) which is then hand carried to GSA for disposal by a GSA Security Officer in accordance with GSA procedures.

5.1.8 Off-Site backup

Backup information is stored in the SC and replicated to the other site.

Whenever a certificate is issued or revoked, and other times as needed, the CA database is backed up and restored at the other FOS site, using standard [*Redacted for Security Purposes*] procedures. The replicated CA and the current backup of the CA database and private keys is sufficient to recover from a system failure.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security or operational incidents if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles are responsible for the integrity of the CA. The functions performed in these roles form the basis of trust for all uses of the EGCA. 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 ISSM and ISSO are Information Assurance roles appointed in accordance with applicable legislation and proscribing directives. The DAA appoints the ISSM, and the ISSM appoints the ISSO. The following is the list of Trusted Roles:

- *Administrator* – authorized to install, configure, and maintain the Operating Systems, Applications and Directory Software; establish and maintain Operating System user accounts; configure Operating System profiles and audit parameters; and generate component keys.
- *Officer* – authorized to issue and revoke certificates; maintain the CA software (after the Administrator has logged into the system, and with the Administrator present); establish and maintain CA user accounts; and configure CA software profiles and audit parameters.
- *Auditor* – authorized to view and maintain audit logs.
- *Operator* – authorized to perform system backup and recovery.

5.2.1.1 Administrator

The Administrator role is responsible for:

- Installation, configuration, and maintenance of the Operating Systems(OS) and Directory Software;
- Establishing and maintaining OS and directory system accounts;
- Configuring audit parameters for the OS and directory;
- Assisting in Generating and Backing up CA keys; and
- Restarting OS and services in case of system failures.

Administrators do not issue certificates.

5.2.1.2 Officer

The Officer role is responsible for issuing certificates, including:

- Registering new Subscribers;
- Verifying the accuracy of information included in certificates;
- Executing the issuance of certificates;
- Validating revocation requests and executing the revocation of certificates;
- Configuring certificate profiles or templates and audit parameters for the CA software; and
- Generating and backing up CA keys.

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 is operating in accordance with this CPS.

5.2.1.4 Operator

The Operator role is responsible for the routine operation of the EGCA including system backups and recovery or changing recording media. The Operator also assists the Administrator with problem resolution and routine maintenance.

5.2.2 Number of Persons Required per Task

To best ensure the integrity of the EGCA equipment and operation, no individual will be assigned more than one Trusted Role, with the exception of Operator. The separation provides a set of checks and balances over the EGCA operation. Since an Administrator is required to gain access to the FPKI facilities, at least one of the participants will always be an Administrator.

Only an Officer has access to the locked racks containing the CA equipment, therefore, both an Administrator and an Officer is required for any task associated with the CA and HSM, including HSM activation and backup and CA key generation, certificate issuance and certificate revocation.

Under no circumstances does any FPKI role perform its own auditor function.

5.2.3 Identification and Authentication for Each Role

Individuals identify and authenticate themselves before being permitted to perform any actions set forth above for that Trusted Role.

At the operating system level, authentication is done by system logon controlled by account authentication in Active Directory. Trusted Roles are given role-based access control on the system enforced by security groups in Active Directory. Administrators

have local and Domain administrator rights on the systems (with separate accounts providing those rights), while Officers are authenticating as a limited user to the CA server.

5.2.4 Separation of Roles

The separation of roles for the EGCA, which is operated at a high eAuthentication level of assurance, is as follows:

- Individual FPKIMA personnel are specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator/Operator, and Auditor roles. No user identity can:
  - Assume both the Administrator and Officer roles; or
  - Assume the Auditor and any other roles.
- The Operator role may be assumed by the Administrator.

The EGCA's crypto module is activated by using the [*Redacted for Security Purposes*] and tokens.

Separation of duty is enforced by only the Administrator/Operator has an account to log onto the system. Each Administrator/Operator logs on using his own account. Once an Administrator is logged on to the EGCA server, the Officer is given logical access to the [*Redacted for Security Purposes*] interface for the EGCA access to the functions for certificate issuance and revocation. The [*Redacted for Security Purposes*] interface requires two of N Trusted Roles enter the activation information for a split [*Redacted for Security Purposes*]. One must be an Administrator and one must be an Officer.

Audit log data is generated automatically by the CA for all access to CA activities.

The Auditor does not have a system account, the administrator logs on the system and provides the Auditor with access to view the audit logs.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

The EAO and the FPKIMA are responsible and accountable for the operation of the EGCA.

All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and are U.S. citizens. The FPKIMA PM and program management team are responsible for evaluating the qualification of each individual selected for a trusted role. The ISSO has oversight of the training provided to trusted roles.

All FPKI personnel serving in Trusted Roles hold TOP SECRET security clearances.

Personnel security procedures are in place, which include separation of duties, least privilege, and individual accountability to mitigate internal security risks due to the actions of personnel as outlined in [NIST SP 800-53]. See [FPKI SSP] "Personnel

Security" security control section for more details.

5.3.2 Background Check Procedures

FPKIMA personnel in Trusted Roles hold Top Secret clearances that require extensive background checks by Government Security personnel. Top Secret clearances are further subject to periodic reviews at least every five years.

5.3.3 Training Requirements

All Trusted Roles undergo security awareness training prior to their appointment to a Trusted Roles and on a periodic basis. They are also trained on the operations of the system.

All personnel performing duties with respect to the operation of the EGCA receive comprehensive training. Training (including On-The-Job-Training (OJT) and review of procedures) is conducted in the following areas by product engineers:

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

Training in the overall security procedures of the FPKI is conducted for all personnel at the initial full operation capability of the EGCA. When a person is assigned to a new FPKI Trusted Role, they receive training in all the operational duties for that role; including a period of shadowing another in that role and then a period of reverse shadowing. In addition, training and review of security procedures is conducted at the time a change in procedures occurs and/or annually. Personnel are required to sign acknowledgements that they have received this training. All personnel training records are maintained by the ISSO.

5.3.4 Retraining Frequency and Requirements

Any significant change to the operations is documented and personnel are informed and made aware of changes in accordance with the personnel training procedures defined in the SOPs. All FPKIMA personnel participate in mandatory refresher training annually to ensure all affected personnel are aware of new changes to procedures and configuration changes. In addition, immediate OJT is conducted when any changes occur within the EGCA operations. Examples of such changes are EGCA software or hardware upgrades, changes in automated security systems, and relocation of equipment. The ISSO maintains a record of the training received by each person assigned to an FPKI Trusted Roles.

5.3.5 Job Rotation Frequency and Sequence

Any rotation or termination of FPKIMA personnel shall not impact the continuity and integrity of the FPKI services. Since there are multiple people fulfilling each trusted role, there is time to identify and train a replacement any time one individual rotates or

terminates his/her position within the FPKIMA.

5.3.6 Sanctions for Unauthorized Actions

The FPKIPA and/or EAO take appropriate administrative and disciplinary actions against personnel who have performed unauthorized actions involving the EGCA or its repository. In the event of an unauthorized action, the ISSO immediately investigates the incident. After the investigation, the ISSO and ISSM determine if the action warrants disciplinary actions based on severity and the recurring frequency of the indiscretion. If the unauthorized action is a significant indiscretion, it is reported to the EAO, the FPKI PM, and the FPKIPA. If the incident is not severe, immediate remedial training is conducted to ensure the offending party is made aware of his/her action and trained on the correct actions in order to prevent further indiscretions.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the EGCA will have the necessary experience, as determined by their supervisor and PM, to be able to fulfill the required functions of their assigned role when given appropriate training on the operational procedures by the FPKIMA. All personnel assigned to the FPKIMA will be U.S citizens. All personnel assigned to FPKIMA Trusted Roles will hold an active U.S. Government Top Secret Clearance. EGCA contractors and subcontractors are contractually obligated to perform their duties in accordance with this CPS.

5.3.8 Documentation Supplied To Personnel

The FPKIMA makes available to all of its personnel the [EGCA CP], EGCA CPS, FPKIMA SOPs and any relevant statutes, policies or contracts when an individual is first assigned to an FPKIMA role.

When these documents are revised, FPKIMA personnel are notified of the changes and updated documents are provided in electronic format via secure file transfer protocol (FTP) or a secure file storage site.

5.4 AUDIT LOGGING PROCEDURES

The FPKIMA generates audit log files for all events relating to the security of the EGCA. In addition to the audit logs detailed below, information relevant to certificate issuance and certificate revocation events is captured on certificate issuance and certificate revocation forms. Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used, depending on the audited event. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits.

Formal audit and accountability policies and procedures have been developed and documented, and are periodically updated in accordance with [NIST SP 800-53]. See [FPKI SSP] “Audit and Accountability” security control section for more details.

5.4.1 Types of Events Recorded

Security auditing capabilities of the EGCA repository, the EGCA operating system, and CA applications have been enabled for logging the types of events specified in Table

5.4-1. The table indicates whether the auditable event is logged automatically by the application/operating system, is logged manually in a logbook as prescribed by applicable procedures, or both. 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. At a minimum, each audit record includes 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 signing process;
- A success or failure indicator when performing certificate revocation; and
- The identity of the entity and/or operator (of the EGCA) that caused the event.

The FPKIMA staff has verified (i.e., obtained vendor statements and conducted direct testing) that the equipment and application software supports capturing audit logs for the events specified in Table 5.4-1 through HTTP access, error logs, and system access logs. Firewall logs are also used to audit who is accessing or attempting to access the system. [*Redacted for Security Purposes*] logs, Directory Server Agent logs, firewall operating system access logs and external firewall logs are audited.

Table 5.4-1. Auditable Events

Auditable Event	FPKI System			CA Enclave		
	Manual / Procedural	**Automatic**	**Location**	**Manual / Procedural**	**Automatic**	**Location**
SECURITY AUDIT						
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	✓		CM Package	✓		CM Package
Any attempt to delete or modify the Audit logs	✓ After a deletion following any archive operation	✓ After a modification following any archive operation	Security Event Logs		✓	[*Redacted for Security Purposes*]
IDENTIFICATION AND AUTHENTICATION						
Successful and unsuccessful attempts to assume a role		✓	Event Logs		✓	[*Redacted for Security Purposes*]
Change in the value of maximum authentication attempts	✓		CM Package Event Log	✓		CM Package Event Log

Auditable Event	FPKI System			CA Enclave		
	Manual / Procedural	Automatic	Location	Manual / Procedural	Automatic	Location
Maximum number of unsuccessful authentication attempts during user login		✓	Security Event Log		✓	[*Redacted for Security Purposes*]
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		✓	Security Event Log		✓	Security Event Log
An Administrator changes the type of authenticator, e.g., from password to biometrics	✓		CM Package	✓		CM Package
KEY GENERATION						
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	Applies to CA only	Applies to CA only	Key Signing Ceremony	✓		Key Signing Ceremony
PRIVATE KEY LOAD AND STORAGE						
The loading of Component private keys	Applies to CA only	Applies to CA only	N/A	✓	✓	HSM Syslog (restoring from backup token)
All access to certificate subject private keys retained within the CA for key recovery purposes	Applies to CA only	Applies to CA only	N/A	✓	✓	HSM Syslog (restoring from backup token)
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE						
All changes to the trusted public keys, including additions and deletions	Applies to CA only	Applies to CA only	N/A	✓		Key Signing Ceremony
PRIVATE KEY EXPORT						

Auditable Event	FPKI System			CA Enclave		
	Manual / Procedural	Automatic	Location	Manual / Procedural	Automatic	Location
The export of private keys (keys used for a single session or message are excluded)	Applies to CA only	Applies to CA only	N/A	✓	✓	[*Redacted for Security Purposes*]
CERTIFICATE REGISTRATION						
All certificate requests	Applies to CA only	Applies to CA only	N/A	✓	✓	[*Redacted for Security Purposes*]
CERTIFICATE REVOCATION						
All certificate revocation requests	Applies to CA only	Applies to CA only	N/A	✓	✓	[*Redacted for Security Purposes*]
CERTIFICATE STATUS CHANGE APPROVAL						
The approval or rejection of a certificate status change request	Applies to CA only	Applies to CA only	N/A	✓		Letter of Authorization
CA CONFIGURATION						
Any security-relevant changes to the configuration of the CA	Applies to CA only	Applies to CA only	N/A	✓	✓	[*Redacted for Security Purposes*]
ACCOUNT ADMINISTRATION						
Roles and users are added or deleted	✓		Event Log	✓	✓	Event Log
The access control privileges of a user account or a role are modified	✓		Event Log	✓	✓	Event Log
CERTIFICATE POLICY MANAGEMENT						
All changes to the Certificate Policy	✓		N/A	N/A		FPKIPA Meeting Minutes Change Proposal and revised Certificate Policy

Auditable Event	FPKI System			CA Enclave		
	Manual / Procedural	Automatic	Location	Manual / Procedural	Automatic	Location
CERTIFICATE PROFILE MANAGEMENT						
All changes to the certificate profile	Cert Profile not captured in Directory	Cert Profile not captured in Directory	N/A	✓		FPKIPA Meeting Minutes Change Proposal and revised Certificate Profile
REVOCATION PROFILE MANAGEMENT						
All changes to the revocation profile	Revocation Profile not captured in Directory	Revocation Profile not captured in Directory	N/A	✓		FPKIPA Meeting Minutes Change Proposal and revised CRL Profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT						
All changes to the certificate revocation list profile	Certificate Revocation List Profile not captured in Directory	Certificate Revocation List Profile not captured in Directory	N/A	✓		FPKIPA Meeting Minutes
MISCELLANEOUS						
Installation of the Operating System	✓	✓	[*Redacted for Security Purposes*]	✓	✓	[*Redacted for Security Purposes*]
Installation of the CA	Applies to CA only	Applies to CA only	N/A	✓	✓	[*Redacted for Security Purposes*]
Installing hardware cryptographic modules	Applies to CA only	Applies to CA only	N/A	✓		CM Package
Removing hardware cryptographic modules	Applies to CA only	Applies to CA only	N/A	✓		CM Package
Destruction of cryptographic modules	Applies to CA only	Applies to CA only	N/A	✓		CM Package
System Startup	✓		[*Redacted for Security Purposes*]	✓	✓	Event Log HSM Boot Log
Logon Attempts to CA Apps	Applies to CA only	Applies to CA only	N/A		✓	[*Redacted for Security Purposes*]

Auditable Event	FPKI System			CA Enclave		
	Manual / Procedural	Automatic	Location	Manual / Procedural	Automatic	Location
Receipt of Hardware / Software	✓			✓		Receiving Doc
Attempts to set passwords	✓		Security Event Log		✓	[*Redacted for Security Purposes*]
Attempts to modify passwords	✓		[*Redacted for Security Purposes*]		✓	[*Redacted for Security Purposes*]
Backing up CA internal database	Applies to CA only	Applies to CA only	N/A		✓	[*Redacted for Security Purposes*]
Restoring CA internal database	Applies to CA only	Applies to CA only	N/A		✓	[*Redacted for Security Purposes*]
File manipulation (e.g., creation, renaming, moving)	✓		CM Package	✓		CM Package
Posting of any material to a repository		✓	[*Redacted for Security Purposes*]	N/A	N/A	N/A
Access to CA internal database	Applies to CA only	Applies to CA only	N/A	✓	✓	[*Redacted for Security Purposes*]
All certificate compromise notification requests	Applies to CA only	Applies to CA only	N/A	✓		Certificate Revocation Form
Loading tokens with certificates	Applies to CA only	Applies to CA only	N/A	✓		CM Package
Shipment of Tokens	Applies to CA only	Applies to CA only	N/A	✓		Receiving Doc
Zeroizing tokens	Applies to CA only	Applies to CA only	N/A	✓		HSM Logs
Rekey of the CA	Applies to CA only	Applies to CA only	N/A	✓		Key Signing Ceremony
Configuration changes to the CA server involving:	Applies to CA only	Applies to CA only	N/A	✓		CM Package
Hardware	Applies to CA only	Applies to CA only	N/A	✓		CM Package
Software	Applies to CA only	Applies to CA only	N/A	✓	✓	CM Package (Application Specific)
Operating System	Applies to CA only	Applies to CA only	N/A	✓	✓	[*Redacted for Security Purposes*]

Auditable Event	FPKI System			CA Enclave		
	Manual / Procedural	Automatic	Location	Manual / Procedural	Automatic	Location
Patches	Applies to CA only	Applies to CA only	N/A	✓	✓	[*Redacted for Security Purposes*]
Security Profiles	Applies to CA only	Applies to CA only	N/A	✓	✓	[*Redacted for Security Purposes*]
PHYSICAL ACCESS / SITE SECURITY						
Personnel Access to room housing CA	✓	✓	SIR (electronic logs managed by COLO provider)	✓	✓	Personnel Sign In sheets (electronic logs managed by COLO provider)
Access to the CA server	Applies to CA only	Applies to CA only	N/A	✓	✓	Personnel Sign In sheets (electronic logs managed by COLO provider)
Known or suspected violations of physical security	✓	✓	SIR (electronic logs managed by COLO provider)	✓	✓	SIR (electronic logs managed by COLO provider)
ANOMALIES						
Software Error conditions		✓	Event Logs		✓	Event Logs
Software check integrity failures		✓	[*Redacted for Security Purposes*]		✓	Event Logs (application specific)
Receipt of improper messages		✓	Firewall logs		✓	Firewall logs
Misrouted messages		✓	Firewall logs		✓	Firewall logs
Network attacks (suspected or confirmed)	✓	✓	[*Redacted for Security Purposes*]		✓	[*Redacted for Security Purposes*]
Equipment failure	✓		SIR	✓		SIR
Obvious and significant network service or access failures	✓	✓	SIR (individual component log)	✓	✓	SIR (individual component log)

Auditable Event	FPKI System			CA Enclave		
	Manual / Procedural	Automatic	Location	Manual / Procedural	Automatic	Location
Violations of Certificate Policy	✓	Certain Violations as documented by this table	SIR	✓	Certain Violations as documented by this table	SIR
Violations of Certification Practice Statement	✓	Certain Violations as documented by this table	SIR	✓	Certain Violations as documented by this table	SIR
Resetting Operating System clock		✓	[*Redacted for Security Purposes*]		✓	System Event Log

If the following events occur, they are manually logged:

- Obtaining a third-party time-stamp
- All security-relevant data that is entered in the system
- All security-relevant messages that are received by the system
- All successful and unsuccessful requests for confidential and security-relevant information
- The manual entry of secret keys used for authentication
- Appointment of an individual to a Trusted Role
- Designation of personnel for multiparty control

5.4.2 Frequency of Processing Log

Audit logs from the Administration and Demilitarized Zones (DMZs) are collected and processed, in an automated continuous process, checking for anomalies. The automatic logger creates alerts if anomalies are encountered.

The FPKIMA Auditor reviews audit logs at least once per week.

The manual logs include:

- Personnel Sign-in log
- Visitor Sign-in Log
- secure container log
- secure rack log

The electronic logs include logs from [*Redacted for Security Purposes*].

The FPKIMA Auditor examines the security audit data generated by the EGCA and

manual logs since the last review, paying particular attention to anomalies and suspicious entries. All security alerts and irregularities are explained in an audit log summary. The FPKIMA Auditor reviews include verifying that the log has not been tampered with, and then briefly inspecting log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

The FPKIMA Auditor collects and prepares audit logs for transfer.

5.4.3 Retention Period for Audit Log

Audit logs are stored onsite until the next audit (weekly) then moved to the Interim storage area. Audit logs are retained offsite at the Interim storage area until they are sent to National Archives and Records Administration (NARA). The FPKIMA Administrator, under supervision of the Auditor, removes audit logs from the EGCA and gives them to the FPKIMA Auditor. Audit logs written to optical disk are labeled with the name of the program (FPKI), a description (e.g. Repository [*Redacted for Security Purposes*] Audit logs), today's date or a range of dates, if applicable, in YYYY/MM/DD format.

Neither the Administrator nor the Auditor can access the EGCA signature key(s).

5.4.4 Protection of Audit Log

The FPKIMA Auditor performs routine review of security audit logs. The policies for protecting security audit data are as follows:

1. Security audit logs are automatically time stamped upon creation.
2. The only authorized people having read access to the logs include the FPKIMA Administrator, Officer, Auditor, Operator, and others possibly designated by the FPKIMA to perform security audit processing.
3. Only the FPKIMA Auditor is authorized to archive audit logs.
4. Audit logs are deleted only under procedural multi-person control, one participating individual must be an Auditor who has no command of the CA key.
5. Audit logs are protected under multi-person control and cannot be modified without detection, one participating individual must be an Auditor who has no command of the CA key.

Daily audit logs are generated on time-stamped digital media and are protected from deletion and modification prior to the end of the audit log retention period. System logs are automatically time stamped. All audit logs are maintained until after the annual audit.

The FPKIMA maintains two internal Network Time Protocol (NTP) servers used to maintain and synchronize system time for all servers, appliances and applications within the EGCA. The two internal servers will be synchronized to NIST.

5.4.5 Audit Log Backup Procedures

Manual audit logs are collected weekly and stored in a secure container in a separate building (Interim storage) from the FPKI facility. Audit logs written to removable media as part of the weekly audit are placed in sealed envelopes and transported to the interim

site under two person control. These audit logs are archived to a NARA archive location annually.

Administration and DMZ event logs and audit summaries are backed up and time stamped automatically and on a continual basis using an automatic logging device. Copies of these and manual paper logs are moved to and stored in the secure container in a separate building (Interim storage) from the FPKI facility. Logs are placed in sealed envelopes and transported under two-person control. Two-person control is achieved by using tamper-evident envelopes with receipt numbers. The material is placed in the envelope and sealed with both people present. One then carries the envelope, while the other keeps the numbered receipt. At the destination, both people confirm there is no evidence of the envelope having been opened or tampered with, and that the number of the envelope matches the receipt number.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system is internal to the EGCA components (see Section 5.4). Audit processes are invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed (as determined during the auditing process and documented in the auditing/trouble handling forms), and the integrity of the system or confidentiality of the information protected by the system is at risk, then the FPKIMA ISSO in conjunction with the ISSM and FPKIMA PM will determine whether to suspend EGCA operation until the problem is remedied. Section 5.4.1 describes the collection procedures (manual or automatic) for the auditable events. Section 5.4.5 describes the protection procedures for backing up audited data that has been collected.

5.4.7 Notification to Event-Causing Subject

No notice that an event was audited is provided to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

The FPKIMA performs self-assessments of the security controls at the time of initial installation and configuration of the EGCA components. Periodic vulnerability assessments are performed monthly or following a system configuration change with the potential for effecting system security (i.e., hardware, software, or network changes or upgrades).

External penetration assessments are conducted on a quarterly basis.

The FPKIMA provides a report of the analysis of the results of both internal and external vulnerability assessments to the FPKIMA PM and ISSM, specifically indicating security vulnerabilities identified and mitigation procedures of those vulnerabilities.

5.5 RECORDS ARCHIVAL

The FPKIMA moves archive records to NARA on an annual basis. NARA receipts for archived material are filed at the Interim Site.

5.5.1 Types of Records Archived

At initialization, the EGCA system equipment configuration files were archived, as well as the CPS and any contractual agreements to which the FPKIMA is bound. During EGCA operation, the following data are recorded for archive:

- EGCA certification and accreditation;
- EGCA Configuration Documentation;
- Certificate Policy;
- Certification Practice Statement;
- Contractual obligations;
- Other agreements concerning operations of the EGCA;
- System and equipment configuration;
- Modifications and updates to system or configuration;
- Certificate requests;
- Revocation requests;
- Subscriber identity Authentication data as per Section 3.2;
- Documentation of receipt and acceptance of certificates;
- Documentation of receipt of tokens;
- All certificates issued or published;
- Record of EGCA Re-key;
- 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 EGCA generates a key. (Not mandatory for single session or one-time use symmetric keys);
- All access to certificate subject private keys retained within the EGCA for key recovery purposes (Not applicable for the EGCA);
- 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;
- Security Incident Reports (SIRs) with remedial action details;
- Violations of Certificate Policy; and
- Violations of Certification Practice.

See Sections 5.4.6 and 5.5.6 for a description of the audit and archive collection procedures.

5.5.2 Retention Period for Archive

Items that are required to be archived in paper format are transferred to the interim site, and then to NARA so they can be retained for the required period, 10 years, 6 months. Other items, such as signed certificates and CRLs, are backed up and stored on the servers themselves. This ensures that there is always a copy available.

The auditor collects electronic log records and paper access log records on a weekly basis. The electronic records are recorded on optical disk. Electronic records written to optical disk are also included in the archive cycle.

The interim site is located at:

[*Redacted for Security Purposes*]

The FOS-W site is currently located at:

[*Redacted for Security Purposes*]

The FOS-E site is currently located at:

[*Redacted for Security Purposes*]

5.5.3 Protection of Archive

Archive data is clearly labeled as follows:

- Classification Label: SBU
- Name of the Program: FPKI
- Type of item (e.g., EGCA Log Report)
- Start Date through End Date
- Copy control number.

The archive media is stored in a safe at the Interim facility, which is temperature controlled and behind locked doors, as described in Section 5.1.

The FPKIMA Auditor maintains a list of individuals who can access the archive files at the Interim site. Archive data is protected in safes and by using the packaging in the Audit Procedures.

The contents of the archive will not be released except as determined by the EAO, FPKIPA or as required by law. Any request for archived information must be made to the FPKIMA PM, who in consultation with the ISSM will determine if the requested information may be provided. If release of such information is authorized, the ISSM and PM inform the ISSO, who will provide the information.

5.5.4 Archive Backup Procedures

Archive records are periodically written to transferable media (e.g., tape or optical disk) and transferred to the Interim site, and then to NARA. Transferable media is put in

sealed envelopes and transferred under control of a trusted role auditor.

5.5.5 Requirements for Time-Stamping of Records

Records are clearly labeled with date/time period information of the data contained in the record. System clocks are kept synchronized via NTP and system logs are automatically time stamped.

5.5.6 Archive Collection System (Internal or External)

The archive information is collected by the FPKIMA Auditor, who is responsible for assuring, using a checklist, that all required records for archive are correctly filed in the records to be archived.

5.5.7 Procedures to Obtain and Verify Archive Information

The FPKIMA auditing official maintains logging information (and receipts) as archived data is transported to short-term and long-term archive facilities.

Archive material retrieved from NARA is verified against the logging information and receipts. Contents of the FPKIMA archives are only released upon request of the EAO or FPKIPA. Individual records pertaining to a specific certificate can be released to the authorized POC for that Subscriber upon request.

5.6 KEY CHANGEOVER

The EGCA key changeover procedures are as follows:

1. The EGCA will generate a self-issued certificate signed by the old private key whose *subjectPublicKeyInfo* field contains the new public key.
2. The EGCA will generate a self-issued certificate signed by the new private key whose *subjectPublicKeyInfo* field contains the old public key.
3. The EGCA will generate a self-signed certificate signed by the new private key whose *subjectPublicKeyInfo* field contains the new public key.
4. The EGCA and all Subscribers will process new certificates as described in this CPS.
5. All certificates generated as part of the key changeover process will be posted to the FPKI repository.

The EGCA signing key has a validity period of three years, and its corresponding certificate has a validity period of six years.

The EGCA will support Subscribers key changeovers by issuing and posting new certificates as required. The old private key is used to sign CRLs that contain certificates signed with that key as long as required. The old key is retained and protected.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The FPKIMA responds to all incidents and suspected compromise events. Detailed

procedures are explained below.

In the event of a disaster, the following steps will be accomplished to regain system functionality:

1. Notification of the GSA Designated Official For Facilities (DOFF) and Facility Emergency Response Team Leader (FERTL). These individuals along with the FPKIMA will assess the outage and determine whether all or part of the Recovery team needs to be assembled.
2. Activation of the Damage Assessment and Disaster Recovery team.
3. Based on the severity of the event, activate the recovery procedures for that severity type.
4. Interface with the FPKIMA management team.
5. The FPKI Repository services are actively supporting traffic at both the FOS-W and FOS-E sites during normal operation. In the case of an outage or disaster at either site, the [*Redacted for Security Purposes*] at the other site will take over and the single remaining site will automatically continue to service FPKI Repository traffic.
6. If the severity of the event is critical (i.e., will impact the next scheduled generation of a CRL) at the currently active site, the EGCA at the alternate site will be activated to begin generation of CRLs and the publisher software on that EGCA will be activated to publish CRLs to its local FPKI Repository.
7. Manage the recovery process of the affected FPKI facility.
8. Submit post recovery logs to FPKIPA.

The EAO will be notified as soon as possible as described in *FPKIMA Incident Management Plan* [FPKIMA IMP]. The FPKIPA will also be notified as soon as possible. If the EGCA will not be able to issue a new CRL within 36 hours from either facility, the FPKIPA will be notified.

If log analysis or other information provides reason to suspect any of the following may have occurred:

- compromise of the EGCA systems;
- physical or electronic attempts to penetrate FPKI Trust Infrastructure systems; or
- denial of service attacks on FPKI Trust Infrastructure repositories,

[FPKIMA IMP] will be followed to investigate and diagnose the suspected incident. The FPKIPA and other appropriate government and non-government organizations will be notified as soon as possible as described in [FPKIMA IMP].

Incident response policies and procedures have been developed, documented and are reviewed and updated periodically, in accordance with [NIST SP 800-53]. See [FPKI SSP] “Incident Response” security control section for more details.

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

In the event the EGCA equipment is damaged or rendered inoperative, but the EGCA

signature keys are not destroyed, EGCA operation is reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

In order to provide 6-hour window for EGCA service re-activation, the FPKIMA has implemented a synchronized FOS-E site. The FOS-E site includes an identical configuration of the FOS-W site. The FOS-E site EGCA is quickly restored via backup tapes.

During system restoration, the FPKIMA needs to ensure the EGCA CRLs are current with latest certificates revoked. Additionally, certificates need to be validated and new public keys certificates issued in the event anomalies exist.

The following reports are generated:

- Activity log – this log is maintained throughout the disaster recovery process;
- Test plan results;
- Equipment list – Update configuration management; and
- Restoration Expense report.

5.7.3 EGCA Private Key Compromise Procedures

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

1. If possible, the certificate of the compromised key will be revoked. A compromised key can be used to sign the new CRL.
2. The EAO, Subscribers, and the FPKIPA and all of its member entities (the POCs list is retrieved from the secure storage container) will be securely notified via telephone (via callback and challenge-response) to the designated POCs.
3. The EGCA will generate a new EGCA key pair in accordance with procedures set forth in Section 6.1.
4. New EGCA certificates will be issued to Subscribers also in accordance with Section 4.3.

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

5.7.4 Business Continuity Capabilities After a Disaster

The EGCA servers operate with back-up power and telecommunications and appropriate infrastructure system redundancies to minimize outages. However, if an outage appears likely to become, or becomes, an extended outage, the disaster recovery plan will come into effect. An extended outage is currently defined as one in which the ability of EGCA to revoke certificates cannot be re-established within 24 hours, however the FPKIMA has the ability to respond to an extended outage at one site. If something happens to one of the FOS sites, all EGCA operations can be shifted to operate from the remaining site within 6 hours

In the case of a disaster whereby both the FOS-W and FOS-E installations are physically

damaged, the EAO, all Sponsors, the FPKIPA and all of its member entities will be securely notified (via callback and challenge-response) and the procedures described in Section 5.7.3 will be followed. The EGCA installation will then be completely rebuilt, by reestablishing the EGCA equipment, generating new private and public keys, being re-certified, and re-issuing all certificates.

5.8 CA OR RA TERMINATION

In the event of termination of the EGCA operation, certificates signed by the EGCA will be revoked, following the standard procedures for revoking certificates (see section 4.9.3). The FPKIMA will advise, using secure communication (callback and challenge-response), all Sponsors, to which the EGCA has issued certificates, of its termination. All documentation and data will be archived using the archival procedures in section 5.5.3.

The FPKIMA Team will coordinate scheduled termination with Sponsors when authorized by the EAO or FPKIPA.

Entities will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought in the event the EGCA is terminated.

6 TECHNICAL SECURITY CONTROLS

The FPKI Trust Infrastructure implements an array of technical security controls in accordance with [NIST SP 800-53] that pertain to this section. See [FPKI SSP] "Access Control," "Audit and Accountability," Identification and Authentication," and "System and Communication Planning" security control sections for more details.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The EGCA was established with a [*Redacted for Security Purposes*] CA. The key pair for the EGCA was generated on the [*Redacted for Security Purposes*] cryptographic module. The key pair generation is RSA for digital signature in compliance with FIPS 140-2, level 3. The private key is never exposed outside the module in unencrypted form. After the key pair generation process, the [*Redacted for Security Purposes*] was backed up onto a secure token and restored to a second [*Redacted for Security Purposes*] at the alternate site. Backup copies of the [*Redacted for Security Purposes*] private keys are also created and stored in locked containers at both sites and the Trusted Operations Center (TOC) site.

EGCA private keys are generated using the EGCA Key Signing Ceremony procedures. These procedures document the role separation and provide an auditable trail. The Key Signing Ceremony procedures are completed with a witness present, each step is verified and the document is signed off on at the end of the procedure.

6.1.1.2 Subscriber Key Pair Generation

In all cases, the Subscriber performs their own key pair generation using a FIPS-approved method.

6.1.2 Private Key Delivery to Subscriber

The Subscribers generate their own key pairs and therefore do not need private key delivery.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered to the certificate issuer electronically in certificate request (i.e., using PKCS#10) messages to the FPKIMA via secure means (e.g., CD delivered by registered mail, courier, secure FTP, or digitally-signed email) as described in Section 4.3.2. Identity checking and proof of possession of the private key will be accomplished as described in Section 4.2.1.

6.1.4 CA Public Key Delivery to Relying Parties

The EGCA Root Certificate will be transported in a secure, out-of-band mechanism, using PKCS#10 messages via digitally-signed e-mail, secure FTP, or CD delivered by registered mail or courier to the Sponsor.

When EGCA updates its signature key pair, the new public key may be distributed in a self-signed certificate or in a key rollover certificate.

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

6.1.5 Key Sizes

After December 31, 2010, all certificates are issued by a [*Redacted for Security Purposes*] CA that signs certificates and CRLs using SHA-256 RSA PKCS#1 signatures. Certificates issued prior to December 31, 2010 were signed using either SHA-1 or SHA-256. The EGCA's key is a 2048 bit RSA key.

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.

6.1.6 Public Key Parameters Generation and Quality Checking

There are no public key parameters for RSA. Therefore, there is no requirement for public key parameter generation and quality checking.

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

The use of a specific key is determined by the key usage 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 bound into EGCA certificates are used only for signing certificates and status information (e.g., CRLs). EGCA certificates subject public key are asserted as follows:

- *keyCertSign* bit to verify other certificates;
- the *cRLSign* bit to verify CRLs; and
- both the *keyCertSign* and *cRLSign* bits to verify both certificate and CRLs.

Section 7 contains further details on key usage.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The CA private keys are protected using FIPS 140-2 Level 3 validated cryptographic module: [*Redacted for Security Purposes*] HSM.

All cryptographic modules are operated such that the private asymmetric cryptographic keys are never output in plaintext. Activation of the HSM requires the [*Redacted for Security Purposes*] and tokens. Physical access to the HSM requires two-party control. See Section 5.1.2.

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

All EGCA private keys are under 2 out of N control, where N≥2. N is the total number of Officers plus one in the FPKIMA. See Sections 5.2 and 5.2.4 for details on how this is achieved. The Trusted Roles present whenever the CA rack is accessed sign the "secure rack access list" which is checked by the auditor during the weekly audits and retained as part of the logs available during the annual PKI Compliance audit.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of EGCA and Subscriber Private Signature Key

The EGCA signature keys are not escrowed.

6.2.3.2 Escrow of CA Encryption Keys

The EGCA does not escrow any CA encryption keys.

6.2.4 Private Key Backup

6.2.4.1 Backup of EGCA and Subscriber Private Signature Key

The EGCA private key is stored in the [*Redacted for Security Purposes*] at both the FOS-W and FOS-E sites. In addition, the EGCA private key is backed up on [*Redacted for Security Purposes*] backup tokens. [*Redacted for Security Purposes*] The backups of the EGCA private keys are made following procedures described in the [*Redacted for Security Purposes*] operations manuals and the FPKIMA HSM manual.

The EGCA is never in possession of Subscriber private signature keys.

6.2.4.2 Backup of Subscriber Private Signature Key

The EGCA is never in possession of Subscriber private keys.

6.2.5 Private Key Archival

No EGCA private keys are archived or escrowed.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

EGCA private keys are generated by and remain in a cryptographic module. The [*Redacted for Security Purposes*] product uses proprietary secure means for transferring

keys from one cryptographic module to another to back up the CA keys.

6.2.7 Private Key Storage on Cryptographic Module

The EGCA private key is only stored in the [*Redacted for Security Purposes*], FIPs-140 Level-3 evaluated cryptographic module and on [*Redacted for Security Purposes*] proprietary backup tokens.

6.2.8 Method of Activating Private Key

The [*Redacted for Security Purposes*] cryptographic module requires that the two Officer tokens be inserted into the [*Redacted for Security Purposes*]. The Administrator must be present.

Procedures for activating and using the private keys, as well as the physical protections procedures for the hardware tokens, are provided in Section 5.1.2.

6.2.9 Methods of Deactivating Private Key

The [*Redacted for Security Purposes*] cryptographic module is always in use and activated. The [*Redacted for Security Purposes*] cryptographic module is protected from unauthorized use by the physical access mechanisms described in Section 5.1.2.1. The [*Redacted for Security Purposes*] cryptographic module is protected from unauthorized logical access by being on the protected CA sub network as described in Section 6.5.1. Additionally, the [*Redacted for Security Purposes*] and hardware tokens are required to obtain direct logical access to the [*Redacted for Security Purposes*] and these are stored as described in Section 5.1.2.1.

6.2.10 Method of Destroying Subscriber (i.e., Officer) Private Signature Key

When an Administrator or Officer leaves, the [*Redacted for Security Purposes*] to access the [*Redacted for Security Purposes*] interface to the CA application are regenerated to remove the piece associated with the terminating individual, or its password is changed by the individual taking the place of the terminating individual.

When a CA private signature key is no longer needed, the key will be deleted from the [*Redacted for Security Purposes*]. If the FPKI Trust Infrastructure CA is being decommissioned, the corresponding [*Redacted for Security Purposes*] will be deleted and all backup tokens will be zeroized.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The EGCA private signing keys are used to sign certificates for one-half of the certificate

lifetime (e.g. for 3 years with a certificate lifetime of 6 years). Rekeying will be performed at 3 years.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

On the [*Redacted for Security Purposes*] device, the [*Redacted for Security Purposes*] tokens are used to activate a [*Redacted for Security Purposes*] to enable use of the CA private signing keys. These tokens satisfy the policy enforced by the [*Redacted for Security Purposes*]. Once the use of the CA private signing keys is enabled, actual use of the private signing keys is under multi-person control of the EGCA software. Activation data for the [*Redacted for Security Purposes*] is generated by the HSM [*Redacted for Security Purposes*].

The EGCA is installed using a [*Redacted for Security Purposes*] CA. Multi-party control of the [*Redacted for Security Purposes*] CA is enforced through physical means, an administrator is required to gain access to the room, and an officer has to unlock the rack containing the CA. In addition, access to the CA software requires authentication of M of N individuals, where M is two, one administrator and one officer, and N is the total number of officers plus one. This M of N authentication makes use of split [*Redacted for Security Purposes*] CA. Each piece of the split [*Redacted for Security Purposes*] is a file stored on a FIPS 140-2 Level 3 Encrypted USB Flash Drives which requires the trusted role to enter a password to access the Flash Drives and a Password to unencrypt the [*Redacted for Security Purposes*] file. The split [*Redacted for Security Purposes*] are updated whenever there is a change in Trusted Role personnel. In addition, new [*Redacted for Security Purposes*] will be generated when an EGCA performs a rekey.

6.4.2 Activation Data Protection

Activation information for the [*Redacted for Security Purposes*] CA will be stored on FIPS 140-2 Level 3 Encrypted USB Flash Drives stored in the Officer's ISC, which are stored in onsite safes when not in use.

Note that on the [*Redacted for Security Purposes*] unit, the activation data is on physical tokens. These tokens are locked in secure containers. The M of N keys are stored in separate containers locked using devices for which no one person has access to both combinations and keys.

The EGCA is configured to temporarily lock out access following three unsuccessful login attempts.

See Sections 5.1.2 and 5.2.2 for descriptions of the procedures for distribution and protection of activation data contained on the hardware tokens.

6.4.3 Other Aspects of Activation Data

Passwords are changed periodically, as described in the SOPs, to decrease the likelihood of discovery. The cryptographic module activation data will be changed not less than

once per year or when an Officer leaves.

6.5 COMPUTER SECURITY CONTROLS

The FPKI Trust Infrastructure implements an array of technical security controls in accordance with [NIST SP 800-53] that pertain to this section. See [FPKI SSP] "Access Control," "Audit and Accountability," Identification and Authentication," and "System and Communication Planning" security control sections for more details.

6.5.1 Specific Computer Security Technical Requirements

The server where the EGCA resides is dedicated to the function of Certificate Authority services. The EGCA server is accessed only via KVM in the locked CA rack. This server publishes all information to an internal FPKI directory, which itself connects through a one-way firewall to the online repository systems in order to post validation information.

The FPKI Repository servers only run those services necessary to operate and maintain the repository and to support on-line certificate validations by Subscribers (e.g., LDAP, DSP, HTTP, DNS, NTP).

All EGCA infrastructure component systems are configured with appropriate security features turned on as recommended by the host operating system vendor in accordance with any associated security validation rating.

The CA server has the following security features and functions:

- Require authenticated logins;
- Provide Discretionary Access Control via permissions and policies defined in the CA software;
- Provide a security audit capability via automatic logging of all CA activity;
- Restrict access control to EGCA services and PKI roles as described in Sections 5.1.2 and 5.2.2;
- Enforce separation of duties for PKI roles as described in Sections 5.1.2 and 5.2.2;
- Require identification and authentication of PKI roles and associated identities as described in Sections 5.1.2 and 5.2.2;
- Prohibit object re-use or require separation for EGCA random access memory. This requirement is met by the configuring the [*Redacted for Security Purposes*] operating system to the Vendor Standard [*Redacted for Security Purposes*]. Windows enforces the required prohibition/separation. [*Redacted for Security Purposes*] was evaluated as EAL4 under Common Criteria, Validation Report Number: CCEVS-VR-07-0023. [*Redacted for Security Purposes*];
- Require use of cryptography for session communication and database security.
- Archive EGCA history and audit data through data collection and archive procedures described in Sections 5.4 and 5.5;
- Require self-test security related EGCA services. CA security audit logs are signed objects and the software verifies those objects at startup and each time the

logs are accessed. If the verification changes, the software provides a message through the user interface and logs the event;
- FIPS 140-2 certified hardware is used to [*Redacted for Security Purposes*] required to access the CA key for certificate issuance and revocation;
- Requires a recovery mechanisms for keys and the EGCA system through backup and protection procedures described in Section 5.5; and
- Enforce domain integrity boundaries for security critical processes through self-test procedures described above.

6.5.2 Computer Security Rating

[*Redacted for Security Purposes*].

6.6 LIFE-CYCLE TECHNICAL CONTROLS

The FPKI Trust Infrastructure implements an array of technical security controls in accordance with [NIST SP 800-53] that pertain to this section. See [FPKI SSP] "Access Control," "Audit and Accountability," Identification and Authentication," and "System and Communication Planning" security control sections for more details.

6.6.1 System Development Controls

The System Development Controls for the EGCA are as follows:

- The EGCA software is commercial-off-the-shelf software that has been developed under a formal development process that is well documented;
- Hardware procured to operate the EGCA has been purchased in a fashion whereby the provider does not know that it is intended for the EGCA operations. The CA software has been installed under the direction and control of authorized FPKI operation personnel. Hardware and software updates will be purchased or developed in the same manner as the original equipment and will be installed by trusted and trained personnel;
- All software and hardware installed in or run on the EGCA server is purchased using commercial buys. Hardware and non-CA software is purchased through standard procurement procedures provided by the FPKIMA. No custom Software has been purchased. An accountable method of packaging and delivery is used to provide a continuous chain of accountability from the vendor to the facility (e.g., UPS, FedEx, USPS Express Mail). The FPKIMA established a relationship with the CA software vendor prior to acquisition that gives assurance that the software has not been tampered with. Installation is performed under multi-person control with only authorized FPKIMA personnel; and
- Proper care is taken to prevent malicious software from being loaded onto the EGCA equipment. From the time the software is received, it remains under continuous control. All shrink wrapped packaging is opened and installed inside the secure EGCA facility under multi-person control**.** Antivirus software is used to scan all applications and files for malicious code, initially, periodically, and any time a new file is introduced to the system. Vulnerability assessments are conducted periodically, and any time a system configuration change occurs (i.e.,

adding a new CA to the FPKI).
- Continuous monitoring of all FPKI systems is performed through Intrusion Detection Systems, vulnerability testing and scanning, external penetrations tests, log analysis, and procedural monitoring as required in operating procedures.
- EGCA software and hardware is dedicated to performing CA functions only.

6.6.2 Security Management Controls

The initial configuration of the FPKI software (i.e., CA software, repository software) as well as any modifications and upgrades is documented and controlled in accordance with FPKI Configuration Management Procedures (separate FPKIMA document). System and application level logging is enabled and reviewed weekly to maintain the ongoing integrity of the software and configuration. The source for the software is described in Section 6.6.1. Audit Procedures are used to ensure the integrity of the software. These procedures are performed on a weekly basis.

6.6.3 Life Cycle Security Ratings

The EGCA system operates under standard maintenance. Upgrades, Information Assurance Vulnerability Alerts (IAVA), and patches to the software and hardware are applied as necessary under FPKI Configuration Management (CM) procedures.

6.7 NETWORK SECURITY CONTROLS

The FPKI Trust Infrastructure implements an array of technical security controls in accordance with [NIST SP 800-53] that pertain to this section. See [FPKI SSP] "Access Control," "Audit and Accountability," Identification and Authentication," and "System and Communication Planning" security control sections for more details.

A secure administration subnet has been established between the secure CA subnet and the DMZ. The CRLs and certificates will be published first to a Master Directory in the secure administration subnet before being pushed out to the public repositories in the DMZ. The FPKI system includes an [*Redacted for Security Purposes*]. The servers in the CA subnet can only be accessed via a KVM in the CA secure rack.

The [*Redacted for Security Purposes*] HSM is protected in a locked rack that Officers have the keys for (located inside the locked system room to which only Administrators and the ISSO have unescorted access).

The FPKI Online Repositories in the DMZ are protected by a Firewall that is configured to only allow access to necessary services on the repository systems (DSP, LDAP, and HTTP) and specific machines; all other activity is blocked and recorded.

The FPKI Directories support DSP and LDAP V3 protocols for operation and interoperability of the FPKI Directories, including support for X.500 directory chaining, referrals, and cross-referencing mechanisms. The FPKI Repository also includes web servers supporting HTTP access.

The FPKIMA uses a commercial service to provide external performance monitoring of FPKI Trust Infrastructure Repository performance. In addition FPKIMA manages

[*Redacted for Security Purposes*] monitoring of the content of the FPKI Trust Infrastructure Repository. The combination of the commercial and FPKIMA monitoring provide a countermeasure for Denial of Service attacks. All unused network ports and services are turned off.

The FOS-W and FOS-E sites are [*Redacted for Security Purposes*].

6.8 TIME-STAMPING

System time is maintained using NTP and a local timeserver synchronized with a time server located at NIST. Clock adjustments are auditable events. See Section 5.4.1.

System time will be accurate to within three minutes by being automatically synchronized using NTP.

7 CERTIFICATE, CRL AND OCSP PROFILES

The EAO has defined the Certificate and CRL profiles used by the EGCA. For ease of reference, this CPS includes a selective description in the following Sections.

7.1 CERTIFICATE PROFILE

Certificates issued by the EGCA conform to the X.509 Certificate and CRL Extensions Profile for the EGCA [EGCA-PROF]. EGCA requires Subscriber certificates that conform to the Certificate Profile for eGov Devices or eGov IdPs in [EGCA-PROF].

Self-Signed certificates must conform to the Self-Signed Certificate Profile in [EGCA-PROF].

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

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

The only private extensions included in certificates issued by EGCA are obtained from the PKCS#10 received from the Sponsor. The FPKIMA will verify that no private extension in the certificate is marked critical.

7.1.3 Algorithm Object Identifiers

Certificates issued by the EGCA will use the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates issued by the EGCA will 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 will be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280.

7.1.5 Name Constraints

Certificates by the EGCA will not contain name constraints.

7.1.6 Certificate Policies Extension

Subscriber certificates issued by the EGCA will assert one of the OIDs listed in

Table 7.1-1 in the certificate policies extension, as appropriate:

Table 7.1-1. 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}

The FPKIMA will verify that the certificate policies extension asserts the OID(s) as specified in the LOA.

7.1.7 Usage of Policy Constraints Extension

The EGCA will not assert policy constraints in certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by the EGCA will not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Certificates issued by the EGCA do not contain a critical certificate policy extension.

7.2 CRL PROFILE

CRLs by the EGCA will conform to the CRL Profile specified in [EGCA-PROF].

7.2.1 Version Numbers

The EGCA will issue X.509 Version 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

The FPKIMA does not support Online Certificate Status Protocol (OCSP) capability.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

The FPKIMA will arrange initially and annually for independent inspections and compliance audits to validate that the EGCA is operating in accordance with the security practices and procedures described in this CPS. Results of the compliance audit will be provided to the EAO, in the form of an Auditor Letter of Compliance that follows the guidelines for such a letter found on the FPKIMA documents web site (Auditor Letter of Compliance, Audit Requirements).

As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of CAs and RAs may be carried out in accordance with the requirements as specified in the [Triennial Audit Guidance] which state after an initial compliance audit, subsequent compliance audits require review of previous year's discrepancies, evaluation of modifications and changes made over the last year, core criteria and triennial criteria.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The EGCA compliance audits will be provided by an independent auditor as agreed between the EAO and FPKIMA. The Auditor selected will be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices. The Auditor must perform such compliance audits as a regular ongoing business activity. The Auditor selected will have a demonstrated proven track record in one or more of the following areas:

- Specialization in Electronic Data Processing (EDP) security audit;
- Knowledge and experience with Compliance Audits and PKI;
- Independence from the organization being audited; or
- Understanding of the Federal certification and accreditation process required by OMB A-130 and the Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347).

The selected Auditor will verify and validate through document reviews and demonstrations that the EGCA complies with the [EGCA CP] and requirements that the EAO imposes on the issuance and management of EGCA certificates.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

As required by FISMA, the selected EGCA compliance auditor is a contractor that is independent from FPKIMA, FPKIPA, and Identity, Credential and Access Management Subcommittee (ICAMSC). This contractor provides an unbiased, independent evaluation and is one whose primary responsibility is the performance of EDP Compliance Audits.

To ensure independence and objectivity, the compliance auditor may not have served the FPKIMA in developing or maintaining the EGCA's Facility or certificate practices statement.

8.4 TOPICS COVERED BY ASSESSMENT

The compliance audit will address all aspects of the EGCA operation or that portion specified for a given year in accordance with the Triennial Audit Guidance document. The compliance audit will verify that EGCAs are operated in compliance with all the requirements of the current version of the EGCA CP and this CPS.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The EGCA compliance auditor will notify, within 24 hours after the conclusion of the compliance audit, the FPKIMA of the results of the compliance audit by e-mail and/or out-of-band writing.

The FPKIMA will provide the audit results to the EAO and in consultation with the EAO will have 10 business days to review the results and the recommendations from the compliance audit to determine the action to be taken.

Based on the findings of the EGCA compliance auditor, a Plan of Action and Milestones (POA&M) will document what steps must be taken. Possible steps include:

- Correction of deficiencies prior to implementing full operation of the EGCA or within another time period as determined by the EAO, FPKIPA and FPKIMA;
- Suspension of full operation of the EGCA (this alternative will execute the emergency procedure described in Section 4.9.1 for revocation of certificates);
- The FPKI Management Authority shall determine what further notifications or actions are necessary to meet the requirements of this CP, and then proceed to make such notifications and take such actions without delay;
- Execute other corrective actions through procedures developed and published by the EAO; and
- Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the EAO may direct the FPKIMA to take additional actions as appropriate, including temporarily halting operation of the EGCA.

8.6 COMMUNICATION OF RESULTS

The selected compliance auditor will communicate results of a compliance audit of the EGCA to the FPKIMA and EAO within 24 hours upon the conclusion of the compliance audit by a signed e-mail and/or in writing. The results will be provided as a written report. The report will contain a summary table of topics covered, areas in which EGCA was found to be non-compliant, a brief description of the problem(s) for each area of non-compliance, and possible remedies for each area. The report will also contain the detailed results of the compliance audit for all topics covered, including the topics in which the EGCA passed and the topics in which the EGCA failed. A comprehensive report may be provided later.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

The FPKIPA and EAO reserve the right to charge a fee to each Sponsor in order to support operations of the EGCA.

9.1.1 Certificate Issuance or Renewal Fees

At this time, the FPKIMA does not charge a fee for certificate issuance or renewal.

9.1.2 Certificate Access Fees

At this time, the FPKIMA does not charge a fee for certificate access.

9.1.3 Revocation or Status Information Access Fee

At this time, the FPKIMA does not charge a fee for access to certificate revocation or status information.

9.1.4 Fees for Other Services

At this time, the FPKIMA does not charge a fee for any other services.

9.1.5 Refund Policy

At this time, since there are no fees associated with FPKIMA services, there is no refund policy in place.

9.2 FINANCIAL RESPONSIBILITY

This CPS contains no limits on the use of any certificates issued by the EGCA or by Subscribers. Rather, entities acting as Relying Parties shall determine what financial limits, if any, they wish to impose for certificates used to complete a transaction.

9.2.1 Insurance Coverage

The EGCA does not provide any insurance or warranty coverage for the use of any certificates issued by the EGCA.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

EGCA information not requiring protection is publicly available in the FPKI repositories, the FPKIPA web site, or the FPKIMA web site. EAO access to Subscriber information is addressed in the Subscriber agreement with that Subscriber. Public access to Subscriber information is determined by the respective Subscriber.

9.3.1 Scope of Confidential Information

The FPKIMA does not maintain any confidential information about Subscribers.

9.3.2 Information Not Within the Scope of Confidential Information

The [EGCA CP] does not stipulate requirements for this Section.

9.3.3 Responsibility to Protect Confidential Information

The EGCA does not maintain any confidential information about Subscriber POCs.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

The initial FPKIMA Privacy Impact Assessment determined there was no requirement for a Privacy Plan as no personal data/information is collected on the general public or government employees.

9.4.2 Information Treated as Private

The following information collected from Subscribers will be kept confidential: information on the agency Sponsor identity card that is not required to be made public (e.g., driver license number, passport number, social security number) and agency registration information. The certificate issuance paper files are stored in the server room, a locked facility with access only by those in trusted roles.

Information stored on the EGCA workstations is protected by password, workstations are located in a secure data center, physical access to the workstations is limited to those in Trusted Roles, and security and access control settings are applied through group policies.

9.4.3 Information Not Deemed Private

Information included in EGCA certificates is not subject to protections outlined in Section 9.4.1.

9.4.4 Responsibility to Protect Private Information

Sensitive information is stored securely and released only in accordance with the provisions of Section 9.4.2.

9.4.5 Notice and Consent to Use Private Information

The FPKIMA does not maintain Subscriber private information, and therefore is not required to provide any notice to or obtain consent from the Subscriber in order to use private information in accordance with the stipulations of Section 9.4.6.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The EGCA will disclose confidential information to any third party when required by this CPS, [EGCA CP], by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information will be authenticated. The authentication will consist of validating the identity of the requester using two forms of photo identifications. The individual's authority to obtain the information will be validated using at least one of the following means:

- The individual has the duly-executed court order from a Federal court;
- The individual has duly-executed request from the respective Agency Office of Inspector General;

- The individual is the Subscriber itself; or
- The individual has a duly-signed request from the Sponsor requesting the release of the information from the Subscriber.

In compliance with 41 CFR 105-60.605, the FPKIMA PM will be notified of any validated requests for disclosure of confidential information. The FPKIMA PM will notify the Appropriate Authority.

9.4.7 Other Information Disclosure Circumstances

There are no other disclosure circumstances.

9.5 INTELLECTUAL PROPERTY RIGHTS

The U.S. Government retains exclusive rights to any products or information developed under or pursuant to this EGCA CPS.

9.6 REPRESENTATIONS AND WARRANTIES

The obligations described below pertain to the EGCA (and, by implication, the FPKIMA. Thus, where the obligations include, for example, a review (or audit) by the EAO or some other body, the purpose of that review pertains to interoperability using the EGCA.

9.6.1 CA Representations and Warranties

EGCA certificates are issued and revoked at the sole discretion of the EAO. When the EGCA issues a certificate to a non-federal entity, it does so for the convenience of the U.S. Federal Government. The FPKIMA warrants that EGCA operational procedures comply with this CPS and [EGCA CP].

9.6.2 RA Representation and Warranties

The FPKIMA makes no representation or warranty that the information in a certificate is accurate other than it matches the information specified in the LOA authorizing the issuance of that certificate.

9.6.3 Subscriber Representations and Warranties

The Sponsor will sign an agreement stating they will accurately represent themselves in all communications with FPKI authorities and other Sponsors.

9.6.4 Relying Parties Representations and Warranties

The FPKIMA makes no representation or warranty about the use of certificates for Relying Parties.

9.6.5 Representations and Warranties of Other Participants

The FPKIMA makes no representation or warranty for other participants.

9.7 DISCLAIMERS OF WARRANTIES

The FPKIMA does not disclaim any responsibilities described in the [EGCA CP].

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

The EGCA CPS does not include any claims of indemnity.

9.10 TERM AND TERMINATION

9.10.1 Term

This CPS becomes effective when approved by the EAO. This CPS has no specified term.

9.10.2 Termination

Termination of this CPS is at the discretion of the EAO.

9.10.3 Effect of Termination and Survival

The requirements of the [EGCA CP] remain in effect through the end of the archive period for the last certificate issued.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The FPKIMA uses the POC information provided by the EAO in the LOA and as updated by Sponsors to communicate with those entities. The FPKIPA listservs maintained by the FPKIMA on behalf of the FPKIPA may also be used for communications to entities.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The FPKIMA shall review the EGCA CPS at least once every year, or when a change is made to the [EGCA CP]. If the FPKIMA determines modifications to this CPS are required, the change, a change justification and contact information for the person requesting the change will be presented to the EAO for review and acceptance.

9.12.2 Notification Mechanism and Period

The [EGCA CP] and any subsequent changes shall be made publicly available.

9.12.3 Circumstances under which OID must be changed

If the EAO determines that there is a requirement to change the OIDs defined in the

[EGCA CP], the EAO will amend the [EGCA CP].

9.13 DISPUTE RESOLUTION PROVISIONS

The EAO will resolve any disputes associated with the use of the EGCA or certificates issued by the EGCA.

9.14 GOVERNING LAW

The construction, validity, performance and effect of certificates issued under this CPS for all purposes are governed by United States Federal law (statute, case law or regulation).

9.15 COMPLIANCE WITH APPLICABLE LAW

The FPKIMA will comply with applicable law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

There are no additional miscellaneous provisions on this CPS.

9.16.2 Assignment

The EGCA CPS does not assign rights or responsibilities other than what is specified in this CPS and the [EGCA CP].

9.16.3 Severability

Should it be determined that one Section of this CPS is incorrect or invalid, the other Section of this CPS shall remain in effect until the CPS is updated. The process for updating this CPS is described in Section 9.12.1.

9.16.4 Enforcement (Attorney's Fees or Waiver of Rights)

Failure by any person to enforce a provision of this CPS will not be deemed a waiver of future enforcement of that or any other provision.

9.17 OTHER PROVISIONS

This CPS does not stipulate any additional provisions.

Appendix A References

ABADSG	Digital Signature Guidelines, 1996-08-01 http://www.abanet.org/scitech/ec/isc/dsgfree.html
EGCA-Prof	X.509 Certificate and CRL Extensions Profile for EGCA, March 2, 2011.
EGCA CP	X.509 Certificate Policy for the E-Governance Certification Authorities http://www.idmanagement.gov/fpkipa/documents/EGovCA-CP.pdf
EGTS Application and Issuance	E-Governance Trust Services (EGTS) Certificate Application and Issuance Process
FPKI Security Profile	FPKI Security Controls Profile of Special Publication 800-53, Security Controls for PKI Systems http://www.idmanagement.gov/fpkipa/documents/FPKI_Profile_SP80053_PKI_Security_Controls.pdf
FPKIMA IMP	Federal Public Key Infrastructure Management Authority (FPKIMA) Incident Management Plan
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
NIST SP 800-53	Recommended Security Controls for Federal Information Systems and Organizations http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999
PKCS#7	Cryptographic Message Syntax Standard http://www.rsa.com/rsalabs/node.asp?id=2129
PKCS#10	Certification Request Syntax Standard http://www.rsa.com/rsalabs/node.asp?id=2132
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999 http://www.ietf.org/rfc/rfc2510.txt

RFC 3280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Housley et al., April 2002. http://www.ietf.org/rfc/rfc3280.txt
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 http://www.ietf.org/rfc/rfc3647.txt
FPKI SSP	Federal Public Key Infrastructure (FPKI) Trust Infrastructure System Security Plan
Triennial Audit Guidance	Triennial Compliance Audit Requirements http://www.idmanagement.gov/fpkipa/documents/TriennialAnnualAuditGuidance.pdf