Public X.509
U.S. Federal PKI Architecture
Certification Practice Statement

13 September 2005

FOREWORD

This Certification Practice Statement (CPS) documents the internal practices and procedures used by the Federal Public Key Infrastructure Operational Authority (FPKI OA) by describing the practices concerning lifecycle services in addition to issuance, such as certificate management (including publication and archiving), revocation, and renewal or re-keying for the United States Federal PKI Architecture (FPKIA).

The FPKIA is the central element of the United States Federal PKI implementation and provides support to the E-Authentication Service Component (ASC) of the Federal Enterprise Architecture. The implementation of the FPKIA encompasses multiple Certificate Authorities (CAs), each implementing a separate FPKI or ASC certificate policy, as well as one common directory/repository architectural structures.

The FPKIA CPS includes four parts, which are as follows:

- U.S. Certification Practice Statement - Part 1:
  X.509 Certification Practice Statement for the Federal Bridge Certification Authority
- U.S. Federal PKI Architecture Certification Practice Statement - Part 2:
  X.509 Certification Practice Statement for the Federal PKI Common Policy Framework Certification Authority
- U.S. Federal PKI Architecture Certification Practice Statement - Part 3:
  X.509 Certification Practice Statement for the E-Governance Certification Authority
- U.S. Federal PKI Architecture Certification Practice Statement - Part 4:
  X.509 Certification Practice Statement for the Citizen and Commerce Class Common Policy Certification Authority

Table of Contents

1. GENERAL INTRODUCTION

A Public Key Infrastructure (PKI) consists of products and services that provide and manage X.509 certificates for public key cryptography. In general, certificates identify the individual named in the certificate and bind that person to a particular public/private key pair. A certificate policy (CP) describes the policies and procedures that are used to verify the binding before certificates are issued, and the maintenance of that binding. A CPS, on the other hand, describes how the CA and the other stakeholders implement procedures and controls to meet the requirements stated in the CP. In other words, the purpose of the CPS is to disclose how the all stakeholders perform their functions and implement controls.

This CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) request for comments (RFC) 2527, CP and Certification Practice Statement Framework.

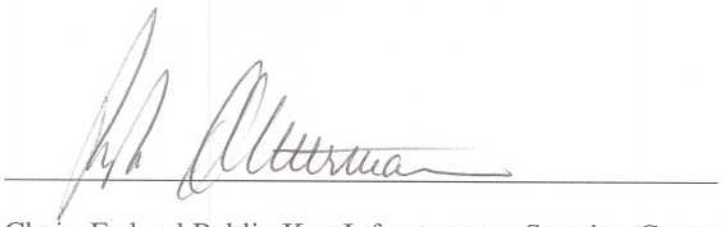
Part 1: X.509 Certification Practice Statement (CPS) For the Federal Bridge Certification Authority (FBCA)

United States Federal PKI Architecture

Federal PKI Architecture X.509 Certification Practice Statement – Part 1: Public X.509 Certification Practice Statement (CPS) For The Federal Bridge Certification Authority (FBCA)

13 September 2005

Signature Page



Chair, Federal Public Key Infrastructure Steering Committee

DATE

Table of Contents

List of Tables

RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	DATE RECEIVED	DATE ENTERED	SIGNATURE OF PERSON ENTERING CHANGE
001	August 2004	August 2004	August 2004	FBCA OA

1. FBCA CPS INTRODUCTION

The Certification Practice Statement (CPS) for the FBCA is part one (1) of the FPKIA CPS and it documents the internal practices and procedures used by the Federal Public Key Infrastructure Operational Authority (FPKI OA) by describing the practices concerning lifecycle services in addition to issuance, such as certificate management (including publication and archiving), revocation, and renewal or re-keying.

The FBCA is a certification authority (CA) that solves the technical interoperability challenge of the Federal PKI to meld individual entity initiatives that use PKI products from a variety of commercial vendors into a Federal PKI and implements certificate based assurance for the FPKI architecture and the E-Authentication technical architecture approach.

The internal practices and procedures to operate the FBCA comply with the requirements, policy and procedures set forth in the X.509 Certificate Policy for the Federal Bridge Certification Authority, dated 10 September 2002 (FBCA CP).

This FBCA CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework.

1.1 OVERVIEW

1.1.1 Certification Practice Statement (CPS)

This Certification Practice Statement (CPS) documents the internal practices and procedures used by the Federal PKI Architecture (FPKIA) Operational Authority (OA). It covers the operation of systems and the management of facilities, which includes the FBCA and the FPKIA repository functionality, used to facilitate interoperability between the FBCA and other Entity PKI domains.

1.1.2 Relationship Between the FBCA CPS and the FBCA CP

The FBCA CP states what assurance can be placed in a certificate issued by the FBCA. The FBCA CPS describes how the FPKI OA practices and procedures establish that assurance.

1.1.3 Relationship Between the FBCA CP and the Entity CP

The levels of assurance of the certificates issued under the FBCA CP are mapped by the FPKIPA to the levels of assurance of the certificates issued by Entity CAs. The policy mappings information is placed into the certificates issued by the FBCA, or otherwise published or used by the FPKI OA (described in section 1.3.1.2) so as to facilitate interoperability.

1.1.4 Interaction with PKIs External to the Federal Government

The FBCA exists to facilitate trusted electronic business transactions for federal organizations. To facilitate the missions of the organizations, interoperability is offered to non-federal entities. The generic term "entity" applies equally to federal organizations and other organizations owning or operating PKI domains. As used in this CP, Entity PKI or Entity CA may refer to an organization's PKI, a PKI provided by a commercial service, or a bridge CA serving a community of interest.

The FBCA will extend interoperability with non-federal entities only when it is beneficial to the federal government.

1.2 IDENTIFICATION

This CPS supports the five levels of assurance which are defined the FBCA CP. Each level of assurance has an Object Identifier (OID), to be asserted in certificates issued by the FBCA. The OIDs are registered under the id-infosec arc as follows:

fbca-policies OBJECT IDENTIFIER	::= {csor-certpolicy 3}
csor-certpolicy OBJECT IDENTIFIER	::= {2 16 840 1 101 3 2 1 }
id-fpki-certpcy-rudimentaryAssurance	::= fbca-policies 1
id-fpki-certpcy-basicAssurance	::= fbca-policies 2
id-fpki-certpcy-mediumAssurance	::= fbca-policies 3
Id-fpki-certpcy-highAssurance	::= fbca-policies 4
id-fpki-certpcy-testAssurance	::= fbca-policies 5

This CPS is referred to as the FBCA CPS.

1.3 COMMUNITY AND APPLICABILITY

1.3.1 PKI Authorities

The following table summarizes the roles relevant to the administration and operation of the FBCA. These roles are entirely defined in the FBCA CP.

Table 1.3.1-1. FBCA Roles

FBCA Role	Description
Federal Chief Information Officers Council	The Federal CIO Council comprises the Chief Information Officers of all cabinet level departments and other independent agencies. The Federal CIO Council has established the framework for the interoperable Federal PKI, and that includes overseeing the operation of the organizations responsible for governing and promoting its use. In particular, the FBCA CP and CPS are established under the authority of and with the approval of the Federal CIO Council.
Federal PKI Policy Authority (FPKIPA)	The FPKIPA is a group of U.S. Federal Government Agencies (including cabinet-level Departments) established pursuant to the Federal CIO Council. The FPKIPA includes representatives of the Agencies that execute a MOA with the FBCA. The FPKIPA is responsible for: • The Federal Bridge Certification Authority (FBCA) Certificate Policy (CP), • The FBCA Certification Practice Statement (CPS), • Accepting applications from Entities desiring to interoperate using the FBCA, • Determining the mappings between certificates issued by applicant Entity CAs and the levels of assurance set forth in the FBCA CP (which will include objective and subjective evaluation of the respective CP contents and any other facts deemed relevant by the FPKIPA), and • After an Entity is authorized to interoperate using the FBCA, ensuring continued conformance of that Entity with applicable requirements as a condition for allowing continued interoperability using the FBCA.
FPKI Operational Authority (FPKI OA)	The FPKI Operational Authority (OA) is the organization that operates the FPKIA CAs. In particular it operates the FBCA, including issuing FBCA certificates when directed by the FPKIPA, posting those certificates and Certification Authority Revocation Lists (CARLs) into the FPKIA repository, and ensuring the continued availability of the repository to all users.
FPKI OA Administrator	The Administrator is the individual within the FPKI OA who has principal responsibility for overseeing the proper operation of the FPKIA CAs including the FPKIA repository.
FPKI OA Officers	These officers are the individuals within the FPKI OA, selected by the ISSO who operate the FBCA and its repository including executing FPKIPA direction to issue FBCA certificates to Entity PCAs or taking other action to affect interoperability between the FBCA and Entity PCAs. The roles include FPKI OA Security Officer, Auditor, and Operator, all described in the FBCA CPS, section 5.2.1.
Entity Principal Certification Authority	The Entity PCA is an entity within a PKI that has been designated to interoperate directly with the FBCA (e.g., through the exchange of

FBCA Role	Description
(Principal CA)	cross-certificates), and which issues either end-entity certificates, certificates, or cross-certificates (or other means of interoperation) to other Entity or external party CAs, or both. It should be noted that an Entity might request that the FBCA interoperate with more than one CA within the Entity; that is, an Entity may have more than one Principal CA. The use of this term shall encompass any CA under the control of the Entity that has a certificate issued to it by the Entity PCA or any CA subordinate to the Principal CA, whether or not the Entity employs a hierarchical or other PKI architecture.
Federal Bridge Certification Authority (FBCA)	The FBCA is the entity operated by the FPKI OA that is authorized by the FPKIPA to create, sign, and issue public key certificates to Entity PCAs. As operated by the FPKI OA, the FBCA is responsible for all aspects of the issuance and management of a certificate including: • Control over the registration process, • The identification and authentication process, • The certificate manufacturing process, • Publication of certificates, • Revocation of certificates, • Re-key of FBCA signing material, and • Ensuring that all aspects of the FBCA services and FBCA operations and infrastructure related to certificates issued under the FBCA CP are performed in accordance with the requirements, representations, and warranties of the FBCA CP.
Registration Authority (RA)	The RA is the entity that collects and verifies each Subscriber's identity and information that are to be entered into his or her public key certificate. The FPKI OA acts as the RA for the FBCA, and performs its function in accordance with a CPS approved by the FPKIPA.
Related Authorities	The FBCA operating under the FBCA CP will require the services of other security, community, and application authorities, such as compliance auditors, information systems security officer (ISSO) and information systems security manager (ISSM), and attribute authorities. This FBCA CPS identifies the parties responsible for providing such services, and the mechanisms used to support these services.
End Entities	Subscribers A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the Certificate Policy asserted in the certificate, and who does not it issue certificates. FBCA Subscribers include only FPKI OA personnel and, when determined by the FPKIPA, possibly certain

FBCA Role	Description
	network or hardware devices such as firewalls and routers when needed for infrastructure protection. CAs is sometimes technically considered “subscribers” to a PKI. However, the term “Subscriber” as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information. Relying Parties A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

The FPKIPA will enter into a Memorandum of Agreement (MOA) (a template MOA is posted at the FPKIPA website http//www.cio.gov/fpkipa) with an Entity setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in the FBCA CP and those in the Entity CP. When the entity belongs to a sovereign nation, the United States Department of State may execute the MOA or delegate the authority to execute the MOA on its behalf.

1.3.2 Applicability

The FBCA does not issue certificates to end-entity subscribers as defined in section 1.3.1; the FBCA only issues certificates to Entity PCAs (cross-certificates) and issues CRLs and CARLs relating to those certificates.

As a key critical infrastructure component, the FPKI OA operates the FBCA at system high level of assurance. The FBCA issues at least one certificate that asserts mapping to the high assurance level, so the FBCA is operated at that level. As described in the FBCA CP, that level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. Note that the data in such transactions NEVER traverses the FBCA infrastructure component.

The FBCA is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statues and regulations. Each Entity specific MOA will identify the level(s) of assurance associated with that Entity.

1.3.2.1 Factors in determining usage

The Relying Party must first determine the level of assurance required for an application, and then select the certificate appropriate for meeting the needs of that application. This will be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the FPKIPA or the FPKI OA.

The FBCA CP contains some helpful guidance, which Relying Parties may consider in making their decisions. Further, Relying Parties should review more detailed guidance governing the use of electronic signatures (which include the use of digital certificates) issued by the Office of Management and Budget implementing the Government Paperwork Elimination Act (Federal Register May 2000: Volume 65, Number 85, Page 25508), as well as more detailed subordinate guidance issued by other Entities pursuant to OMB direction (such as NIST Special Publication 800-25 covering the technical elements of using digital signatures).

1.4 CONTACT DETAILS

1.4.1 Specification administration organization

The FPKIPA is responsible for the maintenance and all aspects of this CPS.

1.4.2 Contact person

Direct all questions regarding this CPS to the Chair of the FPKIPA, whose address can be found at http://www.cio.gov/fpkipa.

1.4.3 Person determining Certification Practice Statement suitability for the policy

The FPKIPA is responsible for determining suitability of this CPS for the FBCA CP.

2. GENERAL PROVISIONS

2.1 OBLIGATIONS

The FPKI OA will abide with the obligations defined in the FBCA CP, by following and implementing the procedures defined in this CPS.

2.1.1 CA Obligations

The FPKI OA, which operates the FBCA, will abide with the obligations defined in the FBCA CP, by following and implementing the procedures defined in this CPS.

2.1.1.1 Sample FBCA Memorandum of Agreement (MOA)

The latest draft of the MOA template can be downloaded from the FPKIPA web site at http://www.cio.gov/fpkipa/library.htm

2.1.2 RA Obligations

The FPKI OA is the RA for the FBCA and is responsible for controlling the registration process, including collecting and verifying the information to be entered into the certificates issued by the FBCA.

2.1.3 Subscriber Obligations

The only potential FBCA subscribers identified are the FPKI OA Administrator and the FPKI OA Security Officers. There are no other FBCA subscribers. The FBCA, however does not issue certificates to end-entity subscribers, rather it merely issues cross-certificates with Entity PCAs, which are not technically deemed as end-entity subscribers.

2.1.4 Relying Party Obligations

The Relying Party decides, pursuant to its own Entity's policies, what steps to take. The FBCA merely provides the tools needed to perform the trust path creation, validation, and certificate policy mappings which the Relying Party may wish to employ in its determination.

2.1.5 Repository Obligations

The FPKI OA operates and uses a variety of mechanisms for posting information into a repository as required by the FBCA CP. The mechanisms supported and operated include:

- Configuring and maintaining a repository (X.500, Lightweight Directory Access Protocol (LDAP)) for all FPKIA CAs; however, each uses its own internal database.

- Maintaining a separate online X.500 Directory Service System supporting LDAP v2 or better, as directed by the FPKIPA, which allows authorized access and retrieval of the certificate information, including all cross-certificates and the status of all cross-certificates issued by the FBCA, and

- Providing administrative access control mechanisms when needed to protect repository information as described in later sections.

The FPKIPA will be maintaining a web server (see section 2.6.4) to post FPKIA for official use only (FOUO) documentation, including the CP, CPS, and FPKIPA procedural documents.

2.1.6 Certificate Issuance to Non-US Government Parties

The FBCA may issue end-entity certificates to contractors and parties regulated by Federal agencies, for the convenience of the Government when those parties have a bona fide need to possess a certificate issued by the FBCA, as established by the FPKIPA. The FBCA issues such end-entity certificates only to FPKIA security officers in support of their activity of administering the FBCA on behalf of GSA. In each such case, a Memorandum of Agreement or similar instrument will be executed, and will contain whatever provisions are determined appropriate by the FPKIPA.

2.2 LIABILITY

Certificates are issued and revoked at the sole discretion of the Federal PKI Policy Authority. When the FBCA issues a cross-certificate to a non-federal entity, it does so for the convenience of the federal government. Any review by the FBCA of a non-federal entity's certificate policy is for the use of the FBCA in determining whether or not interoperability is possible, and if possible, to what extent the non-federal entity's certificate policy maps to the FBCA policy. A non-federal entity must determine whether that entity's certificate policy meets its legal and policy requirements. Review of a non-federal entity's certificate policy by the FBCA is not a substitute for due care and mapping of certificate policies by the non-federal entity.

Entities, acting as Relying Parties, are responsible for determining what financial limits, if any, they wish to impose for certificates used to consummate a transaction. This is entirely at the discretion of the Entity as Relying Party and is likely to depend upon several factors in addition to the certificate assurance level (e.g., likelihood of fraud, other procedural controls, Entity-specific policy or statutorily imposed constraints).

As an example, one Entity may be willing to accept a FBCA Basic assurance level certificate for transactions of a specific financial value for which another Entity would require a FBCA High assurance level certificate.

The FBCA is not financially responsible for any losses incurred from using its services.

2.2.1 Indemnification by Relying Parties and subscribers

The FBCA CP does not stipulate a requirement for this section.

2.2.2 Fiduciary relationships

No fiduciary is intended or should be deemed to arise out of any provision of this CPS.

2.2.3 Administrative processes

Administrative processes set forth by this CPS are determined by the FPKI OA pursuant to the agreement between it and the FPKIPA for the operation of the FBCA.

2.3 INTERPRETATION AND ENFORCEMENT

2.3.1 Severability of Provisions, Survival, Merger, and Notice

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 8.1.

2.3.2 Dispute resolution procedures

The FPKIPA will resolve any disputes associated with the use of the FBCA or certificates issued by the FBCA.

2.4 FEES

The FPKI OA will determine the fees, if any, for FBCA services, as approved by the FPKIPA.

2.5 PUBLICATION AND REPOSITORY

2.5.1 Publication of CA Information

The FPKI OA will deliver this CPS to the FPKIPA and any relevant authority in the Federal government. It will make a redacted version of this CPS publicly available on the FBCA web site described in section 2.6.4.

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" (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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

The FPKI OA will publish information concerning the FBCA necessary to support its use and operation, including:

- The cross-certificates it issues;
- The CRLs and CARLs it issues;
- The Certificate for its certificate signing key;
- This CPS; and
- The FBCA CP, and any waivers granted by the FPKIPA.

2.5.2 Frequency of Publication

Certificates are published following certificate issuance as specified in section 4.2. The CRL is published as specified in section 4.4.

2.5.3 Access controls

The web site publishing this CPS enables a read-only access to the FBCA CPS. Only authorized personnel have access to modify the CPS. The procedure for updating the documents on the web server consists of an out-of-band mechanism. The FPKIA online directory servers reside behind a firewall protecting the FPKIA from the Internet. The public anonymous read access to its information is enabled. Only authorized FPKI OA personnel can update the information stored in this server. Access controls are set by administrative function and assigned roles/responsibilities, and enforced using password-based authenticated subject identity.

The procedures for issuing and updating the cross-certificates, CRLs, and CARLs generated by the FBCA require multi-person access controls. FPKIA internal repository updates are pushed to the online FPKIA directory through the internal one-way firewall. The FBCA is enabled to issue and revoke cross-certificates to Entity PCAs and to generate periodic CARLs/CRLs. Directories are protected from unauthorized modification, requiring a user name and password in order to make updates. Anonymous access is provided via LDAP (port 389) to the public. Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

2.5.4 Repositories

The FPKIA includes an online X.500 Directory Service supporting LDAP V2 operations for the purpose of publishing Entity PCAs cross-certificates, the possible FBCA self-signed certificates, CRLs and CARLs.

The FBCA also provides a web site to publish other FBCA information, including the redacted public version of this CPS and the FBCA CP. Access to the entire CPS is granted only to Entities authorized by the FPKIPA.

Purpose	Network Address
X.500 LDAP V2 or better Directory (LDAP external)	Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.
X.500 or better Directory	Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.
FBCA CPS Website	http://www.cio.gov/fpkipa
FBCA CP Website	http://www.cio.gov/fpkipa
FBCA Interoperability Guidelines	http://www.cio.gov/fpkipa

2.6 COMPLIANCE AUDIT

2.6.1 Frequency of Entity Compliance Audit

The FPKI OA will arrange initially and annually for independent inspections and compliance audits to validate that the FBCA is operating in accordance with the security practices and procedures described in this CPS. Results of the compliance audit will be provided to the FPKIPA.

2.6.2 Identity/Qualifications of Compliance Auditor

The FBCA compliance audits will be provided by an independent auditor as agreed between the FPKIPA and FPKI OA, which has demonstrated a proven track record in one or more of the following areas:

- Specialization in EDP security audit
- Knowledge and experience with Compliance Audits and PKI
- Independence from the organization being audited
- 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 FPKI PA has chosen the following organization to conduct the compliance audit:

Name of the Auditor Organization: KPMG

The selected auditor will verify and validate through document reviews and demonstrations that the FBCA complies with the FBCA CP and requirements that the FPKIPA imposes on the issuance and management of FBCA certificates.

2.6.3 Compliance Auditor's Relationship to Audited Party

As required by the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, the selected FBCA compliance auditor is a contractor that is independent from FPKI OA, FPKI PA, and FPKI Steering Committee. This contractor provides an unbiased, independent evaluation and is one whose primary responsibility is the performance of EDP Compliance Audits.

2.6.4 Topics Covered by Compliance Audit

The compliance audit will address all aspects of the FBCA operation. The scope of the compliance audit includes all practices described in this CPS and other FPKIPA requirements.

2.6.5 Actions taken as a result of deficiency

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

The FPKI OA will provide the audit results to FPKIPA and in consultation with FPKIPA 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 FBCA compliance auditor, the possible courses of actions include:

- Correction of deficiencies prior to implementing full operation of the FBCA or within another time period as determined by the FPKIKPA and FPKI OA
- Suspension of full operation of the FBCA (this alternative will execute the emergency procedure described in section 4.1.1.2 for revocation of certificates),
- Execute other corrective actions through procedures developed and published by the FPKIPA.

In the event of deficiencies on the part of the Entity PCA, the FPKIPA may direct the FPKI OA to suspend interoperations with that Entity PCA by revoking cross-certificates issued to that Entity (this alternative will execute the revocation procedure described in section 4.1.1.2), or take other actions it deems appropriate.

2.6.6 Communication of Result

The selected compliance auditor will communicate results of a compliance audit of the FBCA to the FPKI OA and FPKIPA 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 FBCA 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 FBCA passed and the topics in which the FBCA failed. Notification of compliance audit failure, the topics of failure, reason(s) for failure, and possible remedies will be provided within 24 hours, upon the conclusion of the compliance audit, in a written form (signed e-mail and/or out of band letter) to the FPKI OA and to the FPKIPA. A comprehensive report may be provided later.

2.7 CONFIDENTIALITY

FBCA information not requiring protection is publicly available. Federal PKI Policy Authority access to Entity information is addressed in the MOA with that Entity. Public access to Entity information is determined by the respective Entity.

2.7.1 Types of Information to be Protected

The following information collected from the Entity PCAs will be kept confidential: MOAs, FBCA passwords and private signature keys, 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, etc.) and agency registration information

Information stored on the FBCA workstations is protected by password.

2.7.2 Information Release Circumstances

The FBCA will disclose confidential information to any third party when required by this CPS, FBCA 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 subscriber requesting the release of the information from the subscriber

Court orders and IG requests must be approved by specific Entity General Counsel

2.8 INTELLECTUAL PROPERTY RIGHTS

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

3. IDENTIFICATION AND AUTHENTICATION

This section contains the practices the FPKI OA follows in identifying and Entity PCAs and sponsors involved in the cross certification request process.

3.1 INITIAL REGISTRATION

An Entity registration to the FBCA service is initiated by applying to the FPKIPA to obtain a cross-certificate from the FBCA to the Entity PCA. This application is done using a form supplied by the FPKIPA (available on its web site, http://www.cio.gov/fpkipa that must be filled in by the completed and signed by an authorized official of the Entity (as established on the form). The application contains how the Entity proposes to map the certificate levels of assurance present in the Entity's CP to the levels expressed in the FBCA CP, and how the Entity's certificate profile conforms to the Federal Certificate Profile (available at the FPKIPA web site cited above). The application also describes how the applicant Entity's PKI has been independently audited to ensure conformance by the applicant to its own CP and CPS.

The FPKIPA will evaluate the application and either will accept the policy mapping proposed by the applicant or propose an alternative mapping. If the applicant accepts the alternative mapping, the FPKIPA will execute with the applicant a Memorandum of Agreement (MOA) that reflects the respective responsibilities of the FPKIPA and the Entity along with the policy mappings. After the MOA is signed by the parties, the FPKIPA notifies the FPKI OA to initiate the process for issuing cross-certificates to the Entity PCA and establishing interoperability with the FBCA directory.

3.1.1 Types of names

The FBCA generates and signs certificates where the issuer DN consists of a set of the following X.520 naming elements: C; O; OU; and CN. Certificates may additionally assert an alternate name form subject to requirements set forth below which are intended to ensure name uniqueness.

The FBCA generates and signs certificates where the subject DN contains X.520 naming elements (at least C, O, and OU), the domain component naming element (dc), or a combination of the two.

Test	The Test level of assurance is used by the FBCA prototype bridge and CAs when conducting interoperability testing. The production FBCA does not issue certificates with the Test level of assurance.
Rudimentary	Non-Null Subject Name, or Null Subject Name if Alternative Subject Name is populated and marked critical
Basic	Non-Null Subject Name, and optional Alternative Subject Name if marked non-critical
Medium	X.500 Distinguished Name, and optional Alternative Subject Name if marked non-critical
High	X.500 Distinguished Name, and optional Alternative Subject Name if marked non-critical

The certificates issued to Entity PCAs have an assurance level equal to the highest level of assurance contained in the policy mappings as agreed between the FPKIPA and the Entity PCA.

3.1.2 Need for names to be meaningful

The FBCA supports the generation and publication of cross-certificates with Entity PCAs. Names used in the certificates will identify the person or object to which they are assigned in a meaningful way. The certificates issued by the FBCA contain the relative distinguished name (RDN) of C=US, O=U.S. Government, OU=FBCA, OU= Entrust.

The FBCA operating under the FBCA CP and described in this CPS issue and sign certificates with subject names from within the name-space C=US, O=U.S. Government. For example, the Entity PCA RDN for a certificate issued to the Entity PCA for NIST could be C=US, O=U.S. Government, OU=NIST, OU=Experimental CA1.

Additionally, the FBCA operating under the FBCA CP and described in this CPS may issue and sign certificates with subject names from other name spaces as directed explicitly by the FPKIPA.

The FBCA issues all the Medium or High Assurance levels certificates with name constraints asserted limiting the name space of the Entity PCAs to that appropriate for their domains. Additionally, the FPKIPA may require that such constraints be implemented for the certificates issued at the Test, Basic or Rudimentary levels if it deems appropriate.

3.1.3 Rules for interpreting various name forms

The FBCA certificate profile established by the FPKIPA contains the rules for interpreting name forms. The FBCA certificate profile supports the DN, RFC822, and DCN name forms. The FBCA certificate profile can be found in the FBCA Interoperability Guidelines, which are posted at the FBCA web site (see Section 2.6.4)

3.1.4 Uniqueness of names

The FPKI PA manages the name uniqueness across the FBCA. Names, whether X.500 DNs or other name forms (e.g., an electronic mail address or DNS name), will be assigned by the FPKIPA and made unique. Additionally, the CAs in the FBCA membrane are configured to require name uniqueness when issuing cross-certificates to Entity PCAs. No other name forms other than DN and DC naming are supported.

3.1.5 Name claim dispute resolution procedure

Naming collisions that affect interoperability with the FBCA will be brought to the attention of the FPKIPA for resolution. The FPKI OA will revoke and re-issue all affected certificates as directed by the FPKIPA.

3.1.6 Recognition, authentication and role of trademarks

The FBCA CP stipulates no requirements for this section.

3.1.7 Method to prove possession of private key

The FPKI OA verifies that a cross-certificate applicant possesses the private key corresponding to the public key submitted with the application in accordance with section 4.2. All transactions involved in cross-certificate issuance are recorded as part of the security audit data, as described in section 4.5.1. Since the FBCA is at all times off-line, these messages are exchanged using an out-of-band mechanism as described in section 4.2. The signed PKCS#10 is used to determine proof of possession of the private key. Shared secrets are not used.

The FPKIA does not provide hardware tokens to subjects. The FPKIA generates a certificate based on the PKCS#10 and returns the certificate via out-of-band mechanisms as described in SO01 – Certificate Issuance.

PCAs personal information will be kept confidential as described in section 2.7.1.

3.1.8 Authentication of organization identity Subscriber

The FBCA will issue certificates (i.e., cross-certificates) to Entity PCAs as directed by the FPKIPA. The FPKIPA will authenticate the organization identity as part of the application and MOU processes, as described in sections 3.1.2 and 3.1.11.

3.1.9 Authentication of Individual Identity Subscriber

The FPKI OA Administrators do not have FBCA-issued certificates for their activity. FPKI OA Security Officers are issued certificates for the sole purpose of administering the FBCA.

All data relating to authentication of Entity PCAs is recorded in accordance with section 4.5.1, and archived in accordance with section 4.6.

3.1.10 Authentication of Component Identity subscribers

The FBCA will not issue certificates to FBCA components. No stipulation.

3.1.11 Authentication of Entity PCAs

Entity PCAs are established by the Entity PCA applicant's Entity.

Following the completion of the MOU between the FPKIPA and the Entity PCA, the authorized official of the Entity PCA will designate (sponsor) the individual(s) responsible for completing interoperability with the FBCA (i.e., generating cross-certificate requests, establishing directory interoperability). The Entity PCA will provide the FPKI OA with a written document signed by an authorized official of the Entity PCA that provides identity information of the designated individual(s).

The designated Entity PCA responsible individual(s) will complete and sign a registration document and the FPKI OA will verify the information based on the requirements for the level of assurance of the certificate being issued to the Entity PCA.

FPKI OA records the process that was followed for issuance of each certificate. The process documentation and authentication requirements include the following depending upon the level of assurance (as set forth below):

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Entity PCA responsible individual as required by the level of assurance;
- A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the ID of the individual;
- The date and time of the verification;
- A declaration of identity signed by the applicant using a handwritten signature. If in-person identity proofing is done, this is performed in the presence of the person performing the identity authentication or a trusted agent (i.e., notary public).

For All Levels: The trusted person will present information sufficient for registration at the level of the certificate being requested. The table below summarizes the identification requirements for each level of assurance.

Table 3.1.11-1. FBCA Assurance Levels

Assurance Level	Identification Requirements
Test	The Test level of assurance is used by the FBCA prototype bridge and CAs when conducting interoperability testing. The production FBCA does not issue certificates with the Test level of assurance.
Rudimentary	No identification requirement; applicant may apply and receive a

Assurance Level	Identification Requirements
	certificate by providing his or her e-mail address
Basic	Identity may be established by in-person appearance before a Registration Authority or Trusted Agent; or comparison with trusted information in a data base, of user-supplied information (obtained and/or checked electronically, through other trusted means (such as the U.S. mail), or in-person); or by attestation of a supervisor, or administrative or information security officer, or a person certified by a state or Federal Entity as being authorized to confirm identities (such as notaries public) who uses a stamp, seal or other mechanism to authenticate their identity confirmation
Medium	Identity established by in-person appearance before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities (such as notaries public) who uses a stamp, seal or other mechanism to authenticate their identity confirmation; information provided shall be checked to ensure legitimacy Credentials required are either one Federal Government-issued Picture ID, or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)
High	Identity established by in-person appearance before the Registration Authority or Trusted Agent; information provided shall be checked to ensure legitimacy Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)

3.2 CROSS-CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

3.2.1 Cross-Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes its identity. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period. FBCA cross-certificates issued under this CPS to Entity PCAs will have three-year maximum validity period for authentication certificates.

New cross-certificates will need to be issued to Entity PCAs by the FBCA when the FBCA re-keys (every one-half of the FBCA self-signed certificate validity period), and

when Entity PCAs re-key. Upon Entity PCAs re-key, the FPKI OA will identify and authenticate the Entity PCAs either by:

(a) Performing the initial registration identification process defined in Section 3.1, or

(b) If it has been less than one-half of the certificate validity period since an Entity PCA was identified as required in Section 3.1, using the currently valid certificate issued to the Entity PCA by the FBCA.

Entity PCAs designated responsible individuals identify themselves for the purpose of re-keying as required in table below.

Table 3.2.1-1. Routine Rekey Requirements

Assurance Level	Routine Rekey Identity Requirements for Subscriber Signature and Encryption Certificates
Test	The Test level of assurance is used by the FBCA prototype bridge and CAs when conducting interoperability testing. The production FBCA does not issue certificates with the Test level of assurance.
Rudimentary	Identity may be established through use of current signature key
Basic	Identity may be established through use of current signature key, except that identity shall be reestablished through initial registration process at least once every 15 years from the time of initial registration
Medium	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration
High	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every three years from the time of initial registration

3.2.2 Cross-Certificate Renewal

No Stipulation. The FBCA does not renew cross-certificates.

3.2.3 Cross-Certificate Update

No stipulation. The FBCA does not update cross-certificates.

3.3 OBTAINING A NEW CROSS-CERTIFICATE AFTER REVOCATION

In the event of cross-certificate revocation, other than during a renewal or update action, issuance of a new cross-certificate always requires an initial registration process per Section 3.1 above. This applies to Entity CAs.

3.4 REVOCATION REQUEST

Revocation requests are authenticated and processed as described in section 4.4. The CAs will not allow issuance without verifying the digital signature (this is done by the CA software). Digital signatures are not currently supported, however, when technology avails itself the FBCA will verify digital signatures.

4. OPERATIONAL REQUIREMENTS

4.1 APPLICATION FOR A CROSS-CERTIFICATE

The procedures developed, approved and published (on the FBCA web site) by the FPKI PA for entities to use in applying for a certificate from the FBCA for one or more Entity PCAs are as follows:

1. The candidate Entity completes an application using a form supplied by the Federal PKIPA (available on its web site, http://www.cio.gov/fpkipa), which is signed by an authorized official of the Entity (as established on the form). The application contains how the Entity proposes to map the certificate levels of assurance present in the Entity PCA CP to the levels expressed in the FBCA CP, and how the Entity certificate profile conforms to the FBCA certificate profile (available at the web site cited above). The application also describes how the applicant Entity PKI has been independently audited to ensure conformance by the applicant to its own CP and CPS. The Entity application will include the Entity CP and CPS written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC2527].

2. The FPKIPA acts on the application and makes a determination as to whether to issue a certificate and enter into the MOA with the applicant Entity.

3. The FPKIPA instructs the FPKI OA to issue the certificate to the Entity PCA. Based on the Issuance letter provided by the Policy Authority, the OA team inserts policy OIDs and DN names. This information is provided in the Issuance letter.

4. The FPKIPA also instructs each established Entity PCA to provide the FPKI OA with a memo (on the Entity PCA site letterhead) designating a primary and alternate POC. The Entity PCA authorized official signs this memo. The memo contains the Entity PCA Distinguished Name (DN). The memo also contains the name of the electronic file, which contains the certificate request (PKCS #10 format message). The three items: letter, floppy diskette, and backup floppy

diskette are put in a sealed envelope and securely delivered to the FPKI OA (i.e., in-person, registered mail, courier).

5. Upon issuance, each certificate issued by the FBCA is manually checked to ensure each field and extension is properly populated with the correct information, before the certificate is delivered to the Entity PCA and before it is posted in the repository.

4.1.1 Delivery of Entity PCA public key(s) for FBCA cross-certificate issuance

Entity PCA public keys are delivered to the FBCA electronically in a digitally signed certificate request (i.e., using PKCS #10) message to the FPKI OA via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier). Identity checking and proof of possession of the private key is accomplished as described in this CPS in section 3.1.11 and 4.2 respectively.

4.2 CERTIFICATE ISSUANCE

The FPKI OA issues cross-certificates to the Entity PCA by the following procedure:

1. Upon receiving a signed request message (PKCS#10 message) from the Entity PCA, the designated CA software verifies the signature to prove possession of the private key. Then the FBCA will sign and issue a cross-certificate to the Entity PCA.

2. The certificate issued by the FBCA will be delivered to the Entity PCA in a signed response message (PCKS#10), via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier).

3. Each certificate issued by the FBCA is manually checked to ensure each field and extension is properly populated with the correct information, before the certificate is delivered to the Entity PCA.

4. The FBCA will generate a digitally signed certificate request message and deliver it to the Entity PCA in a PKCS#10 certificate request message, via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier).

5. The Entity PCA will sign and issue a certificate to the FBCA and deliver it to the FBCA in a signed response message (PCKS#10), via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier).

6. The FPKI OA will post both certificates (cross-certificates) in the FBCA repository individually or as a single cross-certificate pair.

4.2.1 Delivery of Subscriber's private key to Subscriber

The FBCA does not generate subscriber private keys. For FPKI OA staff, hardware tokens containing FBCA private signature keys are backed up using the LunaSA procedures described in SO04. Entity private signature keys are not maintained by the FPKIA.

4.2.2 FBCA public key delivery and use

The FBCA public keys are delivered to the Entity PCA(s) as described in section 4.2 above.

4.3 CROSS-CERTIFICATE ACCEPTANCE

The MOA sets forth responsibilities of respective Entities and the FPKIPA before the FPKIPA authorizes issuance of an FBCA cross-certificate to the Entity PCA. Once a cross-certificate has been issued, its acceptance by the Entity PCA commences interoperability with the FBCA via completion of directory chaining between the Entity PCA directory and the FBCA directory. This triggers its obligations under the MOA and this CPS.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Circumstances for revocation of a cross-certificate issued by the FBCA

There are three circumstances where certificates issued by the FBCA can be revoked:

1. When the Federal Policy authority requests that an FBCA-issued certificate be revoked. This will be the normal mechanism for revocation in cases where the FBCA PA determines that an Entity PKI does not meet the FPKI policy requirements or certification of the Entity PKI is no longer in the best interest of the federal government.

2. When the FPKI Operational Authority receives an authenticated request from a previously designated official of the Entity responsible for the Principal CA (such official or official shall be identified in the MOA as authorized to make such a request.

3. When the FPKI Operational Authority personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the FBCA. Under such circumstances, the following individuals may authorize immediate certificate revocation:

    a. Chair of the FPKI Policy Authority

b. Chair of the Federal Identity Credentialing Committee

c. Director of the FPKI Operational Authority

d. As designated by the FPKI Policy Authority

The FPKI PA shall meet as soon as practical to review the emergency revocation.

Whenever any of the above circumstances occur, the associated certificates shall be revoked and placed on the CRL. Revoked certificates are included on all new publications of the certificate status information until the expiration date of the cross-certificate.

The FPKI OA posts the CRL and/or CARL to the FBCA repository (see section 2.6.4) within 6 hours of notification. Certificates are removed from the CRL and/or CARL after the expiration date of the cross-certificate; however, the revoked certificate must appear on at least one published CRL and/or CARL.

4.4.1.1 Who can request revocation of a cross-certificate issued by the FBCA or Entity CA

An FBCA cross-certificate to an Entity PCA is revoked (1) upon direction of the FPKIPA, (2) upon an authenticated request by a previously designated authorized official of the Entity PCA (such official or officials are established in the MOA as authorized to make such a request), or (3) when the FPKI Operational Authority personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the FBCA (see section 4.4.1).

4.4.1.2 Procedure for revocation request

The FPKI OA 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 of the Entity PCA, or the FPKI PA, drafts an authenticated request to revoke a certificate. The individual then notifies the request to the FPKI OA Administrative/Help desk via phone as well as submits the request via signed e-mail to the FPKI OA identifying the certificate to be revoked, explaining the reason for revocation.

2. Upon receipt of a signed revocation request, the FPKI OA authenticates the request by verifying the digital signature and/or making direct contact (call back or challenge/response telephone conversation) with the Entity PCA POC (or the FPKI PA).

3. In the event the request to revoke originates from the Entity PCA, the FPKI OA apprises the FPKIPA of the request for revocation.

4. The FPKIPA evaluates and verifies the need for revocation expressed in the authenticated request. If the revocation request appears to be valid, the FPKIPA will direct the FPKI OA to proceed with revocation.

5. The FPKI OA will revoke the certificate, which automatically generates and adds a CRL entry for that certificate within 6 hours of notification of approval by the FPKIPA.

6. The FPKI OA ensures the new CARL/CRL is posted in the FPKIA repository within 6 hours of notification of approval by the FPKIPA.

7. The Entity PCA also revokes the certificate issued to the FBCA and generates and posts a new CARL/CRL.

The FPKI OA may affect revocation of a certificate prior to notification and approval of the FPKIPA as set forth in emergency revocation procedures consisting of the following steps:

1. Notify all identified POCs in the emergency list of FBCA (i.e., FPKI OA POC, Entity PCA POCs, CP/CPS WG POC). This can be done by either:

   a. Telephone (using one of call-back or challenge/response protocols)

   b. Signed FAX

   c. Signed e-mail

2. Revoke the cross-certificate and post the new CRL/CARL

3. Once the incident has been investigated and documented, issue a new cross-certificate to replace the one that has been revoked, as directed by the FPKIPA.

4.4.1.3 Revocation of a Cross-Certificate Issued by the FBCA

Revocation of an FBCA cross-certificate is accomplished by the generation and publication into the FPKIA repository of status information citing the cross-certificate as revoked and the reason for the revocation, within 6 hours of notification of approval by the FPKIPA or in accordance with emergency procedures provided in section 4.4.1.2.

Further, and separate from the publication of the status information, prompt oral and/or electronic notification is given by the FPKI OA to all Entity PCA POCs..

4.4.1.4 Revocation of a Cross-Certificate Issued by the Entity PCA

Revocation takes effect upon the publication of status information (including the reason for the revocation, which may include loss, compromise) for the cross-certificate issued to the FBCA. Information about a revoked cross-certificate remains in the status information (CRL) until the cross-certificate expires.

4.4.1.5 Revocation Request Grace Period

There is no revocation grace period for the FBCA.

4.4.2 Suspension

Suspension will not be used by the FBCA.

4.4.3 Certification Authority Revocation Lists (CARLs) / Certificate Revocation Lists (CRLs)

The FPKI OA issues Certification Authority Revocation Lists (CARLs) and Certificate Revocation Lists (CRLs) in accordance with the CARL/CRL profile provided in the FBCA Interoperability Guidelines. The contents of CARLs and CRLs are checked to ensure that all information is correct by using mechanisms provided by the CA software or third-party software.

4.4.3.1 CARL/CRL Issuance Frequency

CARLs and CRLs are issued daily, even if there are no changes to be made, to ensure timeliness of information. Certificate status information is posted within 6 hours of notification of approval of revocation or immediately in accordance with emergency revocation procedures provided in section 4.4.1.2. The current CARL/CRL will be removed and replaced with the updated CARL/CRL.

4.4.3.2 CARL/CRL Checking Requirements

The FPKIA repository currently supports CRL/CARL access via X.500 chaining to provide certificate status information (i.e., X.500 DSP). The FPKIA directory system also supports Lightweight Directory Access Protocol (LDAP) CRL/CARL and certificate checking.

4.4.4 On-line Revocation / Status checking availability

The FBCA does not plan to support the Online Certificate Status checking Protocol (OCSP) capability for its cross-certificates.

4.4.5 Other forms of revocation advertisements available

The FBCA does not support any other forms of revocation advertisements.

4.4.6 Checking requirements for other forms of revocation advertisements

The FBCA does not support any other forms of revocation advertisements.

4.4.7 Special requirements related to key compromise

In the event of an Entity PCA private key compromise or loss, a CARL/CRL is published by the FPKI OA within 6 hours of notification of approval by the FPKI PA or within 24 hours, in accordance with procedures described in section 4.4.1.2

4.5 SECURITY AUDIT PROCEDURE

The FPKI OA generates audit log files for all events relating to the security of the FBCA. 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. The security audit logs for each auditable event defined in this section are maintained in accordance with *Retention period for archive*, Section 4.6.2.

4.5.1 Types of Events Recorded

Security auditing capabilities of the FBCA repository, the FBCA operating system, and CA applications have been enabled for logging the types of events specified in the table below. The table indicates whether the auditable event is logged automatically by the application/operating system, or it is logged manually in a logbook as prescribed by applicable procedures. 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 FBCA signing process
- A success or failure indicator when performing certificate revocation
- The identity of the entity and/or operator (of the FBCA) that caused the event.
- A message from any source requesting an action by the FBCA is an auditable event. The message must include message date and time, source, destination and contents.

The FPKI OA staff has verified (i.e., obtained vendor statements and conducted direct testing) that the equipment and application software purchased indeed supports capturing audit logs for the events specified in the table below.

Table 4.5.1-1. Auditable Events

Auditable Event	FPKIA Directories	FBCA

	Manual / Procedural	Automatic	Manual / Procedural	Automatic
SECURITY AUDIT				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	✓		✓	
Any attempt to delete or modify the Audit logs	✓ After a deletion following any archive operation	✓ After a modification following any archive operation		✓
IDENTIFICATION AND AUTHENTICATION				
Successful and unsuccessful attempts to assume a role		✓		✓
Change in the value of maximum authentication attempts	✓		✓	
Maximum number of unsuccessful authentication attempts during user login		✓		✓
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	The account is immediately re-activated	The account is immediately re-activated	The account is immediately re-activated	The account is immediately re-activated
An Administrator changes the type of authenticator, e.g., from password to biometrics	✓		✓	
KEY GENERATION				
Whenever the FBCA generates a key. (Not mandatory for single session or one-time use symmetric keys)	Applies to CA only	Applies to CA only	✓	✓
PRIVATE KEY LOAD AND STORAGE				
The loading of Component private keys	Applies to CA only	Applies to CA only	✓	✓
All access to certificate subject private keys retained within the FBCA for key recovery purposes	Applies to CA only	Applies to CA only	✓	✓
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	✓	✓
PRIVATE KEY EXPORT				
The export of private-keys (keys used for a single session or message are excluded)	Applies to CA only	Applies to CA only	✓	✓
CERTIFICATE REGISTRATION				
All certificate requests	Applies to CA only	Applies to CA only	✓	✓

Auditable Event	FPKIA Directories		FBCA	
	Manual / Procedural	Automatic	Manual / Procedural	Automatic
CERTIFICATE REVOCATION				
All certificate revocation requests	Applies to CA only	Applies to CA only	✓	✓
CERTIFICATE STATUS CHANGE APPROVAL				
The approval or rejection of a certificate status change request	Applies to CA only	Applies to CA only	✓	
FBCA CONFIGURATION				
Any security-relevant changes to the configuration of the FBCA	Applies to CA only	Applies to CA only	✓	✓
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	✓		✓	✓
The access control privileges of a user account or a role are modified	✓		✓	✓
CERTIFICATE PROFILE MANAGEMENT				
All changes to the certificate profile	Cert Profile not captured in Directory	Cert Profile not captured in Directory	✓	
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile	Revocation Profile not captured in Directory	Revocation Profile not captured in Directory	✓	
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	✓	
MISCELLANEOUS				
Installation of the Operating System	✓		✓	
Installation of the FBCA	Applies to CA only	Applies to CA only	✓	✓
Installing hardware cryptographic modules	Applies to CA only	Applies to CA only	✓	✓
Removing hardware cryptographic modules	Applies to CA	Applies to CA	✓	

Auditable Event	FPKIA Directories		FBCA	
	Manual / Procedural	Automatic	Manual / Procedural	Automatic
	only	only		
Destruction of cryptographic modules	Applies to CA only	Applies to CA only	✓	
System Startup	✓		✓	
Logon Attempts to FBCA Apps	Applies to CA only	Applies to CA only		✓
Receipt of Hardware / Software	✓		✓	
Attempts to set passwords	✓			✓
Attempts to modify passwords	✓			✓
Backing up FBCA internal database	Applies to CA only	Applies to CA only		✓
Restoring FBCA internal database	Applies to CA only	Applies to CA only		✓
File manipulation (e.g., creation, renaming, moving)		✓		✓
Posting of any material to a repository		✓		✓
Access to FBCA internal database	Applies to CA only	Applies to CA only	✓	✓
All certificate compromise notification requests	Applies to CA only	Applies to CA only	✓	
Loading tokens with certificates	Applies to CA only	Applies to CA only	✓	
Shipment of Tokens	Applies to CA only	Applies to CA only	✓	
Zeroizing tokens	Applies to CA only	Applies to CA only	✓	
Rekey of the FBCA	Applies to CA only	Applies to C	✓	
Configuration changes to the CA server involving:	Applies to CA only	Applies to CA only	✓	
Hardware	Applies to CA only	Applies to CA only	✓	
Software	Applies to CA only	Applies to CA only	✓	
Operating System	Applies to CA	Applies to CA	✓	✓

Auditable Event	FPKIA Directories		FBCA	
	Manual / Procedural	Automatic	Manual / Procedural	Automatic
	only	only		
Patches	Applies to CA only	Applies to CA only	✓	✓
Security Profiles	Applies to CA only	Applies to CA only	✓	✓
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to room housing FBCA	✓	✓	✓	✓
Access to the FBCA server	Applies to CA only	Applies to CA only	✓	✓
Known or suspected violations of physical security	✓	✓	✓	✓
ANOMALIES				
Software Error conditions	✓	✓	✓	✓
Software check integrity failures	✓	✓	✓	✓
Receipt of improper messages	✓	✓	CA is stand alone	CA is stand alone
Misrouted messages	✓	✓	CA is stand alone	CA is stand alone
Network attacks (suspected or confirmed)	✓	✓	CA is stand alone	CA is stand alone
Equipment failure	✓	✓	✓	✓
Electrical power outages	✓	✓	✓	✓
Uninterruptible Power Supply (UPS) failure	✓	✓	✓	✓
Obvious and significant network service or access failures	✓	✓	CA is stand alone	CA is stand alone
Violations of Certificate Policy	✓	Certain Violations as documented by this table	✓	Certain Violations as documented by this table
Violations of Certification Practice Statement	✓	Certain Violations as documented by this table	✓	Certain Violations as documented by this table
Resetting Operating System clock	✓		✓	

4.5.2 Frequency of processing data

The FPKI OA Auditor reviews audit logs at least once per month as defined in section 5.2. The FPKI OA Auditor will examine 100% of security audit data generated by the FBCA since the last review. All security alerts and irregularities are explained in an audit log summary. The FPKI OA Auditor reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

4.5.3 Retention period for security audit data

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 for three months but their electronic versions are permanently retained on the primary site server and hence these logs are always available. The FPKI OA Administrator removes audit logs from the FBCA and gives them to the FPKI OA Auditor neither of whom commands the FBCA signature key(s).

4.5.4 Protection of security audit data

The FPKI OA Auditor performs routine review of security audit logs. The procedure for protecting security audit data is 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 FPKI OA Administrator, Security Officer, Auditor, Operator, and others possibly designated by the FPKIPA.

3. Only the FPKI OA Auditor is authorized to archive audit logs.

4. Audit logs are deleted only under procedural multi-person control.

5. Audit logs are protected under multi-person control and cannot be modified without detection.

Daily audit logs are generated on time stamped digital media and are protected from deletion and/or modification prior to the end of the audit log retention period. System logs are automatically time stamped and systems use the Network Time Protocol (NTP) to maintain and synchronize their time with the NIST time server. See sections 4.5.5, 4.5.6, 4.6, and 5.0 for descriptions of physical and procedural controls for protection of the data.

4.5.5 Security Audit data backup procedures

FPKIA Directory:

Audit logs and audit summaries are incrementally backed up daily via time stamped digital media. Full backups are performed daily via digital tape media. Weekly, the backups are moved to and stored in secure container in a separate building (interim storage) from the FPKIA facility. Additionally, backups are performed at the hot site location to ensure continuity; shadowing the primary directory and performing weekly backups accomplish this.

FBCA:

Full backups are performed daily via digital tape media. Weekly backups are moved to and stored in secure container in a separate building (interim storage) from the FPKIA facility.

Manual audit logs will be collected weekly and stored in a secure container in a separate building (interim storage) from the FPKIA facility. These audit logs are moved to the hot site archive location quarterly.

4.5.6 Security Audit collection system (internal vs. external)

The audit log collection system is internal to the FBCA components (see section 4.5.1). 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 FPKI OA will determine whether to suspend FBCA operation until the problem is remedied. Section 4.5.1 describes the collection procedures (manual or automatic) for the auditable events. Section 4.5.5 describes the protection procedures for backing up audited data that has been collected.

4.5.7 Notification to event-causing subject

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

4.5.8 Vulnerability Assessments

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

Vulnerability assessments will be conducted as part of security compliance audits as specified by the FPKIPA.

The FPKI OA provides a report of the analysis of the results of vulnerability assessments, specifically indicating security vulnerabilities identified and correction procedures of those vulnerabilities.

4.6 RECORDS ARCHIVAL

4.6.1 Types of events archived

The FPKI OA Auditor produces archive records on a weekly basis. The records are stored on paper and all electronic data to include certificates and CRLs are stored on the offline directory. The electronic records accumulated on the offline directory are backed up daily. Additionally, no electronic records are deleted. The archive records include data received from the certificates and CRLs it generated, certificate requests and certificate revocation requests it received.

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

- FBCA certification and accreditation
- Certification Practice Statement
- Contractual obligations
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- Revocation requests
- Subscriber identity Authentication data as per Section 3.1.9
- Documentation of receipt and acceptance of certificates
- Documentation of receipt of tokens
- All certificates issued or published
- Record of Re-key
- All CARLs and CRLs issued and/or published
- All Audit Logs
- Other data or applications to verify archive contents
- Documentation required by compliance auditors

See Section 4.5 for a description of the audit and archive collection procedures.

4.6.2 Retention period for archive

Weekly, the backups from the primary site are moved to and stored in secure container in the interim storage facility. Quarterly, the weekly backups from the interim storage are moved to and stored in secure container at the hot site storage facility. Records are periodically moved from the hot site for the long term archival at the National Archives and Records Administration (NARA). The backups will be archived at NARA for a period of at least twenty years, six months.

The items that are required to be archived are all archived in paper format, which can be retained for the required period. Other items, such as signed certificates and CRLs, are backed up and stored on the servers themselves. This will ensure that there is always a copy available.

The interim site is located at:

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

The hot site is located at:

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

Only paper records are archived at NARA for long term storage and no special application is required to read these records.

4.6.3 Protection of archive

Long-term protection of the archive is provided as described in the FPKIA SOP SA13.

Archive data is clearly labeled as follows:

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

The archive media is stored in a safe at the interim and the hot site facilities, which are temperature controlled and behind locked doors, as described in section 5.1.

The FBCA Auditor maintains a list of individuals who can access and delete the archive files at the interim site and hot 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 FPKIPA or as required by law. The procedure for releasing information is described in SA06.

4.6.4 Archive backup procedures

Archive records are backed-up as part of the nightly normal system backup procedure to single session, 4mm digital tapes.

Full system backups are performed to daily to digital tape removable storage media.

4.6.5 Requirements for time-stamping of records

Records will be clearly labeled with date/time period information of the data contained in the record as described in section 4.6.3. System logs are automatically time stamped and systems use the NIST time server to maintain synchronize time via Network Time Protocol (NTP).

4.6.6 Archive collection system

The archive information will be collected by the FPKI OA Auditor, who will be responsible for archival.

4.6.7 Procedures to obtain and verify archive information

Creation of archive data is described in section 4.6.1. The archive data is placed in clearly labeled, double wrapped packaging for transport to short-term and long-term archive locations. Transport of archive data is via hand carry for short-term archive by the FPKIA Auditor or approved courier services. Storage and protection of archive data is described in section 5.

The FPKI OA auditing official will maintain logging information (and receipts) as archived data is transported to short-term and long-term archive facilities.

4.7 KEY CHANGEOVER

The FBCA key changeover procedures are as follows:

- The FBCA will generate a self-issued certificate signed by the old private key whose *subjectPublicKeyInfo* field contains the new public key.
- The FBCA will generate a self-issued certificate signed by the new private key whose *subjectPublicKeyInfo* field contains the old public key.
- The FBCA will generate a self-issued certificate signed by the new private key whose *subjectPublicKeyInfo* field contains the new public key.
- The FBCA and all Entity PCAs will process new cross-certificates as described in this CPS.
- All certificates generated as part of the key changeover process will be posted to the FPKIA repository.

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

The FBCA will support Entity PCA key changeovers by issuing and posting new certificates as required.

4.8 COMPROMISE AND DISASTER RECOVERY

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

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 FPKI OA 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 FPKI OA Management team

5. If the severity/scenario (to exceed 6 hours) of the event is critical, activation of the alternate site (hot site).

6. The FBCA POCs ("hot list") will be notified of this change, so that any changes required by the Entity PCAs can be performed

7. Manage the recovery process of the primary FPKIA facility.

8. Submit post recovery logs to FPKIPA

The FPKIPA will be notified as soon as possible as described in DR01 and DR02.

In the event the FBCA equipment is damaged or rendered inoperative, but the FBCA signature keys are not destroyed, FBCA operation will be reestablished as quickly as possible, giving priority to the ability to generate certificate status information." to the end of section 4.8.1

In order to provide 6-hour window for FBCA service re-activation, the FPKI OA has implemented a synchronized hot site. The hot site will include an identical configuration of the primary site. The FPKIA hot site directory is updated by a running script that pulls the information from the primary site on a regular basis. The hot site FBCA is quickly restored via backup tapes.

During system restoration the FBCA will need to ensure CARLs/CRLs are current with their respective Entity PCAs. Additionally, cross-certificates need to be validated and new public keys/cross-certificates issued in the event anomalies exist.

The following reports are generated:

1. Activity log – this log is maintained throughout the disaster recovery process.

2. Test plan results

3. Equipment list – Update configuration management

4. Restoration Expense report

4.8.2 FBCA signature keys are revoked

Within 6 hours, the FPKI OA will securely advise (via callback and challenge-response) the FPKIPA and all of the FBCA POC "hot list" in the event of a disaster where the FBCA installation is physically damaged and all copies of the FBCA signature keys are destroyed.

The FBCA AO will securely (via callback and challenge-response) notify via telephone the FBCA POC "hot list," if the FBCA cannot issue a CARL/CRL within 6 hours (as

described in Disaster Recovery DR01-03 and Help Desk Trouble Handling Procedures HD02).

The FPKIPA will determine whether to revoke the FBCA certificate issued to the Entity PCAs.

The FPKI OA will reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in section 4.8.1.

4.8.3 FBCA signature keys are compromised

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

1. The FPKIPA and all of its member entities (the POCs list is retrieved from the secure storage container) will be securely notified (so that entities may issue CARLs revoking any cross-certificates issued to the FBCA) via telephone (via callback and challenge-response) to the designated POCs;

2. The PCAs that have issued certificates to the FBCA will publish a CARL revoking the cross-certificate issued to the FBCA as set forth above;

3. The FBCA will generate a new FBCA key pair in accordance with procedures set forth in section 4.2

4. New FBCA certificates will be issued to Entity PCAs also in accordance with section 4.2.

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

4.8.4 Secure Facility impaired after a Natural or Other type of Disaster

The FBCA servers will operate with back-up power and telecommunications and appropriate infrastructure system redundancies, and, therefore, no outages longer than 24-hours are anticipated. However, if an outage is anticipated to become, or becomes, an extended outage, the disaster recovery plan will come into effect. An extended outage is defined as one in which the ability of FBCA to revoke certificates cannot be re-established within 24 hours. The details of this plan are defined in the FBCA BCCP and Disaster Recovery Procedures.

In the case of a disaster whereby the FBCA primary installation is physically damaged and all copies of the FBCA signature key are destroyed as a result, the FPKIPA and all of its member entities will be securely notified (via callback and challenge-response, using form 04-034), and the procedures described in section 4.8.1 will be followed. The FBCA installation will then be completely rebuilt, by reestablishing the FBCA equipment, generating new private and public keys, being re-certified, and re-issuing all cross-certificates.

4.9 CA TERMINATION

In the event of termination of the FBCA operation, certificates signed by the FBCA will be revoked. The FPKI OA will advise, using secure communication (callback and challenge-response described in SA09) all cross-certified CAs, to which the FBCA has issued cross-certificates, of its termination. All documentation and data will be archived using the Long Term Storage procedures (SA13).

The FPKI OA Team will coordinate scheduled termination with cross-certified CAs when authorized by the 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 FBCA is terminated.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS FOR THE FBCA

The FBCA imposes physical security requirements that provide similar levels of protection as those specified below. All the physical control requirements apply to the FBCA.

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.1 Site location and construction

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.2 Physical access

Text Removed. This information is 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" (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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.3 Electrical Power

Text removed. This information is 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" (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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.4 Water exposures

The FPKIA room implements water protection safeguards equivalent to those implemented for the GSA FTS computer room.

5.1.5 Fire prevention and protection

The FPKIA room implements fire prevention and protection safeguards equivalent to those implemented for the GSA FTS computer room.

5.1.6 Media storage

The FPKIA room also includes a small safe, fireproof locked cabinets, and a desk where media is stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information is stored at a different location separate from the FPKIA (i.e. in an off-site interim Storage Facility) and after three months it is transported to long-term site specified in section 4.6.2.

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.

5.1.8 Off-site backup

For the FBCA full system backups, sufficient to recover from total system failure, are conducted on a periodic schedule, described in sections 4.5 and 4.6,4. The short-term backup site specified in section 4.6.3 and contains up to three months worth of backup information. The long-term backup site is specified in section 4.6.2.

5.2 PROCEDURAL CONTROLS FOR THE FBCA

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles are responsible or the integrity of the CA. The functions performed in these roles form the basis of trust for all uses of the FBCA. 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 FPKIA encompasses CA products from several vendors. Different commercial products support somewhat different roles, and use different mechanisms for registering or enrolling subscribers and issuing certificates:

1. *Administrator* – authorized to install, configure, and maintain the Operating Systems and Directory Software; establish and maintain Operating System user accounts; configure Operating System profiles and audit parameters; and generate component keys.
2. *Security Officer* – authorized to request or approve certificates or certificate revocations; authorized to install, configure and 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.
3. *Auditor* – authorized to view and maintain audit logs.
4. *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, and;
- Assisting in Generating and Backing up CA keys.

Administrators do not issue certificates to subscribers.

5.2.1.2 Security Officer

The Security Officer role is responsible for issuing certificates, including:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates;
- Requesting, approving and executing the revocation of certificates.
- Configuring certificate profiles or templates and audit parameters for the CA software.
- Generating and backing up CA keys.

5.2.1.3 Auditor

The auditor role is responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the FBCA is operating in accordance with this CPS;

5.2.1.4 Operator

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

5.2.2 Separation of Roles

Role separation, when required as set forth below, is enforced either by the FBCA equipment, or procedurally, or by both means.

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

- Individual FPKI OA personnel are specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Security Officer, Administrator, and Auditor roles. No user identity can:

  Assume both the Administrator and Security Officer roles

  Assume the Auditor and any other roles.

- The Operator role may be assumed by the Administrator, and/or Security Officer.

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.2.3 Number of persons required per task

To best ensure the integrity of the FBCA 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 FBCA operation.

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

5.2.4 Identification and authentication for each role

Individuals identify and authenticate himself/herself before being permitted to perform any actions set forth above for that role or identity.

5.3 PERSONNEL CONTROLS

5.3.1 Background, qualifications, experience, and security clearance requirements

The FPKIPA and the FPKI OA are responsible and accountable for the operation of the FBCA

All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and are U.S. citizens. The procedures governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the FBCA are set described in the FPKIA SSP. Appendix A of this CPS includes selected excerpts from that portion of the FPKIA SSP.

All FPKIA personnel hold TOP SECRET security clearances.

5.3.2 Background check procedures

FPKI OA personnel in trusted roles hold Top Secret clearances.

5.3.3 Training Requirements

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

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

Training in the overall security procedures of the FPKIA is conducted for all personnel at the initial full operation capability of the FBCA. 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.

5.3.4 Retraining frequency and requirements

Individuals responsible for trusted roles are made aware of changes in the FBCA operation as described personnel training procedures documentation. Any significant change to the operations are documented and personnel are informed and made aware of changes in accordance with the personnel training procedures. All FPKI OA personnel will participate in mandatory refresher training annually to ensure all affected personnel are aware of new changes to procedures and configuration changes. In addition, immediate On-the-Job-Training (OJT) is conducted when any changes occur within the FBCA operations. Examples of such changes are FBCA software or hardware upgrades, changes in automated security systems, and relocation of equipment.

5.3.5 Job rotation frequency and sequence

The FBCA CP does not stipulate requirements for this section.

5.3.6 Sanctions for unauthorized actions

The FPKIPA takes appropriate administrative and disciplinary actions against personnel who have performed unauthorized actions involving the FBCA or its repository. In the event of an unauthorized action, the ISSO will immediately investigate the incident. After the investigation, the ISSO and ISSM will determine if the action warrants

disciplinary actions based on severity and the reoccurrence of the indiscretion. If the action is of significant indiscretion, it will be reported to the FPKI Program Manager 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 as to prevent further indiscretions.

5.3.7 Contracting personnel requirements

Contractor personnel employed to perform functions pertaining to the FBCA meet applicable requirements set forth in the FBCA CP and this CPS as determined by the FPKI OA.

5.3.8 Documentation supplied to personnel

The FBCA makes available to all of its personnel the FBCA CP, CPS, and any relevant statutes, policies or contracts. Documentation identifying all personnel receiving and completing training is maintained by the FPKI OA.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 FBCA and CA key pair generation

The key pair for the FBCA is generated on the Chrysalis LunaSA cryptographic module. The key pair generation is RSA for digital signature in compliance with PKCS-1 (FIPS 140-2, level 3). The private key will never be exposed outside the module in unencrypted form. Backup copies of the LunaSA private keys will be created.

FBCA private keys are generated using the FBCA key signing Ceremony procedures. These procedures document the role separation and provide an auditable trail. These procedures are completed with a third party auditor present, where each step is verified and the document is signed off on at the end of the procedure.

6.1.2 Private Key Delivery to Subscriber

The Entity PCA generates its own key pair and therefore does not need private key delivery.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered to the certificate issuer electronically in a certificate request (i.e., using PKCS #10) messages to the FPKI OA via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier) as described in section 4.2. Identity checking and proof of possession of the private key will be accomplished as described in section 4.1.

6.1.4 FBCA cross-certificates and public key availability and delivery to Entity PCAs

The FBCA will post all cross-certificates it issues in the FPKIA repository. The FBCA will also post all cross-certificates issued by the Entity PCAs to the FPKIA. The FBCA and Entity PCA public keys will be transported in a secure, out-of-band mechanism, using PKCS#10 messages via e-mail or floppy disk delivered by registered mail or courier.

6.1.5 Key sizes

Public key sizes are 1024 bits for RSA, SHA-1, in accordance with FIPS 186. SSL or similar protocol is not used.

6.1.6 Public key parameters generation

There are no public key parameters for RSA.

6.1.7 Parameter quality checking

There are no public key parameters for RSA.

6.1.8 Hardware/Software key generation

The FBCA key pairs are generated in a FIPS 140-2 Level 3 validated, LunaSA hardware cryptographic module.

Key pairs for trusted roles and provision of multi-person controls are generated in a FIPS 140-1 Level 2 validated DataKey SmartCard cryptographic module.

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

Keys are certified for use in a combination of digital signature and non-repudiation. Two key usage bits: *cRLSign* and *CertSign*, are set in FBCA certificates.

The use of a specific key is determined by the key usage extension in the X.509 certificate. Section 7 contains further details on key usage.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for cryptographic module

The CA private keys are protected using FIPS 140-2 Level 3 validated cryptographic module: Chrysalis LunaSA hardware token.

Key pairs for FBCA separation of roles are generated in FIPS 140-1 Level 2 validated cryptographic modules (DataKey SmartCards).

All cryptographic modules are operated such that the private asymmetric cryptographic keys are never output in plaintext.

See section 5.2.2 for a description of the procedures used for accessing and operating the FBCA.

6.2.2 FBCA private key multi-person control

All FBCA private keys are under 2 out of N control, where N≥2. N is the total number of Security Officers in the FPKI OA. See Section 6.2.7 for details on how this is achieved.

6.2.3 Key Escrow of FBCA private signature key

The FBCA signature keys used to support non-repudiation services are not escrowed by a third-party.

6.2.3.1 Escrow of Entity CA encryption keys

The FBCA does not perform any encryption key recovery functions.

6.2.4 Private Key Backup

6.2.4.1 Backup of FBCA and Entity CA private signature key

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.2.4.2 Backup of subscriber private signature key

Subscriber private keys are maintained by the subscriber.

6.2.5 Private Key Archival

No FBCA private keys will be archived or escrowed. (See section 6.2.3)

6.2.6 Private key entry into cryptographic module

FBCA private keys are generated by and remain in a cryptographic module. The Chrysalis product uses proprietary secure means for transferring keys from one cryptographic module to another to back up the CA keys.

6.2.7 Method of activating private keys

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.2.8 Methods of deactivating private keys

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.2.9 Method of destroying private signature keys

The triple-DES encrypted key blobs on the hard drive are destroyed and the administrator tokens reinitialized, under the same multi-person control procedures used to initially generate the key pairs described above. Note that if the tokens are not reinitialized, they could be used to restore the key with any backup copy of the key blobs.

6.3 GOOD PRACTICES REGARDING KEY-PAIR MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Usage Periods for the Public and Private Keys

The FBCA private signing keys will be used to sign certificates for one-half of the certificate lifetime (e.g. for 2 years if the certificate lifetime is 4 years). The certificate lifetime will be valid not more than 6 years. Entrust CA issues certificates with a validity period of 10 years. Rekeying will be performed at 3 years.

6.4 ACTIVATION DATA

6.4.1 Activation data generation and installation

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.4.2 Activation data protection

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

Activation data is never shared.

Entrust CA 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 to decrease the likelihood of discovery. The cryptographic module activation data will be changed not less than once every three months

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific computer security technical requirements

The FBCA server is operated on a dedicated workstation connected to the FPKIA CA network and does not run any network services. The internal FPKIA directory/repository connects through a one-way firewall to the online repository system in order to post validation information.

The online FPKIA repository is operated on a dedicated workstation and will only run the network services required to operate the repository and to support on-line certificate validations by Entity CA subscribers (i.e., LDAP, DNS).

The FBCA server is in a configuration that has been clearly demonstrated and passed the Compliance Audit process as described in section 1.7 of the FPKIA System Security Plan (SSP).

The FBCA equipment is configured with appropriate security features turned on as recommended by the host operating system vendor in accordance with any associated security validation rating. The FBCA has the following security features and functions:

- Require authenticated logins via FIPS PUB 140-2, Level 3 and 140-1, Level 2 cryptographic modules
- 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 FBCA 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 FBCA random access memory. It is assumed that verification of meeting this requirement is provided by the Windows 2000 operating system. Windows 2000 enforces the required prohibition/separation. Windows 2000 was evaluated under IT SEC E3/FC2, since the FC2 functional package is equivalent to the Orange Book's C2, it includes the required memory protection controls. More information on the Windows 2000 evaluation is available at: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dngenlib/html/msdn_ntvmm.asp.
- Require use of cryptography for session communication and database security. The use of cryptography for session communication is not required because the certificate

request messages (PKCS#10) are exchanged using an out-of-band mechanism and are imported manually directly at the CA. The CA database is protected via triple-DES cryptography.

- Archive FBCA history and audit data through data collection and archive procedures described in sections 4.5 and 4.6

- Require self-test security related FBCA 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.

- Require a trusted path for identification of PKI roles and associated identities logins via FIPS PUB 140-2, Level 3 and 140-1, Level 2 cryptographic modules. Requires a recovery mechanisms for keys and the FBCA system through backup and protection procedures described in 4.5.5

- Enforce domain integrity boundaries for security critical processes through self-test procedures described above

6.5.2 Computer Security Rating

The FBCA CP does not stipulate requirements for this section. No stipulation.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System development controls

The System Development Controls for the FBCA are as follows:

- The FBCA software is commercial- off-the-shelf software that has been developed under a very formal development process that is well documented.

- Hardware procured to operate the FBCA has been purchased in a fashion whereby the provider does not know that it is intended for the FBCA operations. The CA software has been ordered and installed by certified engineers under the direction and control of authorized FPKIA 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 FBCA server will be purchased using commercial buys. Hardware and non-CA software is purchased randomly, through standard procurement procedures provided by the FPKI OA. No custom software has been purchased. An accountable method of packaging and delivery will be used to provide a continuous chain of accountability from the vendor to the facility (e.g., UPS, Federal Express, USPS Express Mail). The FBCA establishes a relationship with the CA software vendors prior to acquisition that gives assurance

that the software has not been tampered with. Installation is performed under multi-person control with only authorized FBCA operation personnel.

- Proper care is taken to prevent malicious software from being loaded onto the FBCA equipment. From the time the software is received, it remains under continuous control. All shrink wrapped packaging is opened and installed inside the secure FBCA facility under multi-person control**.** McAfee AntiVirus will be 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 at startup, periodically, and any time a system configuration change occurs (i.e., adding a new CA to the FBCA).

- CA software and hardware is dedicated to performing CA functions only.

6.6.2 Security management controls

The initial configuration of the FBCA software (i.e., CA software, repository software) as well as any modifications and upgrades will be documented and controlled in accordance with FPKIA Configuration Management Procedures (separate FPKI OA document). System and application level logging will be 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 above. AP01 – Audit Procedures are used to ensure the integrity of the software. These procedures are performed on a weekly basis.

6.7 NETWORK SECURITY CONTROLS

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are as stated above in Section 6.2

7. CERTIFICATE AND CARL/CRL PROFILES

The FPKIPA has defined the Certificate and CARL/CRL profiles used by the FBCA. The profiles are described in the FBCA Interoperability Guidelines, however, for ease of reference, this CPS also includes a selective description in the following sections.

7.1 CERTIFICATE PROFILE

The FBCA will issue cross-certificates in accordance with the BCA certificate profile contained in the *Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile* [FPKI-Prof].

7.1.1 Version numbers

The FBCA issues X.509 v3 certificates (populate version field with integer "2").Certificate Extensions

No critical extensions will be included in the certificates other than those listed in [FPKI-Prof].

7.1.2 Algorithm object identifiers

Certificates issued by the FBCA comply with the Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile [FPKI-Prof]. In compliance with [FPKI-Prof] cross-certificates issued by the FBCA use the following OIDs for signatures:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

In compliance with [FPKI-Prof] , cross-certificates issued by the FBCA use the following OIDs for identifying the algorithm for which the subject key was generated:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101)

keyExchangeAlgorithm	dod(2) infosec(1) algorithms(1) 22}

Private extensions are not used.

7.1.3 Name forms

The subject and issuer fields of the cross-certificate are populated with an X.500 Distinguished Name, with the attribute type as further constrained by [RFC2459].)

7.1.4 Name constraints

FBCA asserts name constraints in certificates issued to PCAs appropriate for the PKI being certified Certificate policy object identifier.

Cross-certificates issued by the FBCA assert the OID appropriate to the level of assurance with which it was issued.

7.1.5 Usage of Policy Constraints extension

Policy constraints will appear in certificates only when the FBCA directs the OA to inhibit policy mapping.

7.1.6 Policy qualifiers syntax and semantics

In compliance with the FBCA CP the cross-certificates issued by the FBCA do not use policy qualifiers.

7.1.7 Processing semantics for the critical certificate policy extension

Processing semantics for the critical certificate policy extension used by the FBCA conforms to the [FPKI-Prof].

7.2 CARL/CRL PROFILE

The FBCA will issue CARLs and CRLs in accordance with the profile included in [FPKI-Prof].

7.2.1 Version numbers

The FBCA issues X.509 version two (2) CARLs/CRLs.

7.2.2 CARL and CRL entry extensions

Detailed CARL/CRL profiles addressing the use of each extension conform to [FPKI-PROF].

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

Errors, updates, or suggested changes to this document will be communicated to the contact in section 1.4. Such communication will include a description of the change, justification for the change, contact information for the person requesting the change, and an impact assessment.

Changes to this document will be reviewed and approved by the FPKIPA, will be communicated to every Entity Principal CA, and will be posted at the website specified in section 2.6.4.

Errors, updates, or suggested changes to this CPS are notified to all Entity PCAs. All versions of this document will be reviewed and approved by the FPKIPA.

Revised versions of this document will be disseminated to interested parties (see section 8.2)

8.2 PUBLICATION AND NOTIFICATION POLICIES

The FPKIPA will publish information (including the redacted version of this CPS) on the following web sites: http://www.cio.gov/fpkipa.

The redacted version of this CPS will also be disseminated via email to any that request it.

Proposed changes to the CPS will be sent to Entity PCAs.

The FPKIPA will provide an updated and approved document within 1 week to the PA web administrator, who has agreed to post this information.

8.3 CPS APPROVAL PROCEDURES

The FPKIPA will make the determination that this CPS complies with FBCA CP. The FPKIPA will also determine if a change to this CPS is acceptable and that the changed CPS continues to comply with the FBCA CP.

8.4 WAIVERS

There will be no waivers to the CPS – any changes will be effected through approval of a revised CPS.

9. BIBLIOGRAPHY

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

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

FIPS 112 Password Usage, 1985-05-30 http://csrs.nist.gov/fips/

FIPS 140-1 Security Requirements for Cryptographic Modules, 1994-01 http://csrs.nist.gov/fips/fips1401.htm

FIPS 186 Digital Signature Standard, 1994-05-19 http://csrs.nist.gov/fips/fips186.pdf

FOIACT 5 U.S.C. 552, Freedom of Information Act. Http://www4.law.cornell.edu/uscode/5/552.html

FPKI-E Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997

ISO9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997. ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc

ITMRA 40 U.S.C. 1452, Information Technology Management Reform Act of 1996. Http://www4.law.cornell.edu/uscode/40/1452.html

NAG69C Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NSD42 National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. Http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)

NS4005 NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

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

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

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

Security Requirements for Certificate Issuing and Management Components, 3 November 1999, Draft

Digital Signatures, W. Ford

United States Department of Defense X.509 Certificate Policy, Version 5.0, 13 December 1999

10. ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CARL	Certificate Authority Revocation List
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FPKI OA	Federal PKI Operational Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority
GPEA	Government Paperwork Elimination Act of 1998
IETF	Internet Engineering Task Force

ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
MOA	Memorandum of Agreement (as used in the context of this CP, between an Entity and the FPKIPA allowing interoperation between the FBCA and Entity PCA)
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
UPS	Uninterrupted Power Supply

URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

11. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [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	For purposes of this CPS only, agency is defined as any instrumentality of the federal government, executive, legislative, or judicial branch.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an

	identity.
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. [NS4009, "audit 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 certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.

Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two

	Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate, which is composed of two subfields; "date of issue" and "date of next issue".
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an Entity as defined above.

Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
Entity	For purposes of this CPS, Entity is any person, organization, corporation, or government (state, local, federal, or foreign) operating, or directing the operation of, one or more CAs.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity.
Federal Bridge Certification Authority (FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability among Entity Principal Certification Authorities.
Federal Bridge Certification Authority Membrane	The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.
FPKI Operational Authority (FPKI OA)	The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.

Federal Public Key Infrastructure Policy Authority (FPKI PA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [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.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.

Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the FPKIPA and an Entity allowing interoperability between the Entity PCA and the FBCA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).

Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction,

	disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the FPKIPA.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA.
Privacy	Restricting access to subscriber or Relying Party information in accordance with applicable law and policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure	A set of policies, processes, server platforms, software and

(PKI)	workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful

	result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.

System High	The highest security level supported by an information system. [NS4009]
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Token	Hardware or software that contains or can be used to generate cryptographic keys. Examples of hardware tokens include smart cards and memory cards. Software tokens include both software cryptographic modules that store or generate keys and storage devices or messages that contain keys (e.g., PKCS #12 messages).
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

APPENDIX A SELECTED EXCERPTS FROM THE CURRENT FBCA SSP

In order to supplement the description in section 5.3.1 in the main document, this appendix provides the reader with excerpts from the current FBCA System Security Plan (SSP) in the area of personnel security.

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

Part 2: X.509 Certification Practice Statement (CPS) For the Federal Public Key Infrastructure Common Policy Framework (FCPF) Certification Authority

United States
Federal PKI Architecture

Federal PKI Architecture X.509 Certification Practice Statement – Part 2: Public X.509 Certification Practice Statement For the Federal PKI Common Policy Framework Certification Authority

13 September 2005

Table of Contents

1. FCPF CA CPS INTRODUCTION

This Certification Practice Statement (CPS) for the Federal Common Policy Framework Certification Authority (FCPFCA) is part two (2) of the FPKIA CPS and it documents the internal practices and procedures used by the Federal Public Key Infrastructure Architecture Operational Authority (FPKI OA) by describing the practices concerning lifecycle services in addition to issuance, such as certificate management (including publication and archiving), revocation, and renewal or re-keying.

This CPS covers the operation of systems and the management of facilities, which include FCPF CA (trust anchor) and the Federal PKI Architecture common repository functionality, used to post CA certificates and CRLs concerning the qualified shared service providers PKI domains.

FCPF CA acts as the trust anchor for the federal government PKI domains. FCPF CA issues and manages certificates for the shared service provider program as defined by the Shared Services Provider Working Group, which is a subcommittee of the Federal Identity Credentialing Committee (FICC). The Shared Service Provider program is designed to facilitate outsourcing of PKI services by Federal agencies.

The FCPF incorporates three specific certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, and a policy for devices.

This CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework.

This CPS implements and complies with the requirements established in the FCPF, dated 10 February 2004, for the secure distribution of self-signed certificates for use as trust anchors.

1.1 OVERVIEW

1.1.1 Certification Practice Statement

This Certification Practice Statement (CPS) documents the internal practices and procedures used by the Federal PKI Operational Authority (OA). It covers the operation of systems and the management of facilities, which include FCPF CA (trust anchor) and the Federal PKI Architecture common repository functionality, used to post CA certificates and CRLs concerning the qualified shared service providers PKI domains.

1.1.2 Relationship Between the CP and the CPS

The FCPF CP states what assurance can be placed in a certificate issued by the FCPF CA. This Certification Practice Statement (CPS) states how the FCPF CA establishes that assurance.

1.1.3 Scope

This CPS implements the FCPF certificate policy that applies to certificates issued to shared services providers CAs, which, in turn, will then issue certificates under the FCPF policy to CAs devices, Federal employees, contractors and other affiliated personnel. This CPS implements the FCPF and does not apply to certificates issued to groups of people.

1.1.4 Interoperation with CAs Issuing under Different Policies

Interoperation with CAs that issue under different policies will be achieved through policy mapping and cross-certification with the Federal Bridge Certification Authority. Upon formal mapping and approval by the FPKIPA, the FCPF CA is cross-certified with the FBCA element of the Federal PKI hub.

1.2 IDENTIFICATION

This CPS is referred to as the FCPF CPS and provides substantial assurance concerning identity of certificate subjects. Certificates issued to shared service providers CAs in accordance with this CPS assert all the following OIDs in the certificate policy extension:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}

id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

1.3 COMMUNITY AND APPLICABILITY

The following are roles relevant to the administration and operation of CAs under the FCPF policy.

1.3.1 PKI Authorities

The following table summarizes the roles relevant to the administration and operation of the FCPF CA. These roles are entirely defined in the FCPF CP.

Table 1.3.1-1

FCPF Role	***Description***
PKI Policy Authority	The Federal PKI Policy Authority (PA) is a group of U.S. Federal Government Agencies (including cabinet-level Departments) established by the Federal CIO Council. The FPKIPA is responsible maintaining the FCPF policy, approving the CPS for each CA that issues certificates under this policy, and approval of the compliance audit report for each CA issuing certificates under this policy.
Certification Authority	The FCPF CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. The FCPF CA is responsible for the issuing and managing certificates including— – The certificate manufacturing process – Publication of certificates – Revocation of certificates – Generation and destruction of FCPF CA signing keys – Ensuring that all aspects of the FCPF CA services, operations, and infrastructure related to certificates issued under the FCPF CP are performed in accordance with the requirements, representations, and warranties of the FCPF CP.
Registration Authority	The registration authority (RA) is the entity that collects and verifies each subscriber's identity and information that are to be entered into the subscriber's public key certificate. The FCPF RA performs its function in accordance with the FCPF CPS approved by the FPKIPA. The RA is responsible for— – Control over the registration process – The identification and authentication process
Related Authorities	The CAs and RAs operating under the FCPF will require the services of other security, community, and application authorities, such as compliance auditors, information systems security officer (ISSO) and information systems security manager (ISSM), and attribute authorities. This CPS identifies the parties responsible for providing such services, and the mechanisms used to support these services.
Trusted Agent	The trusted agent is a person who satisfies all the trustworthiness requirements for an RA and who performs identity proofing as a proxy for the RA. The trusted agent records information from and verifies biometrics (e.g., photographs) on presented credentials for applicants who cannot

FCPF Role	*Description*
	appear in person at an RA. This CPS identifies the parties responsible for providing such services, and the mechanisms for determining their trustworthiness.
End Entities	Subscribers A subscriber is the entity whose name appears as the subject in a certificate. The subscriber asserts that he or she uses the key and certificate in accordance with the certificate policy asserted in the certificate, and does not issue certificates. For the FCPF, subscribers are limited to Federal employees, contractors and affiliated personnel. CAs are sometimes technically considered "subscribers" in a PKI. However, the term "subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information. Relying Parties A relying party is the entity that relies on the validity of the binding of the subscriber's name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The relying party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A relying party may use information in the certificate (such as CP identifiers) to determine the suitability of the certificate for a particular use. For this certificate policy, the relying party may be any entity that wishes to validate the binding of a public key to the name of a federal employee, contractor, or other affiliated personnel.

1.3.2 Applicability

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. This evaluation is done by each organization for each application and is not controlled by this CP.

This CP is intended to support the use of validated public keys to access Federal systems that have not been designated national security systems. While a validated public key is not generally sufficient to grant access the key may be sufficient when supplemented by appropriate authorization mechanisms. Credentials issued under this CP may also be used for key establishment. This policy is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statues and regulations.

Credentials issued under the user software policy are intended to meet the requirements for Level 3 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth] Credentials issued under the user hardware policy meet the requirements for Level 4 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth]

In addition this policy may support signature and confidentiality requirements for Federal government processes.

1.4 CONTACT DETAILS

1.4.1 Specification Administration Organization

The FPKI OA is responsible for all aspects of this CPS.

1.4.2 Contact Person

Questions regarding this CPS shall be directed to the FPKIA Program Manager and the Chair of the Federal PKI Policy Authority, whose address can be found at http://www.cio.gov/fbca and http://www.cio.gov/fpkipa, respectively.

1.4.3 Person Determining CPS Suitability for the Policy

The FPKIPA shall approve this CPS for the FCPF CA. Reference Section 8.3, CPS Approval Procedures.

2. GENERAL PROVISIONS

2.1 OBLIGATIONS

2.1.1 PA Obligations

The PA —

- Approves this CPS as well as the CPS for each CA that issues certificates under this policy;
- Reviews periodic compliance audits to ensure that this FCPF CA and the other CAs are operating in compliance with their approved CPSes;
- Reviews name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under the FCPF CP;
- Revises the FCPF CP to maintain the level of assurance and operational practicality;
- Publicly distributes the FCPF CP; and
- Coordinates modifications to the FCPF CP to ensure continued compliance by this FCPF CA and the other CAs operating under approved CPSes.

2.1.2 FPKIA Obligations

The FPKI OA—

- Reviews periodic compliance audits to ensure that RAs and other components operated by the OA are operating in compliance with FCPF approved CPS; and
- Reviews name space control procedures to ensure that distinguished names are uniquely assigned within the FPKI OA.

2.1.3 CA Obligations

The FPKI OA, which operates the FCPF CA abides with the stipulations defined in the FCPF CP document, including—

- Providing the FPKIPA with this CPS, as well as any subsequent changes, for conformance assessment.

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Ensuring that registration information is accepted only from the FCPF RA operating under this CPS.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with Section 2.1.4 as requested and/or approved by the FPKIPA.
- Operating or providing for the services of an online repository that satisfies the obligations under Section 2.1.5.

2.1.4 RA Obligations

The FPKI OA is the RA for the FCPF CA and is responsible for controlling the registration process, and conforms to the stipulations of the FCPF CP, including—

- Maintaining its operations in conformance to the stipulations of this CPS.
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
- Ensuring that obligations are imposed on subscribers in accordance with Section 2.1.3, and that subscribers are informed of the consequences of not complying with those obligations.

2.1.5 Subscriber Obligations

The only potential FCPF CA subscribers identified are the FCPF CA OA Administrator and the FCPF CA OA Security Officers, and the shared service providers CAs. The FCPF CA does not issue certificates to any other end-entity subscriber, rather it merely issues CA certificates to subordinate shared service providers and cross-certifies with the FBCA (not a subscriber) upon formal mapping approval by the FPKIPA.

2.1.6 Relying Party Obligations

The relying party decides, pursuant to its own policies, what steps to take. The FCPF CA merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination.

2.1.7 Repository Obligations

The FCPF CA posts all CA certificates and all CRLs in the Federal PKI online directory that is publicly accessible through the Lightweight Directory Access Protocol as well as via X.500 DSP chaining. To promote consistent access to certificates and CRLs, the repository implements access controls preventing modification or deletion of information.

The FPKIPA will be maintaining a web server (see section 2.6.4) to post FCPF CA for official use only (FOUO) documentation, including the CP, CPS, and FPKIPA procedural documents.

2.2 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. Certificates are issued and revoked at the sole discretion of the Federal PKI Policy Authority.

2.3 FINANCIAL RESPONSIBILITY

The FCPF CP contains no limits on the use of certificates issued by CAs under its policy. Rather, entities, acting as Relying Parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

2.3.1 Indemnification by Relying Parties and Subscribers

The FCPF CP does not stipulate a requirement for this section.

2.3.2 Fiduciary Relationships

The FCPF CP does not stipulate a requirement for this section.

2.4 INTERPRETATION AND ENFORCEMENT

The terms and provisions of the PCPF Certificate Policy are interpreted under and governed by applicable Federal law.

2.4.1 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of the FCPF CP, hence the corresponding section in this CPS, is incorrect or invalid, the other sections of this CPS shall remain in effect until the FCPF CP is updated. The process for updating the FCPF CP, and the corresponding FCPF CA CPS, is described Section 8.1 in the FCPF CP and this CPS, respectively.

2.4.2 Dispute Resolution Procedures

The FPKIPA will facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under the FCPF certificate policy. When the dispute is between Federal agencies, and the PA is unable to facilitate resolution, dispute resolution may be escalated to OMB or U.S. Department of Justice, Office of Legal Counsel as necessary.

2.5 FEES

The FCPF CP does not stipulate a requirement for this section. The FPKI OA will determine the fees, if any, for FCPF CA services, as approved by the FPKIPA.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of CA Information

CA Certificates issued to qualified shared service providers and CRLs are published as specified in Section 2.1.7. The FPKI OA will deliver this CPS to the FPKIPA and any relevant authorized authority in the Federal government with need to know. The FCPF CP does not stipulate requirements regarding publication of additional CA information.

2.6.2 Frequency of Publication

CA Certificates issued to subordinate qualified shared service providers are published following FPKIPA approval acceptance as specified in Section 4.3 and proof of possession of private key as specified in Section 3.1.7. The CRL is published as specified in Section 4.4.3.1. All information to be published in the repository shall be published promptly after such information becomes available to the FCPF CA. The FCPF CA time limits within which the OA will publish various types of information are within 15 minutes of issuance

2.6.3 Access Controls

The Federal PKI Architecture OA will protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository are publicly available through the Internet, via LDAP queries and X.500 DSP interactions. Access to other information in the FCPF CA repository (i.e., the Federal PKI online directory system) shall be determined by the OA and by the FPKIPA. This CPS details in section 2.8 what information in the repository is exempt from automatic availability and to whom, and under which conditions, the restricted information may be made available.

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” (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, is omitted in the publicly universally available version of this document. Upon request, this information is available to authorized organizations with a need to know.

The web site publishing this CPS enables a read-only access to the public version of the FCPF CA CPS. Only authorized personnel have access to modify both versions of CPS. The procedure for updating the documents on the web server consists of an out-of-band mechanism.

2.6.4 Repositories

See Section 2.1.7.

2.7 COMPLIANCE AUDIT

2.7.1 Frequency of Entity Compliance Audit

The FPKI OA will arrange initially and annually for independent inspections and compliance audits to validate that the FCPF CA is operating in accordance with the security practices and procedures described in this CPS. Results of the compliance audit will be provided to the FPKIPA.

2.7.2 Identity/Qualifications of Compliance Auditor

The FBCA compliance audits will be provided by an independent auditor as agreed between the FPKIPA and FPKI OA, which has demonstrated a proven track record and thoroughly familiar with the this CPS and the FCPF CP.

The FPKIPA has chosen the following organization to conduct the compliance audit:

Name of the Auditor Organization: KPMG

The selected auditor will verify and validate through document reviews and demonstrations that the FCPF CA complies with the FCPF CP and requirements that the FPKIPA imposes on the issuance and management of FCPF CA certificates.

2.7.3 Compliance Auditor's Relationship to Audited Party

The selected FCPF CA compliance auditor is a contractor that is independent from FPKI OA and the FPKIPA. This contractor provides an unbiased, independent evaluation and is one whose primary responsibility is the performance of EDP Compliance Audits.

2.7.4 Topics Covered by Compliance Audit

The purpose of a compliance audit is to verify that the FCPF CA complies with all the requirements of the current versions of this CPS and the FCPF CP. The compliance audit inspections encompass all aspects of the CA/RA operation thereby identifying potential discrepancies between the requirements of the FPCF CP or the stipulations in this CPS and the design, operation, or maintenance FCPF CA.

2.7.5 Actions taken as a result of deficiency

The FCPF CA compliance auditor will identify and note any discrepancies then notify within 24 hours the FPKI OA. The FPKI OA will then notify the FPKIPA of the results of the compliance audit by e-mail and/or out-of-band writing within 24 hours of the compliance assessment.

Once notified, the FPKIPA and FPKI OA 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 FCPF CA compliance auditor, depending upon the nature and severity of the discrepancy and how quickly it can be corrected, the FPKIPA possible courses of actions include:

- temporarily halt operation of the FCPF CA,
- revoke the FCPF CA self-signed certificate or
- take other actions it deems appropriate.
- The FPKIPA will develop procedures for making and implementing such determinations.

2.7.6 Communication of Results

The auditor will provide the FPKI OA and the FPKIPA with a written (signed email and/or letter) notification of results of the compliance audit of the FCPF CA within 24 hours. The complete results will be provided as a written report. Such report will contain a summary table of topics covered, areas in which FCPF CA 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 FCPF CA passed and the topics in which the FCPF CA failed.

In case of compliance failure, the notification will be provided within 24 hours, upon the conclusion of the compliance audit, in a written form (signed e-mail and/or out of band letter) to the FPKI OA and to the FPKIPA, and will include, the topics of failure, reason(s) for failure, and possible remedies A comprehensive report may be provided later. After 10 days, the FPKI OA will identify a list of corrective measures taken or proposed to be taken and submit to the FPKIPA.

The FPKIPA might request an additional special compliance audit to confirm the implementation and effectiveness of the remedy.

2.8 CONFIDENTIALITY

CA information not requiring protection is made publicly available. Federal PKI Policy Authority access to shared service provider information is addressed in agreement with that shared service provider. Public access to shared service provider information is determined by the respective shared service provider.

The FPCF CA will disclose confidential information to any third party when required by this CPS, FCPF, 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 (IG);
- The individual is the subscriber itself; or
- The individual has a duly signed request from the subscriber requesting the release of the information from the subscriber

Court orders and IG requests must be approved by specific shared service provider General Counsel.

2.9 INTELLECTUAL PROPERTY RIGHTS

No stipulation.

3. IDENTIFICATION AND AUTHENTICATION

This section contains the practices the FPKI OA follows in registering, identifying, and authenticating shared service providers and sponsors involved in the certification request process.

3.1 INITIAL REGISTRATION

The registration process followed by the applicant shared service providers is described in the "Shared Service Provider Roadmap: Navigating the Process to Acceptance" version 1.5 dated 5 march 2004 [ROAD] developed by the FICC shared service provider subcommittee.

3.1.1 Types of Names

The FCPF CA generates and signs certificates where the issuer DN is:

c=us, o=U.S. Government, ou=FBCA, cn=Common Policy Root

The FCPF CA assigns X.500 distinguished names to all shared service provider subscribers. These distinguished names may be in either of two forms: an X.501 distinguished name specifying a geo-political name; and an Internet domain component name.

3.1.2 Need for Names to be Meaningful

Names used in the FCPF CA certificates identify the shared service provider subscriber in a meaningful way and are created by the applicant shared service provider and vetted by the FPKIPA.

The subject name in FCPF CA certificates matches the issuer name in certificates issued by the subject, as required by RFC 3280, even if the subject's name is not meaningful.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are specified in [USGold].

3.1.4 Uniqueness of Names

The FPKIPA manages the name uniqueness for certificates issued by the FCPF CA. The FPKIPA will assign names, whether X.500 DNs or other name forms (e.g., an electronic mail address or DNS name), and ensure their uniqueness. Additionally, the FCPF CA is configured to require name uniqueness when issuing subordinate CA certificates to shared service providers.

This CPS identifies a directory information tree for the assignment of subject names in section 3.1.1 and 3.1.2.

Each shared service provider CA has their own name space and these are verified for correctness during the Shared Service Provider application process.

3.1.5 Name Claim Dispute Resolution Procedure

The FPKIPA will resolve all name collisions disputes that occur within the FCPF CA name space operated by the FPKI OA.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.1.7 Method to Prove Possession of Private Key

The FPKI OA verifies that a prospective shared service provider subordinate certificate applicant possesses the private key corresponding to the public key submitted with the application in accordance with section 4.2. All transactions involved in CA certificate issuance to the shared service provider are recorded as part of the security audit data, as described in section 4.5.1. Since the FPCF CA is at all times off-line, these messages are exchanged using an out-of-band mechanism as described in section 4.2.

3.1.8 Authentication for CA Certificate Issuance

The FPCF CA will issue certificates to shared service providers as directed by the FPKIPA. The FPKIPA will authenticate the shared service provider's organization identity as part of the application processes, as described in "Shared Service Provider Roadmap: Navigating the Process to Acceptance" version 1.2 March 2004.

3.1.9 Authentication of Individual Identity

Only the FPKI OA Security Officers have FPCF CA-issued certificates for their activity.

3.1.10 Authentication of Component Identities

The FPCF CA will not issue certificates to components. No stipulation.

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

The procedures for accomplishing the Certificate Renewal, Update, and Routine Re-Key specified in the FCPF CP are detailed in this CPS.

3.2.1 Certificate Renewal

The FCPF CA does not re-new shared service provider subscriber certificates issued under the FCPF policy, except during recovery from FCPF CA key compromise (see 4.8.3).

3.2.2 Certificate Re-Key

FCPF CA certificate re-key activity follows the same procedures as its initial certificate issuance. If more than 6 years have passed since a subscriber's identity was authenticated as specified in Section 3.1, a shared service provider certificate re-key will follow the same procedures as initial certificate issuance.

3.2.3 Certificate Update

The FCPF CA will generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users.

3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION

In the event of certificate revocation, issuance of a new certificate always requires that the shared service provider go through the initial registration process per Section 3.1 above.

3.4 REVOCATION REQUEST

The FCPF will revoke CA certificates issued to shared service providers only upon explicit request from the FPKIPA. The FCPF CP requires that revocation requests be authenticated. A revocation request by the FPKIPA or a subject is authenticated as described in the revocation procedure SO02. Revocation requests are authenticated and processed as described in section 4.4. The CAs will not allow issuance without verifying the digital signature (this is done by the CA software). Digitally signatured revocation requests are not currently supported, however, will be accepted in the future.

4. OPERATIONAL REQUIREMENTS

4.1 APPLICATION FOR A CERTIFICATE

Following successful completion of the application process by a prospective shared service provider and its subsequent approval by the FPKIPA, the FPKI OA performs the following steps upon FPKIPA request in order to issue a certificate to an applicant (prospective shared service provider):

- Establish the applicant's authorization (by the employing or sponsoring agency) to obtain a certificate. (per Section 3.1)
- Establish and record identity of the applicant (per Section 3.1)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required (per Section 3.1.7)
- Verify any role or authorization information requested for inclusion in the certificate.

These steps, performed in any order that is convenient for the FPKI OA and FPKI approved-applicants and does not defeat security, are completed before any subordinate share service provider CA certificate issuance. All communications among FPKI Authorities supporting the certificate application and issuance process is via an out-of-band secure mechanism, as described in the issuance procedure SO01.

4.1.1 Delivery of Public Key for Certificate Issuance

Shared service provider CA public keys are delivered to the FPKI OA electronically in a digitally signed certificate request (i.e., using PKCS #10) message to the FPKI OA via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier). Identity checking and proof of possession of the private key is accomplished as described in this CPS in sections 3.1.8 and 4.2 respectively.

4.2 CERTIFICATE ISSUANCE

The FPKI OA issues CA certificates to the subordinate shared service provider CA by the following procedure:

1. Upon receiving a signed request message (PKCS#10 message) from the shared service provider CA and having verified the requestor identity as described in section 3.1.8, the FCPF CA software verifies the signature to prove possession of the private key. Then, after all requirements / criteria have been satisfied, the FCPF CA will sign and issue CA certificate to the shared service provider CA.

2. The certificate issued by the FCPF CA will be delivered to the shared service provider CA in a signed response message (PCKS#10), via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier).

3. Each CA certificate issued by the FCPF CA is manually checked to ensure each field and extension is properly populated with the correct information, before the CA certificate is delivered to the shared service provider CA.

4. The FPKI OA will post the certificate (subordinate CA certificate) in the FPKI OA repository.

4.2.1 Delivery of Subscriber's Private Key to Subscriber

The FCPF CA does not generate subscriber private keys.

4.2.2 Public Key Delivery and Use

The public key of the FCPF CA is posted in the FPKI OA online directory for certification trust paths to be created and verified.

Where users rely on the CA's public key as a trust anchor, publication in the repository does not permit verification of the public key. To extract the key from a certificate with confidence that it has not been altered, 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 Certificate, or Trusted Certificate. This document will use the term Trusted Certificate.

The FPKI OA delivers the FCPF CA Trusted certificate to the applicant shared service provider via out-of-band courier mechanism. The FCPF CA will create key rollover certificates as a consequence of FCPF CA re-key. The new FCPF CA keys may be used securely (through the X.509 path validation algorithm) without explicit delivery of the public key to subscribers.

4.3 CERTIFICATE ACCEPTANCE

The MOA sets forth responsibilities of shared service providers and the FPKIPA before the FPKIPA authorizes issuance of an FCPF subordinate CA certificate to the shared service provider CA. Once a subordinate CA certificate has been issued, its acceptance by the shared service provider CA completes the insertion of the shared service provider in the list of approved providers. This triggers its obligations under the MOA and this CPS.

Before a shared service provider can make effective use of its private key, a the FPKI OA will—

- Explain to the shared service provider its responsibilities as defined in Section 2.1.5
- Inform the shared service provider of the creation of a certificate and the contents of the certificate.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Revocation

4.4.1.1 Circumstances for Revocation

There are three circumstances where certificates issued by the FCPF CA can be revoked:

4. When the FPKIPA requests that an FCPF CA-issued certificate be revoked. This will be the normal mechanism for revocation in cases where the FPKIPA determines that a

shared service provider does not meet the FCPF requirements or certification of the shared service provider is no longer in the best interest of the federal government.

5. When the FPKI Operational Authority receives an authenticated request from a previously designated official of the shared service provider responsible for the CA (such official or official shall be identified in the MOA as authorized to make such a request).

6. When the FPKI Operational Authority personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the FCPF CA. Under such circumstances, the following individuals may authorize immediate certificate revocation:

    a. Chair of the FPKI Policy Authority

    b. Chair of the FICC

    c. Director of the FPKI Operational Authority

    d. As designated by the FPKI Policy Authority

The FPKI PA shall meet as soon as practical to review the emergency revocation.

Additionally, certificate is revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding are—

Identifying information or affiliation components of any names in the certificate becomes invalid.

Privilege attributes asserted in the shared service provider certificate are reduced.

The shared service provider can be shown to have violated the stipulations of its MOA.

There is reason to believe the private key has been compromised.

Whenever any of the above circumstances occur, the associated certificates will be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the expiration date of the cross-certificate.

The FPKI OA posts the CRL and/or CARL to the FPKIA repository (see section 2.6.4) within 6 hours of notification. Certificates are removed from the CRL and/or CARL after the expiration date of the certificate; however the revoked certificate must appear on at least one published CRL and/or CARL.

4.4.1.2 Who Can Request a Revocation

An FCPF CA certificate issued to a subordinate shared service provider CA (or cross-certificate to the FBCA) is revoked (1) upon direction of the FPKIPA, or (2) upon an authenticated request

by a previously designated authorized official of the subordinate shared service provider CA (or the FBCA) (such official or officials are established in the MOA as authorized to make such a request) (3) when the FPKI Operational Authority personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the FCPF CA (or cross-certificate to the FBCA) (see section 4.4.1). In the last case, a written notice and brief explanation for the revocation shall subsequently be provided to the shared service provider.

4.4.1.3 Procedure for Revocation Request

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

8. An authorized official of shared service provider CA, or the FPKI PA, drafts an authenticated request to revoke a certificate. The individual then notifies the request to the FPKI OA Administrative/Help desk via phone as well as submits the request via signed e-mail to the FPKI OA identifying the certificate to be revoked, explaining the reason for revocation.

9. Upon receipt of a signed revocation request, the FPKI OA authenticates the request by verifying the digital signature and/or making direct contact (call back or challenge/response telephone conversation) with the shared service provider CA POC (or the FPKI PA).

10. In the event the request to revoke originates from the shared service provider CA, the FPKI OA apprises the FPKIPA of the request for revocation.

11. The FPKIPA evaluates and verifies the need for revocation expressed in the authenticated request. If the revocation request appears to be valid, the FPKIPA will direct the FPKI OA to proceed with revocation.

12. The FPKI OA will revoke the certificate, which automatically generates and adds a CRL entry for that certificate within 6 hours of notification of approval by the FPKIPA.

13. The FPKI OA ensures the new CARL/CRL is posted in the FBCA repository within 6 hours of notification of approval by the FPKIPA.

The FPKI OA may revoke a certificate prior to notification and approval of the FPKIPA as set forth in emergency revocation procedures consisting of the following steps:

4. Notify all identified POCs in the emergency list of FPKIA (i.e., FICC POC, FPKI OA POC, affected shared service provider CA POC, CPWG POC). This can be done by either:

    a. Telephone (using one of call-back or challenge/response protocols)

    b. Signed FAX

    c. Signed e-mail

5. Revoke the certificate and post the new CRL/CARL

6. Once the incident has been investigated and documented, issue a new CA certificate to replace the one that has been revoked, as directed by the FPKIPA.

4.4.1.4 Revocation Request Grace Period

There is no grace period for revocation under the FCPF; the FCPF CA will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests are be processed before the next CRL is published, excepting those requests received within 2 hours of CRL issuance. Revocation requests received within 2 hours of CRL issuance are processed before the following CRL is published.

4.4.2 Suspension

Certificate suspension for CA certificates is not allowed by the FCPF. However, the FCPF allows the use of certificate suspension for end entity certificates.

4.4.3 CRLs

The FCPF CA issues CRLs covering all unexpired certificates issued under the FCPF.

The FPKI OA issues Certification Authority Revocation Lists (CARLs) and Certificate Revocation Lists (CRLs) in accordance with the CARL/CRL profile specified in [CCP-Prof]. The contents of CARLs and CRLs are checked to ensure that all information is correct by using mechanisms provided by the FCPF CA software or third-party software.

4.4.3.1 CRL Issuance Frequency

CARLs and CRLs are issued 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 FCPF CA to the shared service providers. 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 provided in section 4.4.1.3. The current CARL/CRL will be removed and replaced with the updated CARL/CRL.

4.4.4 Online Revocation/Status Checking Availability

The FCPF CA does not plan to support the Online Certificate Status checking Protocol (OCSP) capability for its cross-certificates.

4.4.5 Other Forms of Revocation Advertisements Available

The FCPF CA does not support any other forms of revocation advertisements.

4.4.6 Checking Requirements for Other Forms of Revocation Advertisements

The FCPF CA does not support any other forms of revocation advertisements.

4.4.7 Special Requirements Related to Key Compromise

In the event of a FCPF CA private key compromise, the following operations must be performed.

- Revoke all certificates (cross-certificates, subordinate certificates, self-signed certificates)
- Generate a new signing key pair and corresponding Trusted Certificate;
- Initiate procedures to notify SSPs of the compromise; and
- Securely distribute the Trusted Certificate.
- FCPF CA renews current certificates under the new signing key. (see section 3.2.1)

The above operations are described in the revocation procedure SO02 and security incident/escalation procedures HD01 and HD02.

4.5 SECURITY AUDIT PROCEDURE

The FPKI OA generates audit log files for all events relating to the security of the FCPF CA. 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. The security audit logs for each auditable event defined in this section are maintained in accordance with *Retention period for archive*, Section 4.6.2.

4.5.1 Types of Events Recorded

Security auditing capabilities of the FPKIA repository, the FCPF CA operating system, and CA applications have been enabled for logging the types of events specified in the table below. The table indicates whether the auditable event is logged automatically by the application/operating system, or it is logged manually in a logbook as prescribed by applicable procedures. 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 FCPF CA or signing process
- A success or failure indicator when performing certificate revocation
- The identity of the entity and/or operator (of the FCPF CA) that caused the event.

- A message from any source requesting an action by the FCPF CA is an auditable event. The message includes message date and time, source, destination and contents.

The FPKI OA staff has verified (i.e., obtained vendor statements and conducted direct testing) that the equipment and application software purchased indeed supports capturing audit logs for the events specified in the table below.

Table 4.5.1-1 Auditable Events

Auditable Event	FPKIA Directories		FPCF CA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
SECURITY AUDIT				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	✓			✓
Any attempt to delete or modify the Audit logs	✓ After a deletion following any archive operation	✓ After a modification following any archive operation		✓
Obtaining a third-party time-stamp	✓	✓	✓	✓
IDENTIFICATION AND AUTHENTICATION				
Successful and unsuccessful attempts to assume a role		✓		✓
Change in the value of maximum authentication attempts	✓			✓
Maximum number of unsuccessful authentication attempts during user login		✓		✓
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	The account is immediately re-activated	The account is immediately re-activated		✓
An Administrator changes the type of authenticator, e.g., from password to biometrics	✓			✓
LOCAL DATA ENTRY				
All security-relevant data that is entered in	✓	✓	✓	✓

Auditable Event	FPKIA Directories		FPCF CA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
the system		Through Windows/ISODE Logging		Through Windows/CA Logging
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system	✓	✓ Through firewall Logs and Netmon	✓	✓ Through firewall Logs and Netmon
DATA EXPORT AND OUTPUT				
All successful and unsuccessful requests for confidential and security-relevant information	✓ Manual Logs		✓ Manual Logs	
KEY GENERATION				
Whenever the FBCA-CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	Applies to CA only	Applies to CA only	✓	✓
SECRET KEY STORAGE				
The manual entry of secret keys used for authentication	Applies to CA only	Applies to CA only	✓	✓ CA,Smart Card logging / Luna Logs
PRIVATE KEY LOAD AND STORAGE				
The loading of Component private keys	Applies to CA only	Applies to CA only	✓	
All access to certificate subject private keys retained within the FBCA CA for key recovery purposes	Applies to CA only	Applies to CA only	✓	
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	✓	✓
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret keys (keys used for a single session or message are excluded)	Applies to CA only	Applies to CA only	✓	✓
CERTIFICATE REGISTRATION				

Auditable Event	FPKIA Directories		FPCF CA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
All certificate requests	Applies to CA only	Applies to CA only	✓	✓
CERTIFICATE REVOCATION				
All certificate revocation requests	Applies to CA only	Applies to CA only	✓	✓
CERTIFICATE STATUS CHANGE APPROVAL				
The approval or rejection of a certificate status change request	Applies to CA only	Applies to CA only	✓	✓
FBCA CA CONFIGURATION				
Any security-relevant changes to the configuration of the FBCA CA	Applies to CA only	Applies to CA only	✓	✓
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	✓		✓	✓
The access control privileges of a user account or a role are modified	✓		✓	✓
CERTIFICATE PROFILE MANAGEMENT				
All changes to the certificate profile	Cert Profile not captured in Directory	Cert Profile not captured in Directory	✓	
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile	Revocation Profile not captured in Directory	Revocation Profile not captured in Directory	✓	
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	✓	
MISCELLANEOUS				
Appointment of an individual to a Trusted Role	✓		✓	
Designation of personnel for multiparty control	✓		✓	

Auditable Event	FPKIA Directories		FPCF CA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
Installation of the Operating System	✓		✓	✓
Installation of the FBCA CA	Applies to CA only	Applies to CA only	✓	✓
Installing hardware cryptographic modules	Applies to CA only	Applies to CA only	✓	
Removing hardware cryptographic modules	Applies to CA only	Applies to CA only	✓	
Destruction of cryptographic modules	Applies to CA only	Applies to CA only	✓	
System Startup	✓			✓
Logon Attempts to FBCA CA Apps	Applies to CA only	Applies to CA only		✓
Receipt of Hardware / Software	✓		✓	
Attempts to set passwords	✓			✓
Attempts to modify passwords	✓			✓
Backing up FBCA CA internal database	Applies to CA only	Applies to CA only		✓
Restoring FBCA CA internal database	Applies to CA only	Applies to CA only		✓
File manipulation (e.g., creation, renaming, moving)		✓		✓
Posting of any material to a repository		✓		✓
Access to FBCA CA internal database	Applies to CA only	Applies to CA only	✓	✓
All certificate compromise notification requests	Applies to CA only	Applies to CA only	✓	
Loading tokens with certificates	Applies to CA only	Applies to CA only		✓
Shipment of Tokens	Applies to CA only	Applies to CA only	✓	
Zeroizing tokens	Applies to CA only	Applies to CA only		✓
Rekey of the FBCA CA	Applies to CA only	Applies to CA only	✓	✓
Configuration changes to the CA server involving:	Applies to CA only	Applies to CA only		
Hardware	Applies to CA only	Applies to CA only	✓	✓

Auditable Event	FPKIA Directories		FPCF CA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
Software	Applies to CA only	Applies to CA only	✓	✓
Operating System	Applies to CA only	Applies to CA only	✓	✓
Patches	Applies to CA only	Applies to CA only	✓	✓
Security Profiles	Applies to CA only	Applies to CA only	✓	✓
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to room housing FBCA CA	✓	✓	✓	✓
Access to the FBCA CA server	Applies to CA only	Applies to CA only	✓	✓
Known or suspected violations of physical security	✓	✓	✓	
ANOMALIES				
Software Error conditions	✓	✓	✓	✓
Software check integrity failures	✓	✓	✓	✓
Receipt of improper messages	✓	✓	✓	CA is stand alone
Misrouted messages	✓	✓	CA is stand alone	CA is stand alone
Network attacks (suspected or confirmed)	✓	✓	CA is stand alone	CA is stand alone
Equipment failure	✓	✓	✓	✓
Electrical power outages	✓	✓	✓	✓
Uninterruptible Power Supply (UPS) failure	✓	✓	✓	✓
Obvious and significant network service or access failures	✓	✓	CA is stand alone	CA is stand alone
Violations of Certificate Policy	✓	Certain Violations as documented by this table	✓	Certain Violations as documented by this table

Auditable Event	FPKIA Directories		FPCF CA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
Violations of Certification Practice Statement	✓	Certain Violations as documented by this table	✓	Certain Violations as documented by this table
Resetting Operating System clock	✓			✓

4.5.2 Frequency of Processing Data

The FPKI OA Auditor reviews audit logs at least once per month as defined in section 5.2. The FPKI OA Auditor will examine 100% of security audit data generated by the FCPF CA since the last review. The FPKI OA Auditor reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

4.5.3 Retention Period for Security Audit Data

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 for three months but their electronic versions are permanently retained on the primary site server and hence these logs are always available. The FPKI OA Administrator removes audit logs from the FCPF CA and gives them to the FPKI OA Auditor neither of whom commands the FCPF CA signature key(s).

4.5.4 Protection of Security Audit Data

The FPKI OA Auditor performs routine review of security audit logs. The procedure for protecting security audit data is as follows:

6. Security audit logs are automatically time stamped upon creation

7. The only authorized people having read access to the logs include the FPKI OA Administrator, Security Officer, Auditor, Operator, and others possibly designated by the FPKIPA

8. Only the FPKI OA Auditor is authorized to archive audit logs.

9. Audit logs are deleted only under procedural multi-person control.

10. Audit logs are protected under multi-person control and cannot be modified without detection.

Daily audit logs are generated on time stamped digital media and are protected from deletion and/or modification prior to the end of the audit log retention period. See sections 4.5.5, 4.5.6, 4.6, and 5.0 for descriptions of physical and procedural controls for protection of the data.

4.5.5 Security Audit Data Backup Procedures

FPKIA Directory:

Audit logs and audit summaries are incrementally backed up daily via time stamped digital media. Full backups are performed daily via digital tape media. Weekly, the backups are moved to and stored in secure container in a separate building (interim storage) from the FPKIA facility. Additionally, backups are performed at the hot site location to ensure continuity; shadowing the primary directory and performing weekly backups accomplish this.

FCPF CA:

Full backups are performed daily via digital tape media. Weekly backups are moved to and stored in secure container in a separate building (interim storage) from the FPKIA facility.

Manual audit logs will be collected weekly and stored in a secure container in a separate building (interim storage) from the FPKIA facility. These audit logs are moved to the hot site archive location quarterly.

4.5.6 Security Audit Collection System (Internal vs. External)

The audit log collection system is internal to the FPKIA components (see section 4.5.1). Audit processes are invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the FPKI OA will determine whether to suspend FCPF CA operation until the problem is remedied. The FPKIPA will then determine whether to resume operations. Section 4.5.1 describes the collection procedures (manual or automatic) for the auditable events. Section 4.5.5 describes the protection procedures for backing up audited data that has been collected.

4.5.7 Notification to Event-Causing Subject

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

4.5.8 Vulnerability Assessments

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

Vulnerability assessments are conducted as part of security compliance audits as specified by the FPKIPA.

The FPKI OA provides a report of the analysis of the results of vulnerability assessments, specifically indicating security vulnerabilities identified and correction procedures of those vulnerabilities.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Archived

The FPKI OA Auditor produces archive records on a weekly basis. The records are stored on a removable storage medium (i.e., paper, tape, CD-ROM). The archive records include data received from the certificates and CRLs it generated, certificate requests and certificate revocation requests it received.

At initialization, the FPCF CA system equipment configuration files are archived, as well as the CPS and any contractual agreements to which the FPKI OA is bound. During FCPF CA operation, the following data are recorded for archive

- FPKIA certification and accreditation
- Certification Practice Statement
- Contractual obligations
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- Revocation requests
- Subscriber identity Authentication data as per Section 3.1.9
- Documentation of receipt and acceptance of certificates
- Documentation of receipt of tokens
- All certificates issued or published
- Record of Re-key
- All CARLs and CRLs issued and/or published

- All Audit Logs
- Other data or applications to verify archive contents
- Documentation required by compliance auditors

See Section 4.5 for a description of the audit and archive collection procedures.

4.6.2 Retention Period for Archive

Weekly, the backups from the primary site are moved to and stored in secure container in the interim storage facility. Quarterly, the weekly backups from the interim storage are moved to and stored in secure container at the hot site storage facility. Records are periodically moved from the hot site for the long term archival at the National Archives and Records Administration (NARA). The backups will be archived at NARA for a period of at least ten years, six months.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site and approved by the FPKI OA and FPKIPA. The interim site is located at:

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

The hot site is located at:

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

Prior to the end of the archive retention period, the FPKIA will provide the archived data and the applications necessary to read the archives to the FPKIPA.

4.6.3 Protection of Archive

Long-term protection of the archive is provided as described in the FPKIA SOP SA13. The archive media is stored in a safe at interim and the hot site facilities, which are temperature controlled and behind locked doors, as described in section 5.1.

Archive data is clearly labeled as follows:

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

The interim and the hot site facilities are temperature controlled and behind locked doors.

The FBCA Auditor maintains a list of individuals who can access and delete the on-line archive files at the primary site. Deletion of on-line archive files is accomplished under multi-person control procedures.

The contents of the archive will not be released except as determined by the FPKIPA or as required by law.

4.6.4 Archive Backup Procedures

Archive records are backed-up as part of the nightly normal system backup procedure to single session, 4mm digital tapes.

Incremental backups are performed nightly. Full system backups are performed to daily to digital tape removable storage media.

4.6.5 Requirements for Time-Stamping of Records

Records will be clearly labeled with date/time period information of the data contained in the record as described in section 4.6.3. System logs are automatically time stamped and systems use the NIST time server to maintain synchronize time via Network Time Protocol (NTP).

4.6.6 Archive Collection System (Internal or External)

The archive information will be collected by the FPKI OA Auditor, who will be responsible for archival.

4.6.7 Procedures to Obtain and Verify Archive Information

Creation of archive data is described in section 4.6.1. The archive data is placed in clearly labeled, double wrapped packaging for transport to short-term and long-term archive locations. Transport of archive data is via hand carry for short-term archive by the FPKIA Auditor or approved courier services. Storage and protection of archive data is described in section 5.

The FPKI OA auditing official will maintain logging information (and receipts) as archived data is transported to short-term and long-term archive facilities.

4.7 KEY CHANGEOVER

The FCPF CA key changeover procedures are as follows:

- The FCPF CA will generate a self-issued certificate signed by the old private key whose subjectPublicKeyInfo field contains the new public key.
- The FCPF CA will generate a self-issued certificate signed by the new private key whose subjectPublicKeyInfo field contains the old public key.
- The FCPF CA will generate a self-issued certificate signed by the new private key whose subjectPublicKeyInfo field contains the new public key.
- The FCPF CA and all shared service providers CAs will process new CA certificates as described in this CPS.
- All certificates generated as part of the key changeover process will be posted to the FPKIA repository.

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

The FCPF CA will support shared service provider CA key changeovers by issuing and posting new certificates as required.

Once the key rollover is completed only the new key will be used to sign certificates. The old private key is retained and protected in order to sign CRLs that contain certificates signed by that key.

4.8 COMPROMISE AND DISASTER RECOVERY

The FCPF CA and directory system is deployed so as to provide 24-hour, 365-day availability. The FCPF CA implements features to provide high levels of reliability as described in the following subsections.

The FCPF CA has recovery procedures in place to reconstitute the FCPF CA within 72 hours in the event of a catastrophic failure, as described in the following subsections.

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

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 FPKI OA 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 FPKI OA Management team.

5. If the severity/scenario (to exceed 6 hours) of the event is critical, activation of the alternate site (hot site).

6. The FPKIA POCs (“hot list”) will be notified of this change, so that any changes required by the shared service provider CAs can be performed

7. Manage the recovery process of the primary FPKIA facility.

8. Submit post recovery logs to FPKIPA

In order to provide for rapid FCPF CA service re-activation, the FPKI OA implements a synchronized hot site. The hot site includes an identical configuration of the primary site. The FPKIA hot site online directory is updated by a running script that pulls the information from the primary site on a regular basis. The hot site offline FCPF CA will be quickly restored via backup tapes.

Certificates may need to be validated and new public keys/certificates issued in the event anomalies exist.

The following reports are generated:

1. Activity log – this log is maintained throughout the disaster recovery process.

2. Test plan results

3. Equipment list – Update configuration management

4. Restoration Expense report

The PA will be notified as soon as possible as described in DR01 and DR02.

In the event the FCPF CA equipment is damaged or rendered inoperative, but the FCPF CA signature keys are not destroyed, FCPF CA operation will be reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

4.8.2 CA Cannot Generate CRLs

If the FCPF CA cannot issue a CRL within 72 hours after the time specified in the next update field of its currently valid CRL, the FPKI OA will immediately inform the FPKIPA, as well as the shared service providers where appropriate.

4.8.3 CA Signature Keys are Compromised

If the FCPF CA signature keys are compromised or lost (such that compromise is possible even though not certain) the following procedure (see FPKIA disaster recovery plan) is executed:

1. The FPKIPA and all its members to include Shared Service Providers (SSP) (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;

2. The FCPF CA will generate a new FCPF CA key pair in accordance with procedures set forth in section 4.2

3. New FCPF CA certificates will be issued to shared service provider CAs also in accordance with section 4.2.

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

4.8.4 Secure Facility Impaired after a Natural or Other Type of Disaster

In the case of a disaster whereby the FCPF CA primary installation is physically damaged and all copies of the FCPF CA signature key are destroyed as a result, the FPKIPA and all of its subordinates will be securely notified (via callback and challenge-response), and the procedures described in section 4.8.1 will be followed. The FCPF CA installation will then be completely rebuilt, by reestablishing the FCPF CA equipment, generating new private and public keys, being

re-certified, and re-issuing all subordinate shared service provider certificates. The details of this plan are defined in the FPKI OA BCCP and Disaster Recovery Procedures.

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

4.9 CA TERMINATION

In the event of termination of the FCPF CA operation, certificates signed by the FCPF CA will be revoked. The FPKI OA will advise, using secure communication (callback and challenge-response described in SA09) all the shared service providers, to which the FCPF CA has issued subordinate certificates, of its termination. All documentation and data will be archived using the NARA Storage procedures (SA13).

The FPKI OA Team will coordinate scheduled termination with Shared Service Providers when authorized by the FPKIPA.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.1 Site Location and Construction

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.2 Physical Access

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.3 Electrical Power

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.4 Water Exposures

The FPKIA room implements water protection safeguards equivalent to those implemented for the GSA FTS computer room. At the Primary facility, water pipes are not filled until an actual fire is detected. There is no water suppression system at the Hot Site.

5.1.5 Fire Prevention and Protection

The FPKIA room implements fire prevention and protection safeguards equivalent to those implemented for the GSA FTS computer room. Additionally, both primary site and hot site rooms are equipped with ceiling sprinklers. See section 5.1.6 for more details.

5.1.6 Media Storage

The FPKIA room also includes a small safe, fireproof locked cabinets, and desk where media are stored so as to protect them from accidental damage (water, fire, electromagnetic). Media that contain audit, archive, or backup information are stored at a different location separate from the FPKIA (i.e. in an off-site interim Storage Facility) and after three months they are transported to

long-term site specified in section 4.6.2. Additionally the safes in both primary site and hot site are fire retardant and shield from electromagnetic emissions.

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. See FPKIA procedure SA10 for more details.

5.1.8 Offsite Backup

For the FPKIA full system backups, sufficient to recover from total system failure, are conducted on a periodic schedule, described in section 4.5. The short-term backup site specified in section 4.6.3 and contains up to three months worth of backup information. The long-term backup site is specified in section 4.6.2.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The functions performed in these roles and the people selected to fill them form the basis of trust for the entire Federal PKI Architecture. 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 FPKIA encompasses CA products from several vendors implementing different certificate policies. Different commercial products support somewhat different roles, and use different mechanisms for registering or enrolling subscribers and issuing certificates; however, they can all be re-conducted to the following somewhat abstract roles, derived from roles identified in the CIMC Protection Profile developed by NIST—

5. *Administrator* – authorized to install, configure, and maintain the Operating Systems and Directory Software; establish and maintain Operating System user accounts; configure Operating System profiles and audit parameters; and generate component keys.

6. *Security Officer* – authorized to request or approve certificates or certificate revocations; authorized to install, configure and maintain the CA software; establish and maintain CA user accounts; and configure CA software profiles and audit parameters.

7. *Auditor* – authorized to view and maintain audit logs.

8. *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, and;
- Assisting in Generating and Backing up FCPF CA keys.

Administrators do not issue certificates to subscribers.

5.2.1.2 Security Officer

The security officer role is responsible for issuing certificates, including—

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates;
- Requesting, approving and executing the revocation of certificates.
- Configuring certificate profiles or templates and audit parameters for the CA software.
- Generating and backing up CA keys

5.2.1.3 Auditor

The auditor role is responsible for—

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with this CPS;

5.2.1.4 Operator

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

5.2.2 Separation of Roles

Role separation, when required as set forth below, is enforced either by the FCPF CA equipment, or procedurally, or by both means.

The separation of roles for the FCPF CA, which is operated at the FBCA high assurance level, is as follows—

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

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

Once the FCPF CA is activated, access to the FCPF CA private signing key for issuance and revocation of certificates requires a minimum of 2 FPKI OA Personnel (Security Officer and Administrator), at least one authenticated via individual smartcards.

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

To best ensure the integrity of the FPKIA 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 FPKIA operation.

Under no circumstances does any FPKIA 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 role or identity.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

The FPKIPA and the FPKI OA are responsible and accountable for the operation of the FPKIA.

All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and are U.S. citizens. The procedures governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the FPKIA are described in the FPKIA SSP. Appendix A of this CPS includes selected excerpts from that portion of the FPKIA SSP.

All FPKIA personnel hold TOP SECRET security clearances.

5.3.2 Background Check Procedures

FPKI OA personnel background checks are performed in accordance with TOP SECRET security clearance requirements and demonstrate compliance with requirements set forth in section 5.3.1 of the FCPF.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the FPKIA receive comprehensive training. One-on-one training is conducted in the following areas by certified product engineers—

- CA (or RA) security principles and mechanisms
- All PKI software versions in use on the CA (or RA) system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Stipulations of the FCPF.

Training in the overall security procedures of the FPKIA is conducted for all personnel at the initial full operation capability of the FPKIA. 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.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles are made aware of changes in the FPKIA operation as described personnel training procedures documentation. Any significant changes to the operations are documented and personnel are informed and made aware of changes in accordance with the personnel training procedures. All FPKI OA personnel will participate in mandatory refresher training annually to ensure all affected personnel are aware of new changes to procedures and configuration changes. In addition, immediate On-the-Job-Training (OJT) is conducted when any changes occur within the FBCA operations. Examples of such changes are FPKIA software or hardware upgrades, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

The FBCA CP does not stipulate requirements for this section.

5.3.6 Sanctions For Unauthorized Actions

The FPKIA takes appropriate administrative and disciplinary actions against personnel who have performed unauthorized actions involving the FCPF CA or its repository. In the event of an unauthorized action, the ISSO will immediately investigate the incident. After the investigation, the ISSO and ISSM will determine if the action warrants disciplinary actions based on severity and the reoccurrence of the indiscretion. If the action is of significant indiscretion, it will be reported to the FPKI Program Manager 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 as to prevent further indiscretions.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to the FCPF CA meet applicable requirements set forth in the FCPF and this CPS as determined by the FPKI OA.

5.3.8 Documentation Supplied to Personnel

The FCPF CA makes available to all of its personnel the FCPF, this CPS, and any relevant statutes, policies or contracts. Documentation identifying all personnel receiving and completing training is maintained by the FPKI OA. Standard Operating Procedures are also provided to each FPKI OA team member as it relates to his/her responsibility. These procedures are located in training manual for each specified role.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The key pair for the FPKIA CAs are generated on the Chrysalis LunaSA cryptographic module. The key pair generation is RSA for digital signature in compliance with PKCS-1 (FIPS 140-2, level 3). The private key will never be exposed outside the module in unencrypted form. Backup copies of the LunaSA private keys will be created. Multiparty controls are described in the key generation ceremony procedure.

FPKIA private keys are generated using the FPKIA key signing Ceremony procedures. These procedures document the role separation and provide an auditable trail. These procedures are

completed with a third party auditor present, where 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

Subscriber (shared service provider) key pair generation is performed by the subscriber, using a FIPS approved method.

6.1.2 Private Key Delivery to Subscriber

The shared service provider CA generates its own key pair and therefore does not need private key delivery.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered to the FCPF CA electronically in a certificate request (i.e., using PKCS #10) messages to the FPKI OA via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier) as described in section 4.2. Identity checking and proof of possession of the private key will be accomplished as described in section 4.1.

6.1.4 CA Public Key Delivery to Relying Parties

The FCPF trusted certificate will be transported in a secure, out-of-band mechanism via e-mail or floppy disk delivered by registered mail or courier to the relying parties.

6.1.5 Key Sizes and Signature Algorithms

Trusted certificate public/private key sizes are 2048 bits for RSA, SHA-1, in accordance with FIPS 186. CA certificates issued to shared service providers and CRLs use a 1024 or 2048 (based on the Shared Service Providers private key) public key size for RSA and use SHA-1.

FCPF CA currently does not utilize TLS.

6.1.6 Public Key Parameters Generation

There are no public key parameters for RSA.

6.1.7 Parameter Quality Checking

There are no public key parameters for RSA.

6.1.8 Hardware/Software Subscriber key generation

The FCPF CA key pairs are generated in a FIPS 140-2 Level 3 validated, LunaSA hardware cryptographic module.

Key pairs for trusted roles and provision of multi-person controls are generated in a FIPS 140-1 Level 2 validated DataKey SmartCard cryptographic modules.

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

The FCPF CA issues only CA certificates to shared service provider subordinate CAs and cross-certificates to the FBCA. Such certificates assert both the *keyCertSign* and *cRLSign* bits. The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits are not asserted in certificates issued under the FCPF.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

The FCPF CA private keys are protected using FIPS 140-2 Level 3 validated cryptographic module: Chrysalis LunaSA hardware token.

Key pairs for FPKIA separation of roles are generated in FIPS 140-1 Level 2 validated cryptographic modules: DataKey SmartCards.

All cryptographic modules are operated such that the private asymmetric cryptographic keys are never output in plaintext.

See section 5.2.2 for a description of the procedures used for accessing and operating the FCPF CA.

6.2.2 Private Key Multiperson Control

All FCPF CA private keys, their backups (including during the backup procedure) are under 2 out of N control, where N≥2. N represents the total number of Security Officers. See the following sections for details on how this is achieved.

6.2.3 Private Key Escrow

The FCPF CA signature keys used to support non-repudiation services are not escrowed by a third-party

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.2.4.2 Backup of Subscriber Private Keys

No Stipulation.

6.2.5 Private Key Archival

FCPF CA private signature keys are not archived.

6.2.6 Private Key Entry Into Cryptographic Module

FCPF CA private keys are generated by and remain in a cryptographic module. The Chrysalis product uses proprietary secure means for transferring keys from one cryptographic module to another to back up the CA keys.

6.2.7 Method of Activating Private Keys

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.2.8 Methods of Deactivating Private Keys

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.2.9 Method of Destroying Subscriber Private Keys

The FCPF CA does not maintain subscriber private keys.

6.3 GOOD PRACTICES REGARDING KEY-PAIR MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Usage Periods for the Public and Private Keys

The FCPF CA private signing keys will be used to sign certificates for one-half of the certificate lifetime (e.g. for 2 years if the certificate lifetime is 4 years). The certificate lifetime will be valid not more than 6 years. Rekeying will be performed after 3 years.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.4.2 Activation Data Protection

Activation data is memorized, not written down. If written down, it is secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

Activation data will never be shared.

For FCPF CA administrators, the Microsoft CA is configured to 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 at least every 90 days to decrease the likelihood of discovery.

6.5 COMPUTER SECURITY CONTROLS

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

The FPKIA repository is operated on a dedicated workstation and will only run the network services required to operate the repository and to support on-line certificate validations (i.e., LDAP, DSP).

The FCPF CA server uses configurations that have been clearly demonstrated and passed the Compliance Audit process as described in section 2.7.

The FCPF CA equipment is configured with appropriate security features turned on as recommended by the host operating system vendor in accordance with any associated security validation rating. The FCPF CA has the following security features and functions:

- Require authenticated logins via FIPS PUB 140-2 Level 3 and FIPS PUB 140-1 Level 2 cryptographic modules
- 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 FCPF CA services and FPKIA roles as described in sections 5.1.2 and 5.2.2
- Enforce separation of duties for FPKIA roles as described in sections 5.1.2 and 5.2.2
- Require identification and authentication of FPKIA roles and associated identities as described in sections 5.1.2 and 5.2.2
- Prohibit object re-use or require separation for FCPF CA random access memory. It is assumed that verification of meeting this requirement is provided by the Windows 2003 server operating system. Windows 2003 enforces the required prohibition/separation. Windows 2003 was evaluated under IT SEC E3/FC2, since the FC2 functional package is equivalent to the Orange Book's C2, it includes the required memory protection controls.
- Require use of cryptography for session communication and database security. The use of cryptography for session communication is not required because the certificate request messages (PKCS#10) are exchanged using an out-of-band mechanism and are imported manually directly at the CA. The CA database is protected via triple-DES cryptography.
- Archive FCPF CA history and audit data through data collection and archive procedures described in sections 4.5 and 4.6
- Require self-test security related FCPF CA 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.
- Require a trusted path for identification of FPKIA roles and associated identities logins via FIPS PUB 140-2, Level 3 and 140-1 Level 2 cryptographic modules. Requires a recovery mechanisms for keys and the FPKIA system through backup and protection procedures described in 4.5.5
- Enforce domain integrity boundaries for security critical processes through self-test procedures described above

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The System Development Controls for the FCPF CA are as follows:

- The FCPF CA software is commercial- off-the-shelf software that has been developed under a very formal development process that is well documented.
- Hardware procured to operate the FCPF CA has been purchased in a fashion whereby the provider does not know that it is intended for the FCPF CA operations. The CA software has been ordered and installed by certified engineers under the direction and control of authorized FPKIA 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 FCPF CA server will be purchased using commercial buys. Hardware and non-CA software is purchased randomly, through standard procurement procedures provided by the FPKI OA. An accountable method of packaging and delivery will be used to provide a continuous chain of accountability from the vendor to the facility (e.g., UPS, Federal Express, USPS Express Mail). The FPKIA establishes a relationship with the CA software vendors prior to acquisition that gives assurance that the software has not been tampered with. Installation is performed under multi-person control with only authorized FPKIA operation personnel.
- Proper care is taken to prevent malicious software from being loaded onto the FCPF CA equipment. From the time the software is received, it remains under continuous control. All shrink wrapped packaging is opened and installed inside the secure FPKIA facility under multi-person control. McAfee AntiVirus will be 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 at startup, periodically, and any time a system configuration change occurs (i.e., adding a new CA to the FPKIA).
- The CA hardware and software is dedicated to performing one task: the FCPF CA. Other software installed on the CA machine is used to facilitate proper operation of the CA. Only one CA can be installed on the machine at one time.

6.6.2 Security Management Controls

The initial configuration of the FCPF CA software (i.e., CA software, repository software) as well as any modifications and upgrades will be documented and controlled in accordance with FPKIA Configuration Management Procedures (separate FPKI OA document). System and application level logging will be 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 above.

6.6.3 Life-Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

The description of the practice for cryptographic modules is stated above in Section 6.2

7. CERTIFICATE AND CARL/CRL PROFILES

7.1 CERTIFICATE PROFILE

Certificates issued by the FCPF CA conform to the X.509 Certificate and CRL Extensions Profile for the Common Policy [CCP-PROF].

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

Certificates issued by the FCPF CA conform to the X.509 Certificate and CRL Extensions Profile for the Common Policy [CCP-PROF].

7.1.3 Algorithm Object Identifiers

Certificates issued by the FCPF CA will use the following OIDs for signatures:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

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

Certificates issued by the FCPF CA 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 3280.

7.1.5 Name Constraints

Certificates by the FCPF CA will not contain name constraints.

7.1.6 Certificate Policies Extension

Certificates issued by the FCPF CA will assert one of more of the following OIDs in the certificate policies extension, as appropriate:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

7.1.7 Usage of Policy Constraints Extension

The FCPF CA will assert policy constraints in CA certificates only when the FPKIPA directs the FPKI OA to inhibit policy mapping.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates by the FCPF CA will not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Certificates issued by the FCPF CA will not contain a critical certificate policy extension.

7.2 CRL PROFILE

CRLs by the FCPF CA will conform to the CRL Profile specified in [CCP-PROF].

7.2.1 Version Numbers

The FCPF CA will issue X.509 Version 2 CRLs.

7.2.2 CARL and CRL Entry Extensions

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

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

Errors, updates, or suggested changes to this document will be communicated to the contact in section 1.4. Such communication will include a description of the change, justification for the change, contact information for the person requesting the change, and an impact assessment.

Changes to this document will be reviewed and approved by the FPKIPA, will be communicated to every shared service provider CA, and will be posted at the website specified in section 2.6.4.

Errors, updates, or suggested changes to this CPS are notified to all shared service provider CAs. All versions of this document will be reviewed and approved by the FPKIPA.

Revised versions of this document will be disseminated to interested parties (see section 8.2)

8.2 PUBLICATION AND NOTIFICATION POLICIES

The FPKIPA will publish information (including the redacted version of this CPS) on the following web sites: http://www.cio.gov/fpkipa.

The redacted version of this CPS will also be disseminated via email to any that request it.

Proposed changes to the CPS will be sent to shared service provider CAs.

The FPKIPA will provide an updated and approved document within 1 week to the FPKIPA web administrator, who has agreed to post this information.

The redacted version of this CPS and any subsequent changes shall be made publicly available within 1week of approval.

8.3 CPS APPROVAL PROCEDURES

The FPKIPA will make the determination that this CPS complies with FCPF CP. The FPKIPA will also determine if a change to this CPS is acceptable and that the changed CPS continues to comply with the FCPF CP.

8.4 WAIVERS

There will be no waivers to the CPS – any changes will be effected through approval of a revised CPS.

9. BIBLIOGRAPHY

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

ABADSG	Digital Signature Guidelines, 1996-08-01 http://www.abanet.org/scitech/ec/isc/dsgfree.html
FIPS 112	Password Usage, 1985-05-30 http://csrc.nist.gov/fips/
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
FOIACT	5 U.S.C. 552, Freedom of Information Act Http://www4.law.cornell.edu/uscode/5/552.html
CCP-Prof	X.509 Certificate and CRL Extensions Profile for the Common Policy, December 8, 2003. .
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 2000.
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996 Http://www4.law.cornell.edu/uscode/40/1452.html
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 July 1990 Http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999
PKCS#12	Personal Information Exchange Syntax Standard, April 1997 Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html

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

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

RFC 3280 Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Housley et al., April 2002.

USGold GOVERNMENTWIDE DIRECTORY SUPPORT 2

TECHNICAL SERIES: The Updated USGold Schema, July 14, 1997.

Note: add [E-Auth] when issued by OMB.

10. ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSS	Digital Signature Standard
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FIPS	(U.S.) Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
CCP-Prof	X.509 Certificate and CRL Extensions Profile for the Common Policy
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
MOA	Memorandum of Agreement (as used in the context of this CP, between an Agency and the FPKIPA allowing interoperation between two separate organizational CAs)

NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OID	Object Identifier
PA	Federal PKI Policy Authority
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
U.S.C.	United States Code
WWW	World Wide Web

11. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to IS resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Applicant	The subscriber is sometimes also called an “applicant” after applying to a CA for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls; to ensure compliance with established policies and operational procedures; and to recommend necessary changes in controls, policies, or procedures. [NS4009]

Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009audit trail]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical characteristic of a human being, including a photograph for visual identification. For the purposes of this document, biometrics do not include handwritten signatures.
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.

Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.
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 Authority	A trusted entity that provides online verification to a relying party of a subject certificate's trustworthiness and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Component Private Key	Private key associated with a function of the certificate-issuing equipment, as opposed to being associated with an operator or administrator.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by NIST.
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, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate and (2) whether the message has been altered since the transformation was made.
Discretionary Access Control	Means of restricting access to objects based on user identity.
Duration	A field within a certificate that is composed of two subfields: "date of issue" and "date of next issue."
E-Commerce	The use of network technology (especially the Internet) to buy or sell goods and services.
Employee	Any person employed by an Agency as defined above.

Encrypted Network	A network that is protected from outside access by NSA-approved high-grade (Type I) cryptography. Examples are Secure Internet Protocol Routing Network (SIPRNET) and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions or to establish or exchange a session key for these same purposes.
End Entity	Relying parties and subscribers.
Federal PKI Architecture (FPKIA)	The FPKIA 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]
Inside Threat	An entity with authorized access that has the potential to harm an IS through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge, or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [Adapted from ABADSG, "Commercial key escrow service"].
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key and (2) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	An RA with responsibility for a local community.
Memorandum of Agreement (MOA)	An agreement between an organization and the FPKIPA allowing interoperation between two separate organizational CAs.

Mission Support Information	Information that is important to the support of deployed and contingency forces.
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.
National Security System	Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Nonrepudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009]. Technical nonrepudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal nonrepudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization; the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI OIDs are used to uniquely identify each of the four policies and cryptographic algorithms supported.

Out-of-Band	Communication between parties using a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an IS through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI 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 CP.
Privacy	Restricting access to subscriber or relying party information in accordance with Federal law and Agency policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair used to encrypt confidential information. In both cases, this key is made publicly available, normally in the form of a digital certificate.

Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects but does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.

Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (a.k.a. trust anchor, i.e., the beginning of trust paths) for a security domain.
Secret Key	A "shared secret" used in symmetric cryptography, wherein users are authenticated based on a password, PIN, or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subscriber	A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device.

System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an IS. [NS4009]
Technical Nonrepudiation	The contribution of public key mechanisms to the provision of technical evidence supporting a nonrepudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by relying parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Agency in confirming subscriber identification during the registration process. Trusted Agents do not have automated interfaces with CAs.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor."
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

Trustworthy System	Computer hardware, software and procedures that (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 1401]

Part 3: X.509 Certification Practice Statement (CPS) For the E-Governance Certification Authority

United States Federal PKI Architecture

Federal PKI Architecture X.509 Certification Practice Statement – Part 3: X.509 Certification Practice Statement For the E-Governance Certification Authorities

13 September 2005

Table of Contents

1. EGCA CPS INTRODUCTION

This Certification Practice Statement (CPS) for the EGCA is part three (3) of the FPKIA CPS and it documents the internal practices and procedures used by the Federal Public Key Infrastructure Architecture Operational Authority (FPKI OA) by describing the practices concerning lifecycle services in addition to issuance, such as certificate management (including publication and archiving), revocation, and renewal or re-keying.

This CPS covers the operation of systems and the management of facilities, which include three EGCAs and the Federal PKI Architecture common repository functionality, used to post TLS certificates and CRLs to credential service providers that have been recognized as meeting E-Authentication assurance requirements at Level 1 or 2, as defined in *E-Authentication Guidance for Federal Agencies* [M-04-04], and to agency application servers participating in the E-Authentication program.

EGCAs provide certificates to agency application servers and credential service providers for conducting assertion based authentication transactions.

This CPS implements all the X.509 Certificate Policy for the E-Governance Certification Authorities (EGCP) certificate policies, namely to:

- identify a Level 1 CSP (as a network device) named in the certificate and binds that CSP to a particular public/private key pair,
- identify a Level 2 CSP (as a network device) named in the certificate and binds that CSP to a particular public/private key pair, or
- identify a federal agency server (a network device) supporting one or more E-Authentication applications, and binds that server to a particular public/private key pair.

This CPS implements and complies with the requirements established in the EGCP dated 23 July 2004

This CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework.

1.1 OVERVIEW

1.1.1 Certification Practice Statement

This Certification Practice Statement (CPS) documents the internal practices and procedures used by the Federal PKI Operational Authority (OA). It covers the operation of systems and the

management of facilities, which include EGCAs and the Federal PKI Architecture common repository functionality, used to post TLS certificates and CRLs concerning approved Credential Service Providers (CPs) and agency applications that are conducting federated e-Authentication transactions. Certificates issued under this policy contain a registered certificate policy object identifier (OID), which may be used by a relying party to decide whether a certificate is trusted for a particular purpose.

1.1.2 Relationship Between the CP and the CPS

The EGCP states what assurance can be placed in certificates issued by the EGCAs. This CPS states how the EGCAs establish that assurance. The EGCP states that each CA that issues certificates under the EGCP must have a corresponding CPS, however, since the FPKI OA will establish such CAs as three separate instantiations of the CA application on the same CA server, there will be only one CPS, this document, describing the operation of the E-governance CAs. Should it become necessary to distribute the EGCAs onto separate servers, this CPS will be broken into separate CPS documents each addressing the corresponding policy separately.

1.1.3 Scope

This CPS documents the internal practices and procedures used by the Federal PKI Architecture (FPKIA) Operational Authority (OA). It covers the operation of systems and the management of facilities, which includes the EGCAs and the FPKIA repository functionality, used to issue TLS E-Authentication level 1 and 2 certificates to Credential Service Providers (CSPs) and agency application servers.

1.2 IDENTIFICATION

The EGCP provides substantial assurance concerning identity of certificate subjects. The EGCA issues certificates in accordance with the EGCP asserting at least one (excluding the CA certificates) one of the following OIDs in the certificate policy extension:

id-eGov-Level1 ::= {2 16 840 1 101 3 2 1 3 9}

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}

The EGCAs issues certificates to CSPs under the EGCP that contain either the id-eGov-Level1 OID or the id-eGov-Level2 OID.

The EGCAs issues certificates to agency application servers under the EGCP that contain the id-eGov-Applications OID.

1.3 COMMUNITY AND APPLICABILITY

Certificates issued by the EGCAs under the EGCP are solely to support distribution of authentication information to FPKI OA security officers, the credential service provider servers (CSPs), and the federal application servers (AAs). Use of these certificates for other purposes, while not prohibited, is outside the scope of the EGCP and this CPS.

1.3.1 PKI Authorities

The following table summarizes the roles relevant to the administration and operation of the FBCA. These roles are entirely defined in the EGCP.

Table 1.3.1-1 EGCP Roles

EGCP Role	***Description***
Federal PKI Policy Authority (FPKIPA)	The Federal PKI Policy Authority (PA) 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 PA is responsible for maintaining the EGCP, approving the CPS for each CA that issues certificates under this policy, approving the compliance audit report for each CA issuing certificates under this policy, and is a key component of the E-Authentication Technical Architecture. The PA is also responsible for identifying one or more E-Authentication Authorizing Officials (see 2.1.4).
E-Authentication Authorizing Official	The E-Authentication Authorizing Official (EAO) is responsible for the decision to issue a certificate to a particular CSP or a federal agency application server.
Certification Authority	The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. The CA is responsible for the issuing and managing certificates including— The certificate manufacturing process Publication of certificates Revocation of certificates Generation and destruction of CA signing keys

EGCP Role	*Description*
	Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.
Registration Authority	The registration authority (RA) is the entity that collects and verifies each subscriber's identity and information that are to be entered into the subscriber's public key certificate. The RA performs its function in accordance with a CPS approved by the PA. The RA is responsible for— Control over the registration process The identification and authentication process RA duties are performed by the E-Authentication Authorizing Officials and may also be performed as an additional duty by CA personnel.
FPKI Operational Authority (FPKI OA)	The FPKI Operational Authority (OA) is the organization that operates the EGCA, including issuing E-Governance certificates when directed by the FPKIPA/EAO, posting those certificates and Certification Authority Revocation Lists (CARLs) into the FPKIA repository, and ensuring the continued availability of the repository to all users. The FPKI OA executes the role of CA as well as some RA functions for the EGCAs, as delegated by the EAO.
FPKI OA Administrator	The Administrator is the individual within the FPKI OA who has principal responsibility for overseeing the proper operation of the EGCA including the FPKIA repository.
FPKI OA Security Officers	These Security Officers are the individuals within the FPKI OA, selected by the ISSO who operate the FBCA and its repository including executing FPKIPA/EAO direction to issue EGCA certificates to CSPs or AAs. The roles include FPKI OA Security Officer, Auditor, and Operator, all described in this CPS, section 5.2.1.
Related Authorities	The CAs and RAs operating under the EGCP may require the services of other security, community, and application authorities, such as compliance auditors, information system security officer (ISSO), information system security manager (ISSM), and attribute authorities. This CPS will identify the parties responsible for providing such services, and the

EGCP Role	*Description*
	mechanisms used to support these services.
End Entities	Subscribers A subscriber is the entity whose name appears as the subject in a certificate. For this policy, subscribers are limited to credential service provider (CSPs) and agency application servers (AAs). CSPs provide SAML assertions to agency application servers. Subscribers will use these certificates to establish mutually authenticated TLS connections to provide authentication, integrity, and confidentiality to the transmission of these SAML assertions. 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 or agency application server.

1.3.2 Applicability

The EGCAs only issue certificates to end-entity subscribers as defined in section 1.3.1 and issues CRLs relating to those certificates; the EGCA does not cross-certify with FBCA.

1.4 CONTACT DETAILS

1.4.1 Specification Administration Organization

The FPKI OA, FPKIPA, and the EAO are responsible for all aspects of this CPS. The FPKIPA is responsible for all aspects of EGCP.

1.4.2 Contact Person

Questions regarding this CPS shall be directed to the Chair of the Federal PKI Policy Authority or the EAO, whose address can be found at http://www.cio.gov/fpkipa and http://www.cio.gov/eautihentication, respectively.

1.4.3 Person Determining CPS Suitability for the Policy

The FPKIPA approves the CPS for each EGCA that issues certificates under the EGCP. Refer to Section 8.3, CPS Approval Procedures.

2. GENERAL PROVISIONS

2.1 OBLIGATIONS

2.1.1 PA Obligations

The EGCP establishes the obligations of the FPKIPA as to—

- Approve the CPS for each EGCA that issues certificates under this policy;
- Review periodic compliance audits to ensure that EGCAs are operating in compliance with their approved CPSes;
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under the EGCP;
- Revise the EGCP to maintain operational practicality and consistency with the Medium level of assurance at the FBCA;
- Publicly distribute the EGCP; and
- Coordinate modifications to the EGCP to ensure continued compliance by CAs operating under approved CPSes.

2.1.2 CA Obligations

The EGCP stipulates the obligations of a CA who issues certificates that assert a EGCP policy shall conform to the stipulations of this document, including—

- Providing the FPKIPA and the EAO with a CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Ensuring that registration information is accepted only from approved RAs.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with Section 2.1.5.
- Operating or providing for the services of an online repository that satisfies the obligations under Section 2.1.7, and informing the repository service provider of their obligations if applicable.

2.1.3 RA Obligations

The FPKI OA is the RA for the EGCA and is responsible for controlling the registration process, and conforms to the stipulations of the EGCP, including—

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
- Ensuring that obligations are imposed on subscribers in accordance with Section 2.1.5, and that subscribers are informed of the consequences of not complying with those obligations.

2.1.4 E-Authentication Authorizing Official Obligations

The EGCP defines the obligations for the E-Authentication Authorizing Official (EAO) as to—

- Authorize issuance of certificates to CSPs and determine the appropriate E-Authentication Level for that certificate.
- Authorize issuance of certificates to Federal Agency application servers.

2.1.5 Subscriber Obligations

The only potential EGCAs subscribers identified are the EGCA OA Administrator and the EGCA OA Security Officers, the credential service provider servers (CSPs), and the federal agency application servers (AAs). The EGCAs do not issue certificates to any other end-entity subscriber, rather merely issue TLS certificates to subordinate CSPs and AAs.

The EGCP defines the obligations for such subscribers as to—

- Accurately represent themselves in all communications with the PKI authorities and other subscribers.
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Notify, in a timely manner, the EGCA that issued their certificates of suspicion that their private keys are compromised or lost. Such notification shall be made directly or indirectly through mechanisms consistent with the EGCA CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.

2.1.6 Relying Party Obligations

The relying party decides, pursuant to its own policies, what steps to take. The EGCAs merely provide the tools (i.e., certificates and CRLs) needed to perform the validation of certificates that the relying party may wish to employ in its determination.

2.1.7 Repository Obligations

The EGCAs post all certificates and all CRLs in the FPKIA directory that is publicly accessible through the Lightweight Directory Access Protocol (fpkia.gsa.gov port 389). To promote consistent access to certificates and CRLs, the FPKIA repository implements access controls to prevent modification or deletion of information.

ACLs are set to allow read-only LDAP access to the public (anonymous bind) via the Internet and read-only DSP access to cross-certified entities. The Offline directory ACLs are configured to only allow administrative and update access permissions to authenticated users.

2.2 LIABILITY

The EGCP states that 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.

2.3 FINANCIAL RESPONSIBILITY

This EGCP contains no limits on the use of certificates issued by CAs under its policy. Rather, entities, acting as Relying Parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

2.3.1 Indemnification by Relying Parties and Subscribers

The EGCP does not stipulate requirements for this section.

2.3.2 Fiduciary Relationships

The EGCP does not stipulate requirements for this section.

2.4 INTERPRETATION AND ENFORCEMENT

The terms and provisions of the E-Governance Certificate Policy will be interpreted under and governed by applicable Federal law.

2.4.1 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of the EGCP, hence the corresponding section in this CPS, is incorrect or invalid, the other sections of this CPS shall remain in effect until the EGCP is updated. The process for updating the EGCP, and the corresponding EGCAs CPS, is described Section 8.1 in the EGCP and this CPS, respectively.

2.4.2 Dispute Resolution Procedures

The U.S. Government will facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy.

2.5 FEES

The EGCP does not stipulate requirements for this section. The FPKI OA will determine the fees, if any, for EGCAs services, as approved by the FPKIPA and/or the EAO.

2.6 PUBLICATION AND REPOSTORY

2.6.1 Publication of CA Information

The FPKI OA will deliver this CPS to the FPKIPA and any relevant authority in the Federal government. It will make a redacted version of this CPS publicly available on the FPKIPA web site described in section 2.6.4.

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" (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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

The FPKI OA will publish information concerning the EGCA necessary to support its use and operation, including:

- The certificates it issues to CSPs and AAs;
- The CRLs it issues;
- The Certificate for its certificate signing key;
- The redacted CPS; and

- The EGCP, and any waivers granted by the FPKIPA and/or EAO.

Certificates issued to CSPs and AAs and CRLs are published as specified in Section 2.1.7. The FPKI OA will deliver this CPS to the FPKIPA, EAO, and any relevant authorized authority in the Federal government with need to know. The EGCP does not stipulate requirements regarding publication of additional CA information.

2.6.2 Frequency of Publication

Certificates are published following subscriber acceptance as specified in Section 4.3 and proof of possession of private key as specified in Section 3.1.7. The CRL is published as specified in Section 4.4.3.1. All information to be published in the repository is published promptly after such information becomes available to the EGCAs. New CRLs are published to the offline directory every 18 hours. Additonally, CRLs are published to the online directory every 15 minutes.

2.6.3 Access Controls

The EGCAs protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository are publicly available through the Internet. Access to other information in the CA repositories will be determined by agencies pursuant to their authorizing and controlling statutes. This CPS details in section 2.8 what information in the repository is exempt from automatic availability and to whom, and under which conditions, the restricted information may be made available.

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" (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, is omitted in the publicly universally available version of this document. Upon request, this information is available to authorized organizations with a need to know.

2.6.4 Repositories

See Section 2.1.7.

2.7 COMPLIANCE AUDIT

2.7.1 Frequency of Entity Compliance Audit

The FPKI OA will arrange initially and annually for independent inspections and compliance audits to validate that the EGCAs are operating in accordance with the security practices and procedures described in this CPS. Results of the compliance audit will be provided to the FPKIPA.

2.7.2 Identity/Qualifications of Compliance Auditor

The EGCA compliance audits will be provided by an independent auditor, as agreed between the FPKIPA and FPKI OA, which has demonstrated a proven track record and thoroughly familiar with the this CPS and the EGCP.

The FPKIPA has chosen the following organization to conduct the compliance audit:

Name of the Auditor Organization: KPMG

The selected auditor will verify and validate through document reviews and demonstrations that the EGCAs comply with the EGCP and requirements that the FPKIPA imposes on the issuance and management of EGCA certificates.

2.7.3 Compliance Auditor's Relationship to Audited Party

The selected EGCAs compliance auditor is a contractor that is independent from FPKI OA and the FPKIPA. This contractor provides an unbiased, independent evaluation and is one whose primary responsibility is the performance of EDP Compliance Audits.

2.7.4 Topics Covered by Compliance Audit

The purpose of a compliance audit is to verify that the EGCAs and its recognized RAs comply with all the requirements of the current versions of the EGCP and this CPS. The compliance audit inspections encompass all aspects of the CA/RA operation. The process used by the EAO to determine if a certificate should be issued to a CSP or agency application server is out of scope for the compliance audit.

2.7.5 Actions taken as a result of deficiency

The EGCAs compliance auditor will identify and note any discrepancies then notify within 24 hours of the completion of results, the FPKI OA and FPKIPA of the compliance audit results the FPKI OA and FPKIPA of the results of the compliance audit by e-mail and/or out-of-band writing.

Once notified, the FPKIPA and FPKI OA will have 10 business days to review the results and the recommendations from the compliance audit to determine the action to be taken.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA/EAO may decide to temporarily halt operation of the EGCA(s) or RA, to revoke a certificate issued to the EGCA(s) or RA, or take other actions it deems appropriate.

The FPKIPA/EAO will develop procedures for making and implementing such determinations.

2.7.6 Communication of Results

The auditor will provide the FPKI OA and the FPKIPA with a written (signed email and/or letter) notification of results of the compliance audit of the EGCA within 24 hours of its completion. The complete results will be provided as a written report. Such 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.

In case of compliance failure, the notification will be provided within 24 hours, upon the conclusion of the compliance audit, in a written form (signed e-mail and/or out of band letter) to the FPKI OA and to the FPKIPA, and will include, the topics of failure, reason(s) for failure, and possible remedies A comprehensive report may be provided later. After 30 days, the FPKI OA will identify a list of corrective measures taken or proposed to be taken and submit to the FPKIPA.

The FPKIPA might request an additional special compliance audit to confirm the implementation and effectiveness of the remedy.

2.8 CONFIDENTIALITY

CA information not requiring protection shall be made publicly available. Public access to shared service provider information is determined by the respective organization.

The EGCA will disclose confidential information to any third party when required by this CPS, 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 (IG);
- The individual is the subscriber itself; or
- The individual has a duly signed request from the subscriber requesting the release of the information from the subscriber

Court orders and IG requests must be approved by specific shared service provider General Counsel.

2.9 INTELLECTUAL PROPERTY RIGHTS

The EGCP does not stipulate requirements for this section.

3. IDENTIFICATION AND AUTHENTICATION

A subscriber (prospective CSP or AA) registration to the EGCA (i.e. thereby implementing e-authentication for their electronic transaction with the government) is initiated by an application submitted to the EAO as the first step of a series of activities fully described in the E-Authentication Credential Assessment Framework [CAF] and the E-Authentication Methodology for the E-Governance Certificate Authorities documents available at http://www.cio.gov/eauthentication. This application is done by following a checklist and filling a form that is sent to the EAO for review, assessment, and evaluation. Among other things, the application contains how the applicant subscriber proposes demonstrate compliance with the selected e-authentication level of assurance requirements along with the required substantiating documentation.

The EAO organization will evaluate the application and will work with the applicant organization to complete the assessment. Once the assessment and evaluation phase is successfully completed and accepted the EAO will instruct the FPKI OA to create and issue the appropriate certificate to the accepted applicant subscriber (i.e., CSP or AA).

3.1 INITIAL REGISTRATION

3.1.1 Types of Names

The EGCAs generate and sign certificates where the issuer DN consists of a set of the following X.520 naming elements: C; O; OU; and CN. Certificates may additionally assert an alternate name form subject to requirements set forth below which are intended to ensure name uniqueness.

The EGCA generate and sign certificates where the subject DN contains X.520 naming elements (at least C, O, and OU), the domain component naming element (dc), or a combination of the two.

The names assigned to E-Governance CAs are:

- c=us, o=U.S. Government, ou=FBCA, cn=eGovCSP1
- c=us, o=U.S. Government, ou=FBCA, cn=eGovCSP2
- c=us, o=U.S. Government, ou=FBCA, cn=eGovApp

As established by the EGCP the CSP subscriber names assigned by E-Governance CAs for both e-authentication assurance levels 1 and 2 CSPs are in the following form (based on the information received from the issuance letter):

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

The OU attributes are optional. The common name (CN) may be descriptive, or may be the Internet domain name of the CSP. That is, the common name may be "Acme Corporation" or "csp1.acme.com".

CSP subscriber certificates also include the CSP Internet domain name in the subject alternative name extension and an email address for a human point of contact (based on the information received from the issuance letter).

As established by the EGCP the Agency application server subscriber names assigned by the e-Governance CAs are in the following form (based on the information received from the issuance letter):

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

The organizational units department and agency appear when applicable and are used to specify the federal entity that employs the subscriber. At least one organizational unit will appear in the DN. The common name may be descriptive, or may be the Internet domain name of the server supporting the application. That is, the common name may be "Big Agency Grants Server" or "grants1.bigagency.gov".

Agency application server certificates include the server's Internet domain name in the subject alternative name extension and may include an email address for a human point of contact (based on the information received from the issuance letter).

3.1.2 Need for Names to be Meaningful

The EGCAs operating under the EGCP described in this CPS issue and sign certificates with subject names from within the name-space C=US, O=U.S. Government (based on the information received from the issuance letter).

Additionally, the EGCAs operating under this CPS may issue and sign certificates with subject names from other name spaces as directed by the EAO (based on the information received from the issuance letter).

The subscriber certificates (to AAs and CSPs) issued by the EGCAs include subject names that can be understood and used by relying parties and identify in a meaningful way the subscriber to which they are assigned.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are specified in [USGold].

3.1.4 Uniqueness of Names

Names, whether X.500 DNs or other name forms (e.g., an electronic mail address or DNS name), will be assigned by the EAO and made unique. The EAO will establish name space control procedures for names assigned to subscriber CSPs to ensure name collisions do not occur. The EAO will establish name space control procedures based on [US Gold] for names assigned to Agency application server subscribers.

Established name space control procedures for Internet Domain Names will avoid name collisions in the subject alternative name extension or the common name attribute.

3.1.5 Name Claim Dispute Resolution Procedure

Naming collisions will be brought to the attention of the EAO for resolution. The FPKI OA will revoke and re-issue all affected certificates as directed by the EAO. The EAO shall resolve any name collisions brought to its attention.

3.1.6 Recognition, Authentication and Role of Trademarks

The EGCP does not stipulate requirements for this section.

3.1.7 Method to Prove Possession of Private Key

The FPKI OA verifies that an applicant subscriber possesses the private key corresponding to the public key submitted (through physical delivery methods or using digital signature methods) with the application in accordance with section 4.2. All transactions involved in certificate issuance are recorded as part of the security audit data, as described in section 4.5.1. Since the EGCAs are at all times off-line, these messages are exchanged using an out-of-band mechanism as described in section 4.2.

3.1.8 Authentication of CSP Device Identity

Following the successful completion of the assessment application and acceptance processes and upon direction form the EAO, the FPKI OA verifies (as described in SO01):

- The identity information, in addition to the authenticity of the requester,
- That the requester is listed as a POC on the CSP E-Governance Certificate Issuance Authorization Letter.
- The requester's identity through either digitally signed messages or other secure means (e.g., in person or out-of-band mechanisms.).

The EGCP establishes that the requests for CSP certificates must include:

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

3.1.9 Authentication of Agency Application Servers

Following the successful completion of the assessment application and acceptance processes and upon direction from the EAO, the FPKI OA verifies (as described in SO01):

- The identity information, in addition to the authenticity of the requester,
- That the requester is listed as a POC on the Agency Application's *E-Governance Certificate Issuance Authorization Letter*.
- The requester's identity through either digitally signed messages or other secure means (e.g., in person or out-of-band mechanisms.).

The CSP certificates include information extracted from the PKCS#10 such as, the Equipment identification (i.e., DNS name) and the public keys.:

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

This section describes the procedures for accomplishing the Certificate Renewal, Update, and Routine Re-Key that meet the requirements specified in the EGCP.

3.2.1 Certificate Renewal

The EGCP does not allow renewal of subscriber certificates. except during recovery from CA key compromise (see 4.8.3).

3.2.2 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. (EGCP Section 6.3.2 establishes usage periods for private keys for both EGCAs and subscribers.) Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

The subscriber needs to repeat the procedures defined in Section 3.1 for all certificate issuance requests.

3.2.3 Certificate Update

Updating a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated. (See SO05).

The EGCAs do not update certificates they have issued to CSPs and AAs. If any field value in the certificate changes, such as a subscriber's name (e.g., due to merger or acquisition), then subscriber will provide, in this case, proof of the name change to the EAO or other designated agent in order for new certificate having the new name to be issued. Upon authorization by the EAO, the FPKI OA issues to the entity an updated certificate (and possibly revokes the old certificate).

EGCAs, since they distribute self-signed certificates, will also generate key rollover certificates, where the new public key is signed by the old private key, and vice versa.

When private keys are updated, all current users are notified via telephone and/or e-mail.

The distribution of the new self-signed certificate to current users will use physical delivery methods or using digital signature method to preclude malicious substitution attacks.

3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION

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

3.4 REVOCATION REQUEST

Revocation requests are received via physical delivery methods or digital signatures when available. Revocation request are authenticated using the call back procedures as described in detail in the FPKI OA *Standard Operating Procedures for the E-Governance Certification Authorities* [SOP].

4. OPERATIONAL REQUIREMENTS

4.1 APPLICATION FOR A CERTIFICATE

Application for certificates is governed by the *Standard Operating Procedures for the E-Governance Certification Authorities* [SOP].

4.1.1 Delivery of Public Key for Certificate Issuance

Public keys by the prospective subscribers are delivered to the EGCAs electronically in a digitally signed certificate request (i.e., using PKCS #10) message to the FPKI OA via secure physical delivery methods or digital signatures when available. Identity checking and proof of possession of the private key is accomplished as described in this CPS in section 3.1.8, 3.1.9, and 4.2.

The EGCA does not generate public/private key pairs on behalf of the subscriber.

4.2 CERTIFICATE ISSUANCE

The EGCP allows a certificate to be issued only to a single subscriber. The EGCAs do not issue Certificates containing a public key whose associated private key is shared by multiple subscribers. Note that where multiple devices assert the same DNS name, (e.g., load balanced authentication servers), they are considered a single subscriber and may share the private key corresponding to a certificate issued by the EGCA.

The following procedures take place to issue a AA or CSP Certificate:

- Upon receipt of an authorization letter from the EAO, the FPKI OA will authenticate the request by making direct contact (i.e., call back or challenge/response) with the requestor or establish communication via signed e-mail.
- In communication with the EAO, the FPKI OA verifies his/her name, entity, request for certificate issuance, and the justification. If verification is successful, the FPKI OA issues the certificate. Otherwise, a Security Incident Form is completed and the Information System Security Officer (ISSO) is immediately contacted.
- The FPKI OA fills out the e-Governance CA Issuance Form.
- The FPKI OA Team creates and verifies the accuracy of the certificate contents.
- The FPKI OA sends the certificate to the approved CSP or agency application server technical point of contact through secure physical delivery methods or digital signatures when available..
- The FPKI OA notifies EAO via fax, phone, or signed e-mail that the certificate was created and delivered.

- Upon notifying the EAO and ensuring the success of the certificate delivery, the FPKI OA signs and dates the e-Governance Issuance Form.

- The FPKI OA mails a copy of the form via postal service or signed e-mail to the e-Authentication Program Manager (or authorized official) for their records.
- The FPKI OA files the original form along with the authorization letter for auditing and archival purposes
- All authorization and other attribute information received from a prospective subscriber are verified against the *E-Governance Certificate Issuance Authorization Letter* before inclusion in a certificate. The EAO is responsible for verifying prospective subscriber data before issuing the authorization letter.

4.2.1 Delivery of Subscriber's Private Key to Subscriber

The EGCA does not generate public/private key pairs on behalf of the subscriber.

4.2.2 Public Key Delivery and Use

The EGCAs public keys are available for certificate validation. EGCAs certificates are published in the FPKIA public repository (see 2.1.7), and the verification of public keys is performed using X.509 path validation.

For EGCAs public keys used as trust anchors, the EGCAs ensure that self-signed EGCAs certificates are delivered to users through trusted procedural mechanisms. Such a self-signed CA certificate is sometimes called a Self-signed Certificate, or Trusted Certificate. This document will use the term Trusted Certificate.

The EGCA will deliver Trusted Certificates via secure physical delivery methods or digital signatures when available.

- EGCAs will create key rollover certificates as a consequence of EGCA re-key (See SO05). The new EGCA keys may be used securely (through the X.509 path validation algorithm) without explicit delivery of the public key to subscribers.

4.3 CERTIFICATE ACCEPTANCE

The MOA sets forth responsibilities of respective subscribers and the EAO before the EAO authorizes issuance of an EGCA certificate. Once the MOA has been signed and accepted the EAO will inform the CSP or agency application server POC of the creation of a certificate and the contents of the certificate.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Revocation

Client Security Incident and Client Routine Revocation are two types of revocations managed by the FPKI OA Team. Client Security Incident Revocation are revocations performed prior to the notification and approval of the EAO to prevent security comprise. Client Routine Revocation is a revocation requested through proper authorization channels.

4.4.1.1 Circumstances for Revocation

A certificate is revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding are—

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Privilege attributes asserted in the subscriber's certificate are reduced.
- The 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 subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.

The associated certificate is revoked and placed on the CRL whenever any of the above circumstances occurs. Revoked certificates are included on all new publications of the certificate status information until the certificates expire.

The FPKIA will perform re-issuance of such certificates, as specified in Section 3.1, as quickly as possible except where it would adversely affect the integrity and trust of the system.

4.4.1.2 Who Can Request a Revocation

Client Security Incidents and Client Routine are two types of revocations managed by the FPKI OA. Client Security Incidents are revocations performed prior to the notification and approval of the EAO to prevent security compromise. Client Routine is a revocation requested through proper authorization channels.

In case of client security incidents, the FPKI OA may summarily revoke certificates it issued to maintain the integrity of the system. The FPKI OA will then provide a written notice and brief explanation for the revocation to the subscriber.

For client routine, the EAO can request the revocation of a subscriber's certificate on behalf of any authorized party. A subscriber may request that its own certificate be revoked.

4.4.1.3 Procedure for Revocation Request

A request to revoke a certificate must identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The steps involved in the process of requesting a certification revocation are detailed in the SOP.

4.4.1.4 Revocation Request Grace Period

There is no grace period for revocation under the EGCP; EGCAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests are 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 that are not processed before the next CRL is published are processed before the following CRL is published.

4.4.2 Suspension

The EGCP does not allow certificate suspension.

4.4.3 CRLs

EGCAs issue CRLs covering all unexpired certificates issued under the EGCP.

4.4.3.1 CRL Issuance Frequency

CRLs are issued at least once every 18 hours. Scripts that update the online directory with the latest CRLs are run every 15 minutes to ensure the online directory is up-to-date.

4.4.4 Online Revocation/Status Checking Availability

The EGCP makes no stipulations on this section.

4.4.5 Other Forms of Revocation Advertisements Available

The EGCP does not require any other forms of revocation advertisement.

4.4.6 Checking Requirements for Other Forms of Revocation Advertisements

The EGCP does not require any other forms of revocation advertisement.

4.4.7 Special Requirements Related to Key Compromise

In the event of an EGCA private key compromise, the following operations are performed.

Since EGCAs distribute the public key in a Trusted Certificate, the FPKI OA performs the following operations:

- Generate a new signing key pair and corresponding Trusted Certificate;
- Initiate procedures to notify subscribers of the compromise; and
- Securely distribute the Trusted Certificate.
- The FPKI OA renews current certificates under the new signing key. (see 3.2.1)

4.5 SECURITY AUDIT PROCEDURE

Audit log files are generated for all events relating to the security of the EGCA. Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 4.5.3, *Retention Period for Security Audit Data*.

4.5.1 Types of Events Recorded

All security auditing capabilities of CA operating system and PKI CA applications have been enabled during installation. 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 CA's signing process
- A success or failure indicator when performing certificate revocation
- The identity of the entity and/or operator that caused the event.

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

The EGCAs record the events identified in the list below. Where these events cannot be electronically logged, the EGCAs supplement electronic audit logs with physical logs as necessary. The FPKI OA staff has verified (i.e., obtained vendor statements and conducted direct

testing) that the equipment and application software purchased indeed supports capturing audit logs for the events specified in the table below.

Table 4.5.1-1. Auditable Events

Auditable Event	FPKIA Directories		EGCA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
SECURITY AUDIT				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	✓			✓
Any attempt to delete or modify the Audit logs	✓ After a deletion following any archive operation	✓ After a modification following any archive operation		✓
Obtaining a third-party time-stamp	✓	✓	✓	✓
IDENTIFICATION AND AUTHENTICATION				
Successful and unsuccessful attempts to assume a role		✓		✓
Change in the value of maximum authentication attempts	✓			✓
Maximum number of unsuccessful authentication attempts during user login		✓		✓
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	The account is immediately re-activated	The account is immediately re-activated		✓
An Administrator changes the type of authenticator, e.g., from password to biometrics	✓			✓
LOCAL DATA ENTRY				
All security-relevant data that is entered in the system	✓	✓ Through Windows/ISO DE Logging	✓	✓ Through Windows/CA Logging
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system	✓	✓ Through	✓	✓ Through

Auditable Event	FPKIA Directories		EGCA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
		firewall Logs and Netmon		firewall Logs and Netmon
DATA EXPORT AND OUTPUT				
All successful and unsuccessful requests for confidential and security-relevant information	✓ Manual Logs		✓ Manual Logs	
KEY GENERATION				
Whenever the EGCA generates a key. (Not mandatory for single session or one-time use symmetric keys)	Applies to CA only	Applies to CA only	✓	✓
PRIVATE KEY LOAD AND STORAGE				
The loading of Component private keys	Applies to CA only	Applies to CA only		✓
All access to certificate subject private keys retained within the EGCA for key recovery purposes	Applies to CA only	Applies to CA only		✓
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	✓	✓
SECRET KEY STORAGE				
The manual entry of secret keys used for authentication	Applies to CA only	Applies to CA only	✓	✓ CA,Smart Card logging / Luna Logs
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret -keys (keys used for a single session or message are excluded)	Applies to CA only	Applies to CA only	✓	✓
CERTIFICATE REGISTRATION				
All certificate requests	Applies to CA only	Applies to CA only	✓	✓
CERTIFICATE REVOCATION				
All certificate revocation requests	Applies to CA only	Applies to CA only	✓	✓

Auditable Event	FPKIA Directories		EGCA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
CERTIFICATE STATUS CHANGE APPROVAL				
The approval or rejection of a certificate status change request	Applies to CA only	Applies to CA only	✓	✓
EGCA CONFIGURATION				
Any security-relevant changes to the configuration of the EGCA	Applies to CA only	Applies to CA only	✓	✓
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	✓		✓	✓
The access control privileges of a user account or a role are modified	✓		✓	✓
CERTIFICATE PROFILE MANAGEMENT				
All changes to the certificate profile	Cert Profile not captured in Directory	Cert Profile not captured in Directory	✓	
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile	Revocation Profile not captured in Directory	Revocation Profile not captured in Directory	✓	
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	✓	
MISCELLANEOUS				
Appointment of an individual to a Trusted Role	✓		✓	
Designation of personnel for multiparty control	✓		✓	
Installation of the Operating System	✓		✓	✓
Installation of the FBCA CA	Applies to CA only	Applies to CA only	✓	✓

Auditable Event	FPKIA Directories		EGCA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
Installing hardware cryptographic modules	Applies to CA only	Applies to CA only	✓	
Removing hardware cryptographic modules	Applies to CA only	Applies to CA only	✓	
Destruction of cryptographic modules	Applies to CA only	Applies to CA only	✓	
System Startup	✓			✓
Logon Attempts to EGCA Apps	Applies to CA only	Applies to CA only		✓.
Receipt of Hardware / Software	✓		✓	
Attempts to set passwords	✓			✓
Attempts to modify passwords	✓			✓
Backing up EGCA internal database	Applies to CA only	Applies to CA only		✓
Restoring EGCA internal database	Applies to CA only	Applies to CA only	✓	
File manipulation (e.g., creation, renaming, moving)		✓		✓
Posting of any material to a repository		✓		✓
Access to EGCA internal database	Applies to CA only	Applies to CA only	✓	✓
All certificate compromise notification requests	Applies to CA only	Applies to CA only	✓	
Loading tokens with certificates	Applies to CA only	Applies to CA only		✓
Shipment of Tokens	Applies to CA only	Applies to CA only	✓	
Zeroizing tokens	Applies to CA only	Applies to CA only	✓	
Rekey of the EGCA	Applies to CA only	Applies to C	✓	✓

Auditable Event	FPKIA Directories		EGCA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
Configuration changes to theEGCA server involving:	Applies to CA only	Applies to CA only		
Hardware	Applies to CA only	Applies to CA only	✓	
Software	Applies to CA only	Applies to CA only	✓	
Operating System	Applies to CA only	Applies to CA only	✓	✓
Patches	Applies to CA only	Applies to CA only	✓	✓
Security Profiles	Applies to CA only	Applies to CA only	✓	✓
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to room housing EGCA	✓	✓	✓	✓
Access to the EGCA server	Applies to CA only	Applies to CA only	✓	✓
Known or suspected violations of physical security	✓	✓	✓	
ANOMALIES				
Software Error conditions	✓	✓	✓	✓
Software check integrity failures	✓	✓	✓	✓.
Receipt of improper messages	✓	✓	CA is stand alone	CA is stand alone
Misrouted messages	✓	✓	CA is stand alone	CA is stand alone
Network attacks (suspected or confirmed)	✓	✓	CA is stand alone	CA is stand alone
Equipment failure	✓	✓	✓	✓
Electrical power outages	✓	✓	✓	✓
Uninterruptible Power Supply (UPS) failure	✓	✓	✓	✓

Auditable Event	FPKIA Directories		EGCA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
Obvious and significant network service or access failures	✓	✓	CA is stand alone	CA is stand alone
Violations of Certificate Policy	✓	Certain Violations as documented by this table	✓	Certain Violations as documented by this table
Violations of Certification Practice Statement	✓	Certain Violations as documented by this table	✓	Certain Violations as documented by this table
Resetting Operating System clock	✓		✓	

4.5.2 Frequency of Processing Data

The FPKI OA reviews the audit logs once a week. The FPKI OA reviews all (100 percent) the security audit data generated by the CA since the last review is examined. Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. The FPKI OA procedures include what actions will be followed and associated documentation produced as a result of these reviews.

4.5.3 Retention Period for Security Audit Data

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 for three months but their electronic versions are permanently retained on the primary site server and hence these logs are always available. Audit logs are retained offsite at the interim storage area for three months. The FPKI OA Administrator removes audit logs from the EGCA and gives them to the FPKI OA Auditor neither of whom commands the EGCAs signature key(s).

4.5.4 Protection of Security Audit Data

The FPKI OA Auditor performs routine review of security audit logs. The procedure for protecting security audit data is 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 FPKI OA Administrator, Security Officer, Auditor, Operator, and others possibly designated by the EAO.

3. Only the FPKI OA Auditor is authorized to archive audit logs.

4. Audit logs are deleted only under procedural multi-person control.

5. Audit logs are protected under multi-person control and cannot be modified without detection.

Daily audit logs are generated on time stamped digital media and are protected from deletion and/or modification prior to the end of the audit log retention period. See sections 4.5.5, 4.5.6, 4.6, and 5.0 for descriptions of physical and procedural controls for protection of the data.

4.5.5 Security Audit Data Backup Procedures

FPKIA Directory:

Audit logs and audit summaries are incrementally backed up daily via time stamped digital media. Full backups are performed daily via digital tape media. Weekly, the backups are moved to and stored in secure container in a separate building (interim storage) from the FPKIA facility. Additionally, backups are performed at the hot site location to ensure continuity; shadowing the primary directory and performing weekly backups accomplish this.

EGCA:

Full backups are performed daily via digital tape media. Weekly backups are moved to and stored in secure container in a separate building (interim storage) from the FPKIA facility.

Manual audit logs will be collected weekly and stored in a secure container in a separate building (interim storage) from the FPKIA facility. These audit logs are moved to the hot site archive location quarterly.

4.5.6 Security Audit Collection System (Internal vs. External)

The audit log collection system is internal to the FPKIA components (see section 4.5.1). Audit processes are invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the FPKI OA will determine whether to suspend EGCA operation until the problem is remedied. The EAO will then determine whether to resume operations. Section 4.5.1 describes the collection procedures

(manual or automatic) for the auditable events. Section 4.5.5 describes the protection procedures for backing up audited data that has been collected.

4.5.7 Notification to Event-Causing Subject

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

4.5.8 Vulnerability Assessments

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

Vulnerability assessments, as part of security compliance audits, are conducted as specified by the FPKIPA.

The FPKI OA provides a report of the analysis of the results of vulnerability assessments, specifically indicating security vulnerabilities identified and correction procedures of those vulnerabilities.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Archived

The FPKI OA Auditor produces archive records on a weekly basis. The records are stored on paper and all electronic data to include certificates and CRLs are stored on the offline directory The archive records include data received from the certificates and CRLs it generated, certificate requests and certificate revocation requests it received.

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

- FPKIA certification and accreditation
- Certification Practice Statement
- Contractual obligations
- System and equipment configuration
- Modifications and updates to system or configuration

- Certificate requests
- Revocation requests
- Subscriber identity Authentication data as per Section 3.1.9
- Documentation of receipt and acceptance of certificates
- Documentation of receipt of tokens
- All certificates issued or published
- Record of Re-key
- All CARLs and CRLs issued and/or published
- All Audit Logs
- Other data or applications to verify archive contents
- Documentation required by compliance auditors
- See Section 4.5 for a description of the audit and archive collection procedures.

4.6.2 Retention Period for Archive

Weekly, the backups from the primary site are moved to and stored in secure container in the interim storage facility. Quarterly, the weekly backups from the interim storage are moved to and stored in secure container at the hot site storage facility. Records are periodically moved from the hot site for the long term archival at the National Archives and Records Administration (NARA). The backups will be archived at NARA for a period of at least ten years, six months.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site and approved by the FPKI OA and FPKIPA. The interim site is located at:

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

The hot site is located at:

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

Prior to the end of the archive retention period, the FPKIA will provide the archived data and the applications necessary to read the archives to the FPKIPA.

4.6.3 Protection of Archive

Long-term protection of the archive is provided as described in the FPKIA SOP SA13.

Archive data is clearly labeled as follows:

- Classification Label: SBU
- Name of the Program: FPKIA
- 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 and the hot site facilities, which are temperature controlled and behind locked doors, as described in section 5.1.

The FPKIA ISSO maintains a list of individuals who can access and delete the on-line archive files at the primary site. This list is the FPKIA Form "Access Control Checklist". Deletion of on-line archive files is accomplished under multi-person control procedures as described in the Sections 5.1.2 and 5.2.2" in this CPS.

The contents of the archive will not be released except as determined by the FPKIPA or as required by law. The procedure for releasing information is described in SA06.

4.6.4 Archive Backup Procedures

Archive records are backed-up as part of the nightly normal system backup procedure to single session, 4mm digital tapes.

Full system backups are performed daily to digital tape removable storage media.

4.6.5 Requirements for Time-Stamping of Records

Records will be clearly labeled with date/time period information of the data contained in the record as described in section 4.6.3. System logs are automatically time stamped and systems use the NIST time server to maintain synchronize time via Network Time Protocol (NTP).

4.6.6 Archive Collection System (Internal or External)

The archive information will be collected by the FPKI OA Auditor, who will be responsible for archival.

4.6.7 Procedures to Obtain and Verify Archive Information

Creation of archive data is described in section 4.6.1. The archive data is placed in clearly labeled, double wrapped packaging for transport to short-term and long-term archive locations. Transport of archive data is via hand carry for short-term archive by the FPKIA Auditor or approved courier services. Storage and protection of archive data is described in section 5.

The FPKI OA auditing official will maintain logging information (and receipts) as archived data is transported to short-term and long-term archive facilities.

4.7 KEY CHANGEOVER

The EGCA key changeover procedures (see SO05) are as follows:

- The EGCA will generate a self-issued certificate signed by the old private key whose *subjectPublicKeyInfo* field contains the new public key.
- The EGCA will generate a self-issued certificate signed by the new private key whose *subjectPublicKeyInfo* field contains the old public key.
- The EGCA will generate a self-issued certificate signed by the new private key whose *subjectPublicKeyInfo* field contains the new public key.
- The EGCA and all CSPs and AAs will process new CA certificates as described in the e-governance SOP.
- All certificates generated as part of the key changeover process will be posted to the FPKIA 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 CSP and AA key changeovers by issuing and posting new certificates as required.

The EGCAs signing key have a validity period as described in Section 6.3.2.

Once the key rollover is completed only the new key will be used to sign certificates. The old private key is retained and protected in order to sign CRLs that contain certificates signed by that key. See key changeover procedure SO05 for more deails.

4.8 COMPROMISE AND DISASTER RECOVERY

The EGCA and FPKIA directory system are deployed so as to provide 24-hour, 365-day availability. The EGCA implements features to provide high levels of reliability as described in the following subsections.

The EGCA has recovery procedures in place to reconstitute the EGCA within 72 hours in the event of a catastrophic failure, as described in the following subsections.

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

In the event of a disaster, the following steps will be accomplished to regain system functionality (including when the CA equipment is damaged or rendered inoperative, but the CA signature keys are not destroyed) so that CA operation is reestablished as quickly as possible, giving priority to the ability to generate certificate status information:

1. Notification of the GSA Designated Official For Facilities (DOFF) and Facility Emergency Response Team Leader (FERTL). These individuals along with the FPKI OA 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 FPKI OA Management team.

5. If the severity/scenario (to exceed 6 hours) of the event is critical, activation of the alternate site (hot site).

6. The FPKIA POCs (“hot list”) will be notified of this change, so that any changes required by the shared service provider CAs can be performed

7. Manage the recovery process of the primary FPKIA facility.

8. Submit post recovery logs to FPKIPA

In order to provide for rapid EGCA service re-activation, the FPKI OA implements a synchronized hot site. The hot site includes an identical configuration of the primary site. The FPKIA hot site online directory is updated by a running script that pulls the information from the primary site on a regular basis. The hot site offline EGCA will be quickly restored via backup tapes.

Certificates may need to be validated and new public keys/certificates issued in the event anomalies exist.

The following reports are generated:

1. Activity log – this log is maintained throughout the disaster recovery process.
2. Test plan results
3. Equipment list – Update configuration management
4. Restoration Expense report

The FPKIPA will be notified as soon as possible as described in DR01 and DR02.

4.8.2 CA Cannot Generate CRLs

If the EGCA cannot issue a CRL within 72 hours after the time specified in the next update field of its currently valid CRL, the FPKI OA will immediately inform the FPKIPA, as well as the AAs and CSPs where appropriate. See DR01 for details.

4.8.3 CA Signature Keys are Compromised

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

1. 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;

2. The EGCA will generate a new EGCA key pair in accordance with procedures set forth in section 4.2

3. New EGCA certificates will be issued to AAs and CSPs also in accordance with section 4.2.

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

See Revocation Procedures SO02 for details on the revocation process, including CA Key Compromise.

4.8.4 Secure Facility Impaired after a Natural or Other Type of Disaster

In the case of a disaster whereby the EGCA primary installation is physically damaged and all copies of the EGCA signature key are destroyed as a result, the FPKIPA and the EAO will be securely notified (via callback and challenge-response described in SO02) at the earliest feasible time, the FPKIPA will take whatever action it deems appropriate, and the procedures described in section 4.8.1 will be followed. However, copies of the private keys are maintained at the interim site and hot site. See HD01 and DR01 for details. 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 subordinate shared service provider certificates. The details of this plan are defined in the FPKI OA BCCP and Disaster Recovery Procedures.

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

4.9 CA TERMINATION

In the event of termination of the EGCA operation, certificates signed by the EGCA will be revoked. The FPKI OA will advise, using secure communication (callback and challenge-response described in SA09) all the CSPs and AAs, to which the EGCA has issued TLS certificates, of its termination. All documentation and data will be archived using the NARA Storage procedures (SA13).

The FPKI OA Team will coordinate scheduled termination with CSPs and AAs when authorized by the FPKIPA.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.1 Site Location and Construction

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

The FPKIA Hot Site: Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.2 Physical Access

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.3 Electrical Power

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

5.1.4 Water Exposures

The FPKIA room implements water protection safeguards equivalent to those implemented for the GSA FTS computer room. At the Primary facility, water pipes are not filled until an actual fire is detected. There is no water suppression system at the hotsite.

5.1.5 Fire Prevention and Protection

The FPKIA room implements fire prevention and protection safeguards equivalent to those implemented for the GSA FTS computer room. Additionally, the room is equipped with ceiling sprinklers. See section 5.1.6 for more details.

5.1.6 Media Storage

The FPKIA room also includes a GSA-certified small safe, fireproof locked cabinets, and desk where media are stored so as to protect them from accidental damage (water, fire, electromagnetic). Media that contain audit, archive, or backup information are stored at a different location separate from the FPKIA (i.e. in an off-site interim Storage Facility) and after three months they are transported to long-term site specified in section 4.6.2. Additionally the

safes in both primary site and hot site are fire retardant and shield from electromagnetic emissions.

5.1.7 Waste Disposal

The disposal of sensitive or classified information is handled in accordance with the GSAFTS procedures for disposal of such material. Burn bag procedures are in place. See FPKIA procedure SA10 for more details.

5.1.8 Offsite Backup

For the FPKIA full system backups, sufficient to recover from total system failure, are conducted on a periodic schedule, described in section 4.5. The short-term backup site specified in section 4.6.3 and contains up to three months worth of backup information. The long-term backup site is specified in section 4.6.2.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The functions performed in these roles and the people selected to fill them form the basis of trust for the entire Federal PKI Architecture. 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 FPKIA encompasses CA products from several vendors implementing different certificate policies. Different commercial products support somewhat different roles, and use different mechanisms for registering or enrolling subscribers and issuing certificates; however, they can all be re-conducted to the following somewhat abstract roles, derived from roles identified in the CIMC Protection Profile developed by NIST—

9. *Administrator* – authorized to install, configure, and maintain the Operating Systems and Directory Software; establish and maintain Operating System user accounts; configure Operating System profiles and audit parameters; and generate component keys.

10. *Security Officer* – authorized to request or approve certificates or certificate revocations; authorized to install, configure and 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.

11. *Auditor* – authorized to view and maintain audit logs.

12. *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, and;
- Assisting in Generating and Backing up EGCAs keys.

Administrators do not issue certificates to subscribers.

5.2.1.2 Security Officer

The Security Officer role is responsible for issuing certificates, including—

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates;
- Requesting, approving and executing the revocation of certificates.
- Configuring certificate profiles or templates and audit parameters for the CAs software.
- Generating and backing up CAs keys

5.2.1.3 Auditor

The auditor role is responsible for—

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

5.2.1.4 Operator

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

5.2.2 Separation of Roles

Role separation, when required as set forth below, is enforced either by the EGCA equipment, or procedurally, or by both means.

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

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

Separation of roles is accomplished through the use of RSA Passage hardware tokens and procedures that ensure separation of roles and multi-person control of the EGCA where required and specified in section 5.1.2.

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

Once the EGCA is activated, access to the EGCA private signing key for issuance and revocation of certificates requires a minimum of 2 FPKI OA Personnel, at least one authenticated via individual smartcards.

Audit log data is generated automatically by the EGCA for all access and EGCA activities.

To best ensure the integrity of the FPKIA 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 FPKIA operation.

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

5.2.3 Identification and Authentication For Each Role

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

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

The FPKIPA and the FPKI OA are responsible and accountable for the operation of the FPKIA

All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and are U.S. citizens. The procedures governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the FPKIA are described in the FPKIA SSP. Appendix A of this CPS includes selected excerpts from that portion of the FPKIA SSP.

All FPKIA personnel hold TOP SECRET security clearances.

5.3.2 Background Check Procedures

FPKI OA personnel background checks are performed in accordance with TOP SECRET security clearance requirements and demonstrate compliance with requirements set forth in section 5.3.1 of the EGCP.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the FPKIA receive comprehensive training. Training includes review of all related procedures and rules of behavior. Training is conducted in the following areas by certified product engineers:

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

- Stipulations of the EGCP.

Training in the overall security procedures of the FPKIA is conducted for all personnel at the initial full operation capability of the FPKIA. 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.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles are made aware of changes in the FPKIA operation as described in personnel training procedures documentation. Any significant changes to the operations are documented and personnel are informed and made aware of changes in accordance with the personnel training procedures. All FPKI OA personnel will participate in mandatory refresher training annually as to ensure all affected personnel are aware of new changes to procedures and configuration changes. In addition, immediate On-the-Job-Training (OJT) is conducted when any changes occur within the FPKIA operations. Examples of such changes are FPKIA software or hardware upgrades, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

The EGCP does not stipulate requirements for this section.

5.3.6 Sanctions For Unauthorized Actions

The FPKI OA takes 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 will immediately investigate the incident. After the investigation, the ISSO and ISSM will determine if the action warrants disciplinary actions based on severity and the reoccurrence of the indiscretion. If the action is of significant indiscretion, it will be reported to the FPKI Program Manager 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 as to prevent further indiscretions.

5.3.7 Contracting Personnel Requirements

See section 5.3.1. Contractor personnel employed to perform functions pertaining to the EGCA meet applicable requirements set forth in the EGCP and this CPS as determined by the FPKI OA.

5.3.8 Documentation Supplied to Personnel

The FPKI OA makes available to all of its personnel the EGCP, this CPS, and any relevant statutes, policies or contracts. The training is role based to ensure that recipients understand the

procedures, rules of behavior and security issues for fulfilling their duties. Documentation identifying all personnel receiving and completing training is maintained by the FPKI OA. All procedures and forms are provided to all FPKI OA personnel. However, individuals are required to review procedures and forms pertaining to their specific role during training.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The key pair for the FPKIA CAs are generated on the Chrysalis LunaSA cryptographic module. The key pair generation is RSA for digital signature in compliance with PKCS-1 (FIPS 140-2, level 3). The private key will never be exposed outside the module in unencrypted form. Backup copies of the LunaSA private keys will be created.

FPKIA private keys are generated using the FPKIA key signing Ceremony procedures. These procedures document the role separation and provide an auditable trail. These procedures are completed with a third party auditor present, where 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

Subscriber (CSPs and AAs) key pair generation is performed by the subscriber, using a FIPS approved method.

6.1.2 Private Key Delivery to Subscriber

Subscribers (AAs and CSPs) generate their own key pairs; hence there is no need to deliver private keys, and this section does not apply.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered to the EGCA electronically in a certificate request (i.e., using PKCS #10) messages to the FPKI OA via secure physical delivery methods or digital signatures when available. Identity checking and proof of possession of the private key will be accomplished as described in section 4.1.

6.1.4 CA Public Key Delivery to Relying Parties

The EGCA trusted certificate will be transported in a secure, out-of-band mechanism via e-mail or floppy disk delivered by registered mail or courier to the relying parties

Key rollover certificates are signed with the EGCA current private key are thus posted to the FPKIA directory/repository, so secure distribution is not required. CA Trusted Certificates are distributed via secure physical delivery methods or digital signatures when available. See section 6.1.3 and SO05.

6.1.5 Key Sizes and Signature Algorithms

EGCA trusted certificate public key sizes are 2048 bits for RSA, SHA-1, in accordance with FIPS 186. EGCA certificates issued to CSPs, AAs, and CRLs use a 2048 public key size for RSA and use SHA-1. The EGCA currently does not utilize TLS to meet any security requirements. Signatures on certificates and CRLs that are issued on or after January 1, 2009 will be generated using SHA-256.

6.1.6 Public Key Parameters Generation

There are no public key parameters for RSA.

6.1.7 Parameter Quality Checking

There are no public key parameters for RSA.

6.1.8 Hardware/Software Subscriber key generation

The EGCA key pairs are generated in a FIPS 140-2 Level 3 validated, LunaSA hardware cryptographic module.

Key pairs for trusted roles and provision of multi-person controls are generated in a FIPS 140-1 Level 2 validated RSA Passage cryptographic modules.

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

EGCA certificates assert the *digitalSignature*, *keyCertSign*, and *cRLSign* bits and does not assert the *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

The EGCAs private keys are protected using FIPS 140-2 Level 3 validated cryptographic module: Chrysalis LunaSA hardware token.

Key pairs for FPKIA separation of roles are generated in FIPS 140-1 Level 2 validated cryptographic modules: RSA Passage SmartCards.

All cryptographic modules are operated such that the private asymmetric cryptographic keys are never output in plaintext.

See section 5.2.2 for a description of the procedures used for accessing and operating the EGCA.

6.2.2 Private Key Multiperson Control

All EGCA private keys, their backups (including during the backup procedure) are under 2 out of N control, where N≥2. N represents the total number of Security Officers. See the following sections for details on how this is achieved.

6.2.3 Private Key Escrow

Neither EGCA nor Subscriber private keys are ever escrowed.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.2.4.2 Backup of Subscriber Private Keys

Subscriber private keys are not maintained by the FPKI OA. FPKI OA does not back up subscriber keys.

6.2.5 Private Key Archival

EGCA private keys will not be archived.

6.2.6 Private Key Entry Into Cryptographic Module

EGCA private keys are generated by and remain in a cryptographic module. The Chrysalis product uses proprietary secure means for transferring keys from one cryptographic module to another to back up the CA keys. This procedure does not involve encryption.

6.2.7 Method of Activating Private Keys

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.2.8 Methods of Deactivating Private Keys

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.2.9 Method of Destroying Subscriber Private Keys

The FPKI OA does not manage subscriber private keys. Regarding the FPKI OA personnel private keys, the triple-DES encrypted key blobs on the hard drive are destroyed and the administrator tokens reinitialized, under the same multi-person control procedures used to initially generate the key pairs described above. Note that if the tokens are not reinitialized, they could be used to restore the key with any backup copy of the key blobs.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Usage Periods for the Public and Private Keys

The EGCA private signing keys will be used to sign certificates for one-half of the certificate lifetime (e.g. for 2 years if the certificate lifetime is 4 years). The certificate lifetime will be valid not more than 6 years. Rekeying will be performed after 3 years.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.4.2 Activation Data Protection

Activation data is memorized, not written down. If written down, it is secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.4.3 Other Aspects of Activation Data

Passwords are changed at least every 90 days to decrease the likelihood of discovery.

6.5 COMPUTER SECURITY CONTROLS

Text removed. This Information is 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" (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

The EGCA server uses configurations that have been clearly demonstrated and passed the Compliance Audit process as described in section 2.7.

The EGCA equipment is configured with appropriate security features turned on as recommended by the host operating system vendor in accordance with any associated security validation rating. The EGCA has the following security features and functions:

- Require authenticated logins via FIPS PUB 140-2 Level 3 and FIPS PUB 140-1 Level 2 cryptographic modules
- 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 FPKIA roles as described in sections 5.1.2 and 5.2.2
- Enforce separation of duties for FPKIA roles as described in sections 5.1.2 and 5.2.2
- Require identification and authentication of FPKIA roles and associated identities as described in sections 5.1.2 and 5.2.2
- Prohibit object re-use or require separation for random access memory. It is assumed that verification of meeting this requirement is provided by the Windows 2000 operating system. Windows 2000 enforces the required prohibition/separation. Windows 2000 was evaluated under IT SEC E3/FC2, since the FC2 functional package is equivalent to the Orange Book's C2, it includes the required memory protection controls. More information on the Windows 2000 evaluation is available at: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dngenlib/html/msdn_ntvmm.asp.

- Require use of cryptography for session communication and database security. The use of cryptography for session communication is not required because the certificate request messages (PKCS#10) are exchanged using an out-of-band mechanism and are imported manually directly at the CA. The CA database is protected via triple-DES cryptography.
- Archive EGCA history and audit data through data collection and archive procedures described in sections 4.5 and 4.6
- 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.
- Require a trusted path for identification of FPKIA roles and associated identities logins via FIPS PUB 140-2, Level 3 and 140-1 Level 2 cryptographic modules. Requires a recovery mechanisms for keys and the FPKIA system through backup and protection procedures described in 4.5.5

Enforce domain integrity boundaries for security critical processes through self-test procedures described above.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

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 very formal development process that is well documented. Information to that regard was requested from the vendor and proprietary documentation was reviewed.
- There is neither hardware nor software developed specifically for the EGCAs.
- 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 ordered and installed by certified engineers under the direction and control of authorized FPKIA 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 will be purchased using commercial buys. Hardware and non-CA software is purchased randomly, through standard procurement procedures provided by the FPKI OA. An accountable method of packaging and delivery will be used to provide a continuous chain of accountability from the vendor to the facility (e.g., UPS, Federal Express, USPS Express Mail). The FPKIA

establishes a relationship with the CA software vendors prior to acquisition that gives assurance that the software has not been tampered with. Installation is performed under multi-person control with only authorized FPKIA operation personnel.

- 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 FPKIA facility under multi-person control. McAfee AntiVirus will be 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 at startup, periodically, and any time a system configuration change occurs (i.e., adding a new CA to the FPKIA).
- The CA hardware and software is dedicated to performing one task: the CA. Other software installed on the CA machine is used to facilitate proper operation of the CA. Only one CA can be installed on the machine at one time.
- All applications required to perform the operation of the CA are obtained from sources authorized by local policy

6.6.2 Security Management Controls

The initial configuration of the EGCA software (i.e., CA software, repository software) as well as any modifications and upgrades will be documented and controlled in accordance with FPKIA Configuration Management Procedures (separate FPKI OA document). System and application level logging will be 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 above.

6.6.3 Life-Cycle Security Ratings

The EGCP stipulates no requirements for this section.

6.7 NETWORK SECURITY CONTROLS

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

The description of the practice for cryptographic modules is stated above in Section 6.2

7. CERTIFICATE AND CRL PROFILES

7.1 CERTIFICATE PROFILE

Certificates issued by the EGCA conform to the X.509 Certificate and CRL Extensions Profile for the Common Policy [CCP-PROF] with the exception of the policy OIDs. Policy OIDs for certificates issued under this policy are specified below in Section 7.1.6.

Subscriber certificates conform to the Certificate Profile for Computing and Communication Devices in [CCP-PROF] CA certificates conform to the Self-Issued CA Certificate Profile in [CCP-PROF].

Entity certificate extension information are found in the Issuance letter.

7.1.1 Version Numbers

The CA will issue X.509 v3 certificates (populate version field with integer “2”).

7.1.2 Certificate Extensions

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

7.1.3 Algorithm Object Identifiers

Certificates issued under the EGCP and described by this CPS use the following OIDs for signatures:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates issued under the EGCP and described in this CPS 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 are populated with an X.500 Distinguished Name, with the attribute type as further constrained by Section 3.1.1.

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

7.1.5 Name Constraints

Certificates issued under the EGCP do not contain name constraints.

7.1.6 Certificate Policies Extension

Certificates issued under the EGCP described by this CPS assert one or more of the following OIDs in the certificate policies extension, replacing the OIDs listed in the [CCP-PROF], as appropriate:

id-eGov-Level1 ::= {2 16 840 1 101 3 2 1 3 9}

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}

7.1.7 Usage of Policy Constraints Extension

Certificates issued under the EGCP described by this CPS do not contain policy constraints.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under the EGCP described by this CPS do not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

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

7.2 CRL PROFILE

CRLs issued by a CA under the EGCP described by this CPS conform to the CRL Profile specified in [CCP-PROF].

7.2.1 Version Numbers

The EGCAs issue X.509 Version 2 CRLs.

7.2.2 CRL Entry Extensions

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

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

Errors, updates, or suggested changes to this document will be communicated to the contact in section 1.4. Such communication will include a description of the change, justification for the change, contact information for the person requesting the change, and an impact assessment.

Changes to this document will be reviewed and approved by the FPKIPA, will be communicated to every CSP and AA, and will be posted at the website specified in section 2.6.4.

Errors, updates, or suggested changes to this CPS are notified to all CSPs and AAs. All versions of this document will be reviewed and approved by the FPKIPA.

Revised versions of this document will be disseminated to interested parties (see section 8.2).

8.2 PUBLICATION AND NOTIFICATION POLICIES

The FPKIPA will publish information (including the redacted version of this CPS) on the following web sites: http://www.cio.gov/fpkipa.

The redacted version of this CPS will also be disseminated via email to any that request it.

Proposed changes to the CPS will be sent to shared service provider CAs.

The FPKIPA will provide an updated and approved document within 1 week to the FPKIPA web administrator, who has agreed to post this information.

The redacted version of this CPS and any subsequent changes shall be made publicly available within 1week of approval.

8.3 CPS APPROVAL PROCEDURES

The FPKIPA and or the EAO will make the determination that this CPS complies with EGCP. The EGCA and FPKI OA must meet all requirements of an approved CPS before commencing operations. In some cases, the PA and/or the EAO may require the additional approval of an authorized agency. The PA and/or the EAO will make this determination based on the nature of the system function, the type of communications, or the operating environment.

8.4 WAIVERS

The PA and/or the EAO will not issue waivers; EGCAs issuing under this policy meet all facets of the EGCP.

9. BIBLIOGRAPHY

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

ABADSG	Digital Signature Guidelines, 1996-08-01 http://www.abanet.org/scitech/ec/isc/dsgfree.html
CAF	E-Authentication Interim Credential Assessment Framework (CAF), 12/19/2003 release 1.3.0. http://www.eapartnership.org/docs/CAF_CAFv1-3.doc
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
CCP-PROF	X.509 Certificate and CRL Extensions Profile for the Common Policy, July 8, 2004.
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 2000.
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996 Http://www4.law.cornell.edu/uscode/40/1452.html
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999
M-04-04	E-Authentication Guidance for Federal Agencies, December 16, 2003.
PKCS#1	RSA Cryptography Standard, Technical Note, Version 2.1. 14 June 2002. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf
RFC 2527	Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999
RFC 3280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Housley et al., April 2002.
SOP	Standard Operating Procedures for the E-Governance Certification Authorities, March 2004.

SP 800-63 Electronic Authentication Guideline, Burr, Polk, and Dodson.

USGold GOVERNMENTWIDE DIRECTORY SUPPORT 2

TECHNICAL SERIES: The Updated USGold Schema, July 14, 1997.
http://csrc.nist.gov/pki/twg/directory_references.htm

10. ACRONYMS AND ABBREVIATIONS

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

OMB	Office of Management and Budget
PA	Federal PKI Policy Authority
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
POC	Point of Contact
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SAML	Security Assertion Markup Language
SHA-1	Secure Hash Algorithm, Version 1
SHA-256	Secure Hash Algorithm, 256-bit version
TLS	Transport Layer Security
U.S.C.	United States Code
WWW	World Wide Web

11. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to IS resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Applicant	The subscriber is sometimes also called an “applicant” after applying to a CA for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.

Audit	Independent review and examination of records and activities to assess the adequacy of system controls; to ensure compliance with established policies and operational procedures; and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009audit trail]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical characteristic of a human being, including a photograph for visual identification. For the purposes of this document, biometrics do not include handwritten signatures.
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 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 Authority	A trusted entity that provides online verification to a relying party of a subject certificate's trustworthiness and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Component Private Key	Private key associated with a function of the certificate-issuing equipment, as opposed to being associated with an operator or administrator.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Credential Service Provider	An organization that offers one or more credential services.

Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate and (2) whether the message has been altered since the transformation was made.
Discretionary Access Control	Means of restricting access to objects based on user identity.
E-Commerce	The use of network technology (especially the Internet) to buy or sell goods and services.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions or to establish or exchange a session key for these same purposes.
End Entity	Relying parties and subscribers.

Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge, or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [Adapted from ABADSG, "Commercial key escrow service"].
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key and (2) even knowing one key, it is computationally infeasible to discover the other key.

Mutual Authentication	Authentication when parties at both ends of a communication activity authenticate each other (see "Authentication").
Naming Authority	An organizational entity responsible for assigning DNs and for assuring that each DN is meaningful and unique within its domain.
Nonrepudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009]. Technical nonrepudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal nonrepudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization; the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI OIDs are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties using a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Privacy	Restricting access to subscriber or relying party information in accordance with Federal law and Agency policy.

Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair used to encrypt confidential information. In both cases, this key is made publicly available, normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects but does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Secret Key	A "shared secret" used in symmetric cryptography, wherein users are authenticated based on a password, PIN, or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.
Server	A system entity that provides a service in response to requests from clients.
Subscriber	A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device.

System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by relying parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Agency in confirming subscriber identification during the registration process. Trusted Agents do not have automated interfaces with CAs.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor."
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 1401]

Part 4: X.509 Certification Practice Statement (CPS) For the Citizen and Commerce Class Common (C4) Certificate Policy Certification Authority

United States Federal PKI Architecture

Federal PKI Architecture X.509 Certification Practice Statement – Part 4: X.509 Certification Practice Statement For the Citizen and Commerce Class Common (C4) Certification Authority

13 September 2005

Table of Contents

1. INTRODUCTION

The Certification Practice Statement (CPS) for the C4CA is part four (4) of the FPKIA CPS and it documents the internal practices and procedures used by the Federal Public Key Infrastructure Architecture Operational Authority (FPKI OA) by describing the practices concerning lifecycle services in addition to issuance, such as certificate management (including publication and archiving), revocation, and renewal or re-keying.

This CPS covers the operation of systems and the management of facilities, which include three C4CAs and the Federal PKI Architecture common repository functionality, used for the purpose of authenticating citizens and commercial enterprises for many electronic services as established in the X.509 Citizen and Commerce Class Common Certificate Policy (C4CP).

The C4CA issues certificates to subordinate certificate providers, whose policies satisfy the C4CP requirements, and which, in turn, issue certificates to citizens and commercial entities. All certificates issued assert the OIDs specified in the Citizen & Commerce Certificate policy.

This CPS implements and complies with the requirements established in the C4CP, dated 22 December 2002.

This certification practice statement (CPS) is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework.

2. GENERAL PROVISIONS

The C4CA issues subordinate CA certificates, maintains and distributes certificate status information, and protects the private key(s) used to sign certificates and certificate status information.

Agreements with CAs subordinate to the C4CA require that subscribers of these CAs are to inform their CA if they believe their private key(s) have been compromised, stolen, or lost.

Relying parties determine whether or not certificates that satisfy this policy are appropriate for their application, and whether certificate status information need be verified before use.

2.1 LIABILITY

Transactions involving private citizens, businesses and government agencies are controlled by state, local and federal law. The Federal Tort Claims act defines the circumstances under which a federal agency may be held liable for the negligent acts of one (or more) of its employees. Negligent acts committed by businesses and individuals will be controlled by state and local law.

2.2 FINANCIAL RESPONSIBILITY

The C4CP contains no limits on the use of its certificates. Limits on financial liability should be established by the C4CA in advance of use of Certificates issued under this policy. In the absence of any such agreement, a financial limit of $500.00 is presumed.

2.2.1 Indemnification by relying parties

Under no circumstances will a federal agency agree to indemnify CAs subordinate to the C4CA issuing certificates under C4CP. CAs subordinate to the C4CA and their subscribers may reach their own agreements as to indemnification when interoperating with federal government entities.

2.2.2 Fiduciary relationships

Federal agencies agreeing to use these certificates do not have a fiduciary relationship with CAs operating under this policy. The existence of a fiduciary relationship (if any) between CAs subordinate to the C4CA and subscribers is determined by contract or agreement between those parties.

2.2.3 Administrative processes

Administrative processes agreed upon between the C4CA and the subscriber CA are memorialized in an agreement.

2.3 INTERPRETATION AND ENFORCEMENT

2.3.1 Governing law

This C4CP is interpreted under the principles used in construing federal agreements, grants and contracts as interpreted by the U.S. Court of Appeals for the Federal Circuit.

2.3.2 Severability, survival, merger, notice

Should it be determined that one section of the C4CP is incorrect or invalid, the other section of the C4CP shall remain in effect until the C4CP is updated.

2.3.3 Dispute resolution procedures

The FICC will resolve any disputes associated with the use of the C4CA or certificates issued by the C4CA.

2.4 COMPLIANCE AUDIT

The FPKI OA arranges initially and annually for independent inspections and compliance audits to validate that the C4CA is operating in accordance with the security practices and procedures described in this CPS. Results of the compliance audit is provided to the FPKIPA.

The C4CA compliance audits will be provided by an independent auditor as agreed between the FPKIPA and FPKI OA, which has demonstrated a proven track record and thoroughly familiar with the this CPS and the C4CP.

The FPKIPA has chosen the following organization to conduct the compliance audit:

Name of the Auditor Organization: KPMG

The selected auditor will verify and validate through document reviews and demonstrations that the C4CA complies with the C4CP and requirements that the FPKIPA imposes on the issuance and management of C4CA certificates.

The selected C4CA compliance auditor is a contractor that is independent from FPKI OA and the FPKIPA. This contractor provides an unbiased, independent evaluation and is one whose primary responsibility is the performance of EDP Compliance Audits.

Only prospective subordinate CAs submitting successful compliance audit result by a compliance auditor, which is organizationally independent from the owner of the prospective subordinate CA and qualified to audit CA processes, are allowed to apply for provisional or approved status. To maintain approved status, a CA subordinate to the C4CA needs to repeat the compliance audit process at least every three years.

2.5 CONFIDENTIALITY

Confidentiality requirements (if any) are determined by agreement between subscriber and CA.

3. IDENTIFICATION AND AUTHENTICATION

The C4CA will issue certificates with the following issuer DN:

c=us, o=U.S. Government, ou=FBCA, cn=C4 CA

The CA is responsible for authenticating the identity of the subject before certificate issuance. The identity of the subject must be stated in the common name attribute of the subject distinguished name. The identity may be established in any of the following manners:

(1) The identity may be established through in-person appearance at the credential provider, or its agent, with physical credentials (e.g., driver's license or birth certificate). Collection of certified mail is one example of in-person appearance at an agent of the credential provider.

(2) The identity may be established using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as:

- the ability to place calls from or receive phone calls at a given number; or
- the ability to obtain mail sent to a known physical address.

(3) Where an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, or retail company) exists, the identity may be authenticated through information derived from the business relationship such as:

- the ability to obtain mail at the billing address used in the business relationship; or
- verification of information established in previous transactions (e.g., previous order number) ; or
- the ability to place calls from or receive phone calls at a phone number used in previous business transactions.

The C4CA authenticates and issues certificates to subordinate CAs as described in SO01. Subordinate CAs are responsible for authenticating and issuing certificates to individuals.

The C4CA is responsible for ensuring the uniqueness of certificate subject names for all certificates issued by the C4CA. Under no circumstances are additional certificates containing the same subject name issued to a different subscriber (person, role, or organization). The FPKIPA apprises, in the issuance letter, the FPKI OA of the subject DN. SO01 describes the process the FPKI OA uses to verify the uniqueness of the DN and issue the certificate.

When a request to revoke a subordinate CA certificate is received, the FPKI OA authenticates the identity of the requester as described in SO02.

4. OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The C4CP requires that CAs that wish to become subordinate of the C4 root in the FPKIA under C4CP to follow the process described on http://www.cio.gov/fpkipa/index.htm

Following successful completion of the application process by a prospective applicant and its subsequent approval by the FICC, the FPKI OA performs the following steps upon request in order to issue a certificate to an applicant (using the information found in the issuance letter received from the Policy Authority):

- Establish the applicant's authorization (by the employing or sponsoring agency) to obtain a certificate.
- Establish and record identity of the applicant
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required
- Verify any role or authorization information requested for inclusion in the certificate.

These steps, performed in any order that is convenient for the FPKI OA and FPKI approved-applicants and does not defeat security, are completed before any subordinate CA certificate issuance. All communications among FPKI Authorities supporting the certificate application and issuance process is via an out-of-band secure mechanism.

4.2 CERTIFICATE ISSUANCE

The FPKI OA issues CA certificates to the certificate provider CAs by the following procedure:

- Upon receiving a signed request message (PKCS#10 message) from the CA, the C4CA software verifies the signature to prove possession of the private key. Then the C4CA will sign and issue a CA certificate to the CA.

- The certificate issued by the FCPF CA will be delivered to the certificate provider CA in a signed response message (PCKS#10), via secure non-electronic means (e.g., floppy disk delivered by registered mail or courier).

- Each CA certificate issued by the C4CA is manually checked to ensure each field and extension is properly populated with the correct information, before the CA certificate is delivered to the subordinate CA.

4.3 CERTIFICATE ACCEPTANCE

The MOA sets forth responsibilities of subordinate certificate provider CAs and the FPKIPA before the FPKIPA authorizes issuance of a C4CA subordinate CA certificate. Once a subordinate CA certificate has been issued, its acceptance by the certificate provider CA completes the insertion of the certificate provider in the list of approved providers. This triggers its obligations under the MOA and this CPS.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

CAs subordinate to the C4CA as well as the C4CA itself maintain and distribute certificate status information until certificate expiration. When a certificate status changes, the new status is published in the next CRL within 24 hours.

Certificate status information is distributed using X.509 CRLs.

4.5 SECURITY AUDIT PROCEDURES

The FPKI OA generates audit log files for all events relating to the security of the C4CA. 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. The security audit logs for each auditable event defined in this section are maintained as described in Section 4.6..

Auditable Event	FPKIA Directories		C4CA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
SECURITY AUDIT				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	✓			✓
Any attempt to delete or modify the Audit logs	✓ After a deletion following any archive operation	✓ After a modification following any archive operation		✓
IDENTIFICATION AND AUTHENTICATION				
Successful and unsuccessful attempts to assume a role		✓		✓
Change in the value of maximum authentication attempts	✓			✓
Maximum number of unsuccessful authentication attempts during user login		✓		✓
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	The account is immediately re-activated	The account is immediately re-activated		✓
An Administrator changes the type of authenticator, e.g., from password to biometrics	✓			✓
KEY GENERATION				

Auditable Event	FPKIA Directories		C4CA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
Whenever the FBCA-CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	Applies to CA only	Applies to CA only	✓	✓
PRIVATE KEY LOAD AND STORAGE				
The loading of Component private keys	Applies to CA only	Applies to CA only		✓
All access to certificate subject private keys retained within the FBCA CA for key recovery purposes	Applies to CA only	Applies to CA only		N/A - Implemented UniCERT version does not support Key Archival and Recovery
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	✓	✓
PRIVATE KEY EXPORT				
The export of private-keys (keys used for a single session or message are excluded)	Applies to CA only	Applies to CA only	✓	✓
CERTIFICATE REGISTRATION				
All certificate requests	Applies to CA only	Applies to CA only	✓	✓
CERTIFICATE REVOCATION				
All certificate revocation requests	Applies to CA only	Applies to CA only	✓	✓
CERTIFICATE STATUS CHANGE APPROVAL				
The approval or rejection of a certificate status change request	Applies to CA only	Applies to CA only	✓	✓
FBCA CA CONFIGURATION				
Any security-relevant changes to the configuration of the FBCA CA	Applies to CA only	Applies to CA only	✓	✓
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	✓		✓	✓
The access control privileges of a user account or a role are modified	✓		✓	✓
CERTIFICATE PROFILE MANAGEMENT				

Auditable Event	FPKIA Directories		C4CA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
All changes to the certificate profile	Cert Profile not captured in Directory	Cert Profile not captured in Directory	✓	
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile	Revocation Profile not captured in Directory	Revocation Profile not captured in Directory	✓	
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	✓	
MISCELLANEOUS				
Installation of the Operating System	✓		✓	✓
Installation of the FBCA CA	Applies to CA only	Applies to CA only	✓	✓
Installing hardware cryptographic modules	Applies to CA only	Applies to CA only	✓	
Removing hardware cryptographic modules	Applies to CA only	Applies to CA only	✓	
Destruction of cryptographic modules	Applies to CA only	Applies to CA only	✓	
System Startup	✓			✓
Logon Attempts to FBCA CA Apps	Applies to CA only	Applies to CA only		✓
Receipt of Hardware / Software	✓		✓	
Attempts to set passwords	✓			✓
Attempts to modify passwords	✓			✓
Backing up FBCA CA internal database	Applies to CA only	Applies to CA only		✓
Restoring FBCA CA internal database	Applies to CA only	Applies to CA only		✓
File manipulation (e.g., creation, renaming, moving)		✓		✓

Auditable Event	FPKIA Directories		C4CA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
Posting of any material to a repository		✓		✓
Access to FBCA CA-internal database	Applies to CA only	Applies to CA only	✓	✓
All certificate compromise notification requests	Applies to CA only	Applies to CA only	✓	
Loading tokens with certificates	Applies to CA only	Applies to CA only		✓
Shipment of Tokens	Applies to CA only	Applies to CA only	✓	
Zeroizing tokens	Applies to CA only	Applies to CA only	✓	✓
Rekey of the FBCA CA	Applies to CA only	Applies to C	✓	✓
Configuration changes to the CA server involving:	Applies to CA only	Applies to CA only		
Hardware	Applies to CA only	Applies to CA only	✓	
Software	Applies to CA only	Applies to CA only	✓	
Operating System	Applies to CA only	Applies to CA only	✓	✓
Patches	Applies to CA only	Applies to CA only	✓	✓
Security Profiles	Applies to CA only	Applies to CA only	✓	✓
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to room housing FBCA CA	✓	✓	✓	✓
Access to the FBCA CA server	Applies to CA only	Applies to CA only	✓	✓
Known or suspected violations of physical security	✓	✓	✓	
ANOMALIES				
Software Error conditions	✓	✓	✓	✓
Software check integrity failures	✓	✓	✓	✓
Receipt of improper messages	✓	✓	CA is	CA is

Auditable Event	FPKIA Directories		C4CA	
	Manual / Procedural	Automatic	Manual/ Procedural	Automatic
			stand alone	stand alone
Misrouted messages	✓	✓	CA is stand alone	CA is stand alone
Network attacks (suspected or confirmed)	✓	✓	CA is stand alone	CA is stand alone
Equipment failure	✓	✓	✓	✓
Electrical power outages	✓	✓	✓	✓
Uninterruptible Power Supply (UPS) failure	✓	✓	✓	✓
Obvious and significant network service or access failures	✓	✓	CA is stand alone	CA is stand alone
Violations of Certificate Policy	✓	Certain Violations as documented by this table	✓	Certain Violations as documented by this table
Violations of Certification Practice Statement	✓	Certain Violations as documented by this table	✓	Certain Violations as documented by this table
Resetting Operating System clock	✓		✓	

4.6 RECORDS ARCHIVAL

The FPKI OA Auditor produces archive records on a weekly basis. The records are stored on a removable storage medium (i.e., paper, tape, CD-ROM). The archive records include data received from the certificates and CRLs it generated, certificate requests and certificate revocation requests it received.

At initialization, the C4CA system equipment configuration files are archived, as well as the CPS and any contractual agreements to which the FPKI OA is bound.

4.7 KEY CHANGEOVER

The C4 CA key changeover procedures are as follows:

- The C4CA will generate a self-issued certificate signed by the old private key whose subjectPublicKeyInfo field contains the new public key.
- The C4CA will generate a self-issued certificate signed by the new private key whose subjectPublicKeyInfo field contains the old public key.

- The C4CA will generate a self-issued certificate signed by the new private key whose subjectPublicKeyInfo field contains the new public key.
- The C4CA and all subordinate CAs will process new CA certificates as described in this CPS.
- All certificates generated as part of the key changeover process will be posted to the FPKIA repository.
- The C4CA signing key has a validity period of three years, and its corresponding certificate has a validity period of six years.
- The C4CA will support subordinate CA key changeovers by issuing and posting new certificates as required.

4.8 COMPROMISE AND DISASTER RECOVERY

The C4CA and directory system is deployed so as to provide 24-hour, 365-day availability. The C4CA implements features to provide high levels of reliability as described in the following subsections.

The C4CA has recovery procedures in place to reconstitute the C4CA within 72 hours in the event of a catastrophic failure, as described in the following subsections.

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

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

- Notification of the GSA Designated Official For Facilities (DOFF) and Facility Emergency Response Team Leader (FERTL). These individuals along with the FPKI OA will assess the outage and determine whether all or part of the Recovery team needs to be assembled.
- Activation of the Damage Assessment and Disaster Recovery team.
- Based on the severity of the event, activate the recovery procedures for that severity type.
- Interface with the FPKI OA Management team.
- If the severity/scenario (to exceed 6 hours) of the event is critical, activation of the alternate site (hot site).
- The FPKIA POCs (“hot list”) will be notified of this change, so that any changes required by the subordinate CAs can be performed
- Manage the recovery process of the primary FPKIA facility.
- Submit post recovery logs to FPKIPA

In order to provide for rapid FCPF CA service re-activation, the FPKI OA implements a synchronized hot site. The hot site includes an identical configuration of the primary site. The FPKIA hot site online directory is updated by a running script that pulls the information from the primary site on a regular basis. The hot site offline C4CA will be quickly restored via backup tapes.

Certificates may 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
- Restoration Expense report

The PA will be notified as soon as possible.

4.8.2 CA Cannot Generate CRLs

If the C4CA cannot issue a CRL within 72 hours after the time specified in the next update field of its currently valid CRL, the FPKI OA will immediately inform the FPKIPA/FICC, as well as the shared service providers where appropriate.

4.8.3 CA Signature Keys are Compromised

If the C4CA signature keys are compromised or lost (such that compromise is possible even though not certain) the following procedure is executed:

- 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;
- The C4CA will generate a new C4 CA key pair in accordance with procedures set forth in section 4.2
- New C4CA certificates will be issued to CAs also in accordance with section 4.2.

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

4.8.4 Secure Facility Impaired after a Natural or Other Type of Disaster

In the case of a disaster whereby the C4CA primary installation is physically damaged and all copies of the C4CA signature key are destroyed as a result, the FPKIPA and all of its

subordinates will be securely notified (via callback and challenge-response), and the procedures described in section 4.8.1 will be followed. The C4CA installation will then be completely rebuilt, by reestablishing the C4CA equipment, generating new private and public keys, being re-certified, and re-issuing all subordinate shared service provider certificates. The details of this plan are defined in the FPKI OA BCCP and Disaster Recovery Procedures.

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

4.9 CA TERMINATION

C4CA will inform all the subordinate CAs and cross-certified CAs prior to planned termination or suspension of operations. Subordinate CAs will inform the C4CA prior to planned termination or suspension of operations. Details of termination are covered in the FPKIA Procedure SA09. If operations are disrupted by disaster or other unexpected events, FPKIA procedure DR01 – *Disaster Recovery Procedures* is implemented, including prompt notification to all affected parties.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

The FPKI OA uses trusted roles to augment procedural controls. A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The functions performed in these roles and the people selected to fill them form the basis of trust for the entire Federal PKI Architecture. 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. Also, role separation is enforced to ensure no one person is capable to manipulating multiple critical aspects the system.

The FPKIA encompasses CA products from several vendors implementing different certificate policies. Different commercial products support somewhat different roles, and use different mechanisms for registering or enrolling subscribers and issuing certificates; however, they can

all be re-conducted to the following somewhat abstract roles, derived from roles identified in the CIMC Protection Profile developed by NIST—

- *Administrator* – authorized to install, configure, and maintain the Operating Systems and Directory Software; establish and maintain Operating System user accounts; configure Operating System profiles and audit parameters; and generate component keys.

- *Security Officer* – authorized to request or approve certificates or certificate revocations; authorized to install, configure and maintain the CA software; 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.

The FPKIPA and the FPKI OA are responsible and accountable for the operation of the FPKIA.

The persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and are U.S. citizens. The procedures governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the FPKIA are described in the FPKIA SSP.

All FPKIA personnel hold TOP SECRET security clearances.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

C4CA uses RSA private keys with 1024 bits. Subordinate CAs and their subscribers use RSA or DSA private keys with 1024 bits or larger.

The C4CA private key(s) used to sign certificates and certificate status information are generated and maintained on the Chrysalis LunaSA cryptographic modules validated against FIPS 140-2 Level 3.

End Entity certificates issued to subordinate CAs subscribers under the C4CP are not required to include the key usage extension; if it appears, the *digitalSignature* bit must be asserted.

CA Certificates issued under the C4CP include the key usage extension. Certificates containing CA public keys that are used to verify certificates assert *keyCertSign*; certificates containing CA public keys that are used to verify CRLs assert *crlSign*.

Subscriber key pair generation is performed by the subscriber, using a FIPS approved method.

Public keys are delivered to the C4CA electronically in a certificate request (i.e., using PKCS #10) messages to the FPKI OA via secure non-electronic means (e.g., floppy disk delivered by

registered mail or courier) as described in section 4.2. Identity checking and proof of possession of the private key will be accomplished as described in section 4.2.

6.2 PRIVATE KEY PROTECTION

The C4CA private key(s) used to sign certificates and certificate status information are maintained in cryptographic modules validated against FIPS 140-2 Level 3.

The subordinate CAs private key(s) used to sign certificates and certificate status information are generated and maintained on the Chrysalis LunaSA cryptographic modules validated against FIPS 140 Level 2 (or higher).

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

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

The C4CA private signing keys will be used to sign certificates for one-half of the certificate lifetime (e.g. for 2 years if the certificate lifetime is 4 years). The certificate lifetime will be valid not more than 6 years. Rekeying will be performed after 3 years.

6.4 ACTIVATION DATA

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

Activation data is memorized, not written down. If written down, it is secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

Passwords are changed at least every 90 days to decrease the likelihood of discovery.

6.5 COMPUTER SECURITY CONTROLS

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal

Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

The FPKIA repository is operated on a dedicated workstation and will only run the network services required to operate the repository and to support on-line certificate validations (i.e., LDAP, DSP).

The C4CA server uses configurations that have been clearly demonstrated and passed the Compliance Audit process.

The C4CA equipment is configured with appropriate security features turned on as recommended by the host operating system vendor in accordance with any associated security validation rating.

6.6 LIFE CYCLE TECHNICAL CONTROLS

The initial configuration of the C4CA software (i.e., CA software, repository software) as well as any modifications and upgrades will be documented and controlled in accordance with FPKIA Configuration Management Procedures (separate FPKI OA document). System and application level logging will be enabled and reviewed weekly to maintain the ongoing integrity of the software and configuration.

6.7 NETWORK SECURITY CONTROLS

Text removed. This Information is 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” (GSA Order 1800.3b and Draft GSA Order 1800.3c), and therefore, in compliance with the Federal Information Security Management Act of 2002 (Title III of the E-Government 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, is omitted in the publicly universally available version of this document. Upon request, the complete CPS document is available to authorized organizations with a need to know.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

The description of the practice for cryptographic modules is stated above in Section 6.2.

7. CERTIFICATE AND CRL PROFILES

The C4CA issues X.509 version 3 certificates. Certificates contain RSA public keys of 1024 bits or larger. Certificates are signed using RSA, with Secure Hash Algorithm version 1 (SHA-1).

C4CAs distribute X.509 version 2 CRLs.

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

The Federal PKI Policy Authority reviews this CPS at least once every year.

8.2 PUBLICATION AND NOTIFICATION POLICIES

The redacted version of this CPS, the C4CP and any subsequent changes shall be made publicly available within one week of approval.

8.3 CPS APPROVAL PROCEDURES

This CPS is approved by the Federal PKI Policy Authority