Certificate Policy
for
Access Certificates for Electronic Services

U.S. General Services Administration

Federal Acquisition Service

May 12, 2017

Version 3.2

May 12. 2017

Signature Page

JEFFREY VOINER

Digitally signed by JEFFREY VOINER
DN: c=US, o=U.S. Government, ou=General Services Administration, cn=JEFFREY VOINER, 0.9.2342.19200300.100.1.1=47001002099614
Date: 2017.05.15 08:39:13 -04'00'

Program Manager, Access Certificates for Electronic Services DATE

RECORD OF CHANGES

Change Number	Section	Date	Current CP Version Changes
1.0	**3.1.2.6**	**9-13-05**	**9-13-05**
2.0	**All**	**3-04-08**	Update CP to conform to RFC 3647 and to address changes in FPCA CP and FPCPF
2.1	**All**	**1-21-09**	All FPCPF information placed in ***Notes***
2.2	**All**	**5-28-09**	Update CP to address comments to modifications in change numbers 2 and 3 (FPCPF information in *Notes* have now been removed to avoid confusion).
2.3	**1.1.3, 1.2, 1.3, 1.3.2, 1.4.1, 4.9.7, 5.3.1**	**10-2-09**	Update CP to address issues related to Federal Employee OIDs.
2.4		**12-27-10**	Update CP to include new OID and support for SHA-1 after 12/31/2010
2.5	**All**	**10-23-13** **3-27-14**	Update CP for compliance with latest FBCA CP and other latest policies and technologies Made it independent of FBCA CP and clarified role of ACES PMO Office
2.6	**1.2. 2.2.1, 5.5.4, 6.1.5, 6.3.2**	**8-18-14** **1-4-15**	Updates for first pass at FBCA CP mapping

2.7	**All**	**7-30-2015**	Added verification of RP, dropped unused policies, schedule, & C&A requirements and updates due to mapping
3.0	**All**	**12-23-2015**	Revised based on ACES Issuer comments, updated to remove GSA document references and replaced ATO with 800-53 references
3.1	**All**	**01-04-2017**	Remove government system language and fix disparate requirements identified during the ACES Vendor CPS review process. Integrate CAB Forum and trusted root program requirements. Clarify foreign national ID proofing requirements
3.2	**All**	**5-12-2017**	1) Remove separate Server Authentication Issuing CA requirement. 2) Removed term "Approved Relying Party". 3) Require test certificate websites for SSL certificates. 4) Removed remaining hardware certificate references

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF TABLES

1. INTRODUCTION

This Certificate Policy (CP) document defines the certificate policies for issuance and maintenance of public key certificates by authorized Certificate Authorities (CAs). The development of a National Information Infrastructure (NII) centered on the use of the Internet has the potential to:

- Improve citizen access to government services and information
- Reduce government operating costs through the implementation of electronic business processes.
- Facilitate secure e-commerce transactions in the private sector

Realizing these potential benefits will require the use of digital signatures to verify the identity of both senders and receivers of electronic messages, as well as the integrity of the messages themselves. Use of digital signatures requires the use of public key cryptography and public key certificates to bind an individual public key to an identity.

Because public key certificates and the systems that support their use are major prerequisites for expanding Federal use of the Internet, it is important to begin facilitating their implementation. In support of this goal, GSA's Federal Acquisition Service (FAS) has initiated projects aimed at providing commercial public key certificate services to the public (referred to as "Access Certificates for Electronic Services" or "ACES"). GSA will sign a Memorandum of Agreement (MOA) with service providers to make the services presented in this policy available.

Only CAs authorized to operate in accordance with this ACES CP and in an MOA signed with the GSA ACES PMO, shall assert the ACES CP Object Identifiers (OIDs) in the certificate policies extension of any certificates (Authorized ACES CAs).

ACES public key certificates are utilized by non-government individuals for authentication or submitting digitally signed artifacts to Federal, state, local, and other government entities (Relying Parties). Any use of or reference to this ACES CP outside of the purview of GSA FAS is completely at the using party's risk.

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

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

The use of SHA-1 to create digital signatures was deprecated beginning January 1, 2011[1]. There were SHA-1 specific policy OIDs defined in this CP for use between January 1, 2011 and December 31, 2013. SHA-1 certificates are no longer valid under this ACES CP.

[1] http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

1.1 OVERVIEW

1.1.1 Certificate Policy (CP)

ACES certificates 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 assurance level. The OID corresponds to a specific level of assurance for all ACES certificates issued under this CP, the CP is available to all Relying Parties. Each ACES certificate issued shall assert the appropriate certificate policy OID in the *Certificate Policies* extension.

This ACES CP is compliant with the following Trusted Root Program requirements:

1) Adobe Approved Trust List Technical Requirements version 1.4

While this ACES CP complies with Trusted Root Program requirements it does not imply ACES certificates are publicly trusted. The ACES root, Federal Common Policy CA, is enabled for specific key usages in each Trusted Root Program which may or may not align with certificate uses in this ACES CP. The ACES Policy Authority (GSA-ACES@gsa.gov) should be contacted with specific questions.

1.1.2 Relationship Between the ACES CP and the Authorized ACES CA's Certification Practice Statements (CPS)

The ACES CP states what assurance can be placed in a certificate issued by an Authorized ACES CAs. Each Authorized ACES CA shall provide a detailed Certification Practice Statement (CPS) that states how the Authorized ACES CA establishes that assurance in accordance with this ACES CP and the ACES MOA.

1.1.3 Scope

The ACES program exists to facilitate trusted electronic business transactions between Federal applications and non-Federal users. This ACES CP describes the following:

- Roles, responsibilities, and relationships among the CAs, Registration Authorities (RAs), Certificate Manufacturing Authorities (CMAs), Repositories, Subscribers, Relying Parties, and the Policy Authority (PA) (referred to collectively herein as "Program Participants") authorized to participate in the PKI described by this ACES CP
- The primary obligations and operational responsibilities of the Program Participants
- The rules and requirements for the issuance, acquisition, management, and use of ACES certificates to verify digital signatures

This ACES CP provides a high level description of the policies and operation of the ACES Program. Specific detailed requirements for the services outlined in this document may be found in each Authorized ACES CA's MOA and CPS.

1.2 DOCUMENT IDENTIFICATION

This Policy is registered with the Computer Security Objects Register (CSOR) at the National Institute of Standards and Technology (NIST), and has been assigned the object identifiers (OIDs) described in Table 1 for the ACES Certificates defined in this Policy.

All ACES certificates issued under this ACES CP shall reference the ACES CP by including the appropriate OID in the *Certificate Policies* extension of the ACES certificate. Only ACES OIDS may be used within ACES certificates, except as specifically authorized by this ACES CP.

ACES CP Description	NIST CSOR Description	Policy OID
ACES policy Arc	aces OBJECT IDENTIFIER	::= { csor-certpolicy 1 }
ACES policy OIDS	aces policy OBJECT IDENTIFIER	2.16.840.1.101.3.2.1.1
ACES Authorized ACES CA[2]	aces-ca OBJECT IDENTIFIER	2.16.840.1.101.3.2.1.1.1
ACES Unaffiliated Individual Certificates	aces-identity OBJECT IDENTIFIER	2.16.840.1.101.3.2.1.1.2
ACES Business Representative Certificates	aces-business-rep OBJECT IDENTIFIER	2.16.840.1.101.3.2.1.1.3
ACES Application SSL Server Certificates	aces-SSL OBJECT IDENTIFIER	2.16.840.1.101.3.2.1.1.5

Table 1. Object Identifiers

1.3 COMMUNITY AND APPLICABILITY

This ACES CP describes a bounded public key infrastructure. It describes the rights and obligations of persons and entities authorized under this ACES CP to fulfill any of the following roles:

- Certificate Service Provider
  - Certification Authority (CA)
  - Registration Authority (RA)
  - Certificate Manufacturing Authority (CMA)
  - Repository
- End Entity
  - Unaffiliated Individual
  - Business Representative
  - Device
  - State and Local Government

[2] ACES Authorized CA certificate OIDS may be included in certificates issued to subordinate CAs within and internal to the Authorized ACES CA's PKI.

  - Relying Party
- Policy Authority

Requirements for persons and entities authorized to fulfill any of the above roles are defined in this Section.

Additional obligations are set forth in other provisions of this ACES CP; and in the GSA ACES MOAs, including requirements of the CPS, System Security Plan (SSP), Privacy Practices and Procedures (PPP), and Subscriber Agreements.

1.3.1 ACES PKI Authorities

1.3.1.1 ACES Policy Authority

The GSA FAS serves as the Policy Authority and is responsible for organizing and administering the ACES CP. Additionally, the Policy Authority is responsible for managing the Authorized ACES CAs in accordance with the ACES MOA and the ACES CP and resolving name space collisions within the ACES program.

1.3.1.2 ACES Program Management

GSA FAS serves as the ACES Program Management Office (PMO) and is responsible for organizing and administering the ACES program and the ACES MOAs. The ACES PMO is the Policy Management Authority (PMA) for the ACES PKI. Additional responsibilities of the ACES PMO include:

1. Signing an MOA with the FPKIPA on behalf of the ACES program;
2. Sponsoring authorized ACES CAs for cross-certification with the FPKI; and
3. Ensuring all authorized ACES CAs are audited and operated in compliance with the ACES CP.
4. If new OIDs are required, the ACES PMO shall assign new OIDs to certificate policies as needed, and shall maintain control over the numbering sequence of OIDs within the ACES arc. The ACES PMO shall coordinate with NIST to keep the CSOR Public Key Infrastructure (PKI) Objects Registration up-to-date. Authorized ACES CAs requiring new OIDs shall submit a request to the ACES PMO.

1.3.1.3 Authorized ACES CAs

A CA may issue certificates that assert the policies defined in this ACES CP only if such CA first qualifies as an Authorized ACES CA by:

1. Entering into an appropriate MOA with the GSA ACES PMO;
2. Documenting the specific practices and procedures it will implement to satisfy the requirements of this ACES CP in an ACES CPS; and
3. Successful maintenance of cross-certification with the FBCA, under sponsorship of the ACES PMO.

Each Authorized ACES CA shall be responsible for all aspects of the issuance and management of ACES Certificates, including:

- The application/enrollment process
- The identification verification and authentication process
- The certificate manufacturing process
- Dissemination and activation of certificates
- Publication of certificates
- Renewal, suspension, revocation, and replacement of certificates
- Verification of certificate status upon request
- Generation and destruction of CA signing keys
- Ensuring that all aspects of the Authorized ACES CA services and Authorized ACES CA operations and infrastructure related to ACES Certificates issued under this ACES CP are performed in accordance with the requirements, representations, and warranties of this ACES CP.
- The Authorized ACES CA will submit to an annual PKI compliance audit of all operational aspects related to this ACES CP including all RA functions whether performed internally or by a third party.
- Assume responsibility of all CAs that validate to the Authorized ACES CA are compliant with this ACES CP.
- Assume responsibility of all contracted or subcontracted business operations of the Authorizes ACES CA.

The Authorized ACES CA shall be responsible for ensuring that all work is performed under the supervision of the Authorized ACES CA or responsible employees of the Authorized ACES CA, and shall provide assurance of the trustworthiness and competence of employees and their satisfactory performance of duties relating to provision of ACES services. Each Authorized ACES CA or employee of the Authorized ACES CA to whom information may be made available or disclosed shall be notified in writing by the Authorized ACES CA that information so disclosed to such Authorized ACES CA or employee can be used only for the purposes and to the extent authorized herein.

Authorized ACES CAs shall comply with all applicable Federal and GSA requirements, including those for the prevention and reporting of waste, fraud, and abuse set forth in the ACES MOA.

1.3.1.3.1 Cross-Certification with the FBCA

The Authorized ACES CA shall designate a CA within the Authorized ACES PKI to cross certify directly with the FBCA (e.g., through the receipt of a cross-certificate). The designated CA issues either end-entity certificates or CA certificates to other Authorized

ACES CAs, or both. Where the Authorized ACES CA operates a hierarchical PKI, the designated CA may be the ACES Issuer's root CA.

Authorized ACES CAs may request that the FBCA cross certify with more than one CA within their PKI, whether or not the Authorized ACES CA employs a hierarchical or other PKI architecture.

1.3.1.4 Certificate Status Servers

Authorized ACES CAs shall include Online Certificate Status Protocol (OCSP) responders to provide online, near real-time status information as current as the latest Certificate Revocation List. The OCSP responders may be provided on behalf of the Authorized ACES CA as a Certificate Status Server (CSS), where the CSS is identified in certificates as an authoritative source for revocation information (i.e., authority information access [AIA] certificate extension). The OCSP CSSs identified in certificates issued by Authorized ACES CA CSSs are within the scope of this ACES CP.

1.3.2 Registration Authorities (RAs)

Each Authorized ACES CA shall perform the role and functions of the RA. An Authorized ACES CA may subcontract RA functions to third party and/or trusted agent RAs who meet trustworthiness requirements and agree to be bound by this ACES CP. The Authorized ACES CA CPS shall identify the parties responsible for providing such services and the mechanisms for determining their trustworthiness. The Authorized ACES CA remains responsible for the performance of those services in accordance with this ACES CP and the GSA ACES MOA.

The RA is responsible for applicant registration, certificate application, and authentication of identity functions for Unaffiliated Individuals, Business Representatives, and Servers. An RA may be also responsible for handling suspension and revocation requests, and for aspects of Subscriber education.

The Authorized ACES CA shall ensure audits include all RA functions whether performed internally or by a third party.

1.3.3 Subscribers[3]

A Subscriber is the entity whose name appears as the subject in a certificate. A subscriber asserts that the key and certificate are used in accordance with the certificate policy and key usage asserted in the certificate. An Authorized ACES CA may issue ACES certificates to the following classes of Subscribers:

- Members of the general public (Unaffiliated Individuals)
- Individuals authorized to act on behalf of business entities (i.e., Sponsoring Organizations) recognized by the Authorized ACES CA, such as employees, officers, and agents of a Sponsoring Organization (Business Representatives)

[3] CAs are sometimes technically considered "subscribers" in a PKI; however, the term "subscriber" as used in this ACES CP dos not refer to CAs.

- Application Servers

The Government has the right to add authorized users at any time during the term of this ACES CP.

1.3.4 Relying Parties

A Relying Party uses a Subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. 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 Relying Party is responsible for deciding how to configure their application for trusted roots but the ACES program relies on the Federal Common Policy CA as the ACES Root CA.

This CP makes no assumptions or limitations regarding the identity of all Relying Parties. While Relying Parties are generally Subscribers, Relying Parties are not required to have an established relationship with the GSA or an Authorized ACES CA. However, ACES Relying Parties are those persons and entities authorized to sponsor, accept and rely upon ACES Certificates for purposes of authentication and verifying digital signatures on electronic records and messages. Government operated applications wishing to accept ACES Certificates agree to be bound by the terms of this Policy.

1.3.5 Other Participants

The Authorized ACES CAs may require the services of other security, community, and application authorities. The Authorized ACES CA CPS shall identify the parties, define the services, and designate the mechanisms used to support these services.

1.3.5.1 Certificate Manufacturing Authorities (CMAs)

A CMA is responsible for the functions of manufacturing, issuance, suspension, and revocation of ACES certificates.

Each Authorized ACES CA shall perform the role and functions of the CMA. An Authorized ACES CA may subcontract CMA functions to third party CMAs who agrees to be bound by this ACES CP, but the Authorized ACES CA remains responsible for the performance of those services in accordance with this ACES CP and the GSA ACES MOA.

1.3.5.2 Repositories

Each Authorized ACES CA shall perform the role and functions of the Repository, as described in Section 2.1.1, Repository Obligations. An Authorized ACES CA may subcontract performance of the Repository functions to a third party Repository who agrees to be bound by this ACES CP, but the Authorized ACES CA remains responsible

for the performance of those services in accordance with this Policy and the requirements of its GSA ACES MOA.

1.3.5.3 Application Servers

Authorized ACES CAs may issue certificates to Government Agency's or Organizations running servers for various purposes as described below.

1.3.5.3.1 ACES Secure Sockets Layer (SSL) Server Certificates

Authorized ACES CAs may issue ACES SSL Server Certificates for use on Application Servers to allow mutual authentication and/or trusted SSL communications between citizens and government Agencies. After December 31, 2015, the Fully Qualified Domain Name of the Web server shall be contained in the subjectAltName extension of these certificates.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Subscribers and Relying Party Applications may use ACES digital signature certificates to mutually authenticate Subscribers and Relying Party Applications. Subscribers and Applications servers may use ACES encryption certificates to enable the confidentiality service on the data exchanged.

The sensitivity of the information processed or protected using certificates will vary significantly. Relying Parties must evaluate the environment and 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 Relying Party for its application and is not controlled by this ACES CP.

ACES Unaffiliated Individual certificates, where the issuance of the certificate is based only on remote verification of identity (i.e., online registration with no "in-person" verification of identity prior to issuance) may be used at a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.

All ACES certificates, where the issuance of the certificate is based on "in-person" verification of identity prior to issuance, are intended to be used at the medium level of assurance relevant to environments where risks and consequences of data compromise are moderate. All ACES certificates are software certificates. This may include transactions having substantial or very high monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

Table 2 summarizes the functional uses of ACES certificates.

ACES Certificate Type	Subscriber	Purpose	Use of Certificate
ACES Authorized ACES CA certificates	ACES Authorized ACES CAs and subordinate CAs	Establish and generate the CA certificates	To establish and verify the trust relationship of the issuing CA with the certificates it issues. To enable the Authorized ACES CA to issue Subscriber certificates and to issue certificates to subordinate CAs within an Authorized ACES CA PKI.
Unaffiliated Individual Certificate (Basic and Medium)	Unaffiliated Individual	Digital Signature	To enable an Unaffiliated Individual ACES Subscriber and Relying Parties to mutually authenticate themselves electronically for information and transactions and to verify digitally signed documents/transactions
		Encryption	To enable an Unaffiliated Individual ACES Subscriber to use confidentiality services (encryption and decryption) on his/her information and transactions
		Authentication	To enable an Unaffiliated Individual ACES Subscriber to use identity and token authentication services
Business Representative Certificate (Medium Assurance)	Business Representative authorized to act on behalf of a Sponsoring Organization	Digital Signature	To enable a Business Representative to mutually authenticate themselves to conduct business-related activities electronically and to verify digitally signed documents/ transactions
		Encryption	To enable a Business Representative to use confidentiality services (encryption and decryption) on his/her information and transactions
		Authentication	To enable a Business Representative ACES Subscriber to use identity and token authentication services
ACES SSL Server Certificate	Server	Authentication and Encrypted Data Transmission	To enable authenticated encrypted communications between Subscribers and servers
FBCA Cross-Certificate	N/A	Authentication of FPKI certificates	To enable mutual authentication with the FPKI Note: no longer required after December 2015.

Table 2. Functional Uses of ACES Certificates

This ACES CP is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statutes and regulations.

Authorized ACES CAs shall, at a minimum, issue ACES Business Representative Certificates.

1.4.2 Prohibited Certificate Uses

Certificates that assert ACES policy OIDs should not be used in a manner inconsistent with the usages specified in the key usage and extended key usage extensions of the certificate, or in a manner inconsistent with the subscriber agreement.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

GSA FAS (as the Policy Authority and MOA Authority) administers this ACES CP:

Federal Acquisition Service
General Services Administration
18th and F Streets, NW
Washington, DC 20405-0007

1.5.2 Contact Person

Questions regarding this CP shall be directed to:

Attn.: Jeffrey Voiner, Federal Acquisition Service
Phone: 571-970-7006

1.5.3 Person Determining CPS Suitability for the ACES CP

The CPS must conform to this ACES CP. GSA FAS is responsible for ensuring that the CPSs of Authorized ACES CAs conform to the ACES CP and ACES MOAs. Questions regarding suitability of the CPSs shall be directed to:

Attn: Jeffrey Voiner
ACES Program Manager
Federal Acquisition Service
General Services Administration
Telephone: 571-970-7006
Email address: Jeffrey.Voiner@GSA.gov

The determination of suitability of a CPS shall be based on verification of compliance with the ACES CP by an independent, trusted third-party, including results of the verification process and recommendations. See Section 8, Compliance Audits and Other Assessments, for further details.

1.5.4 CPS Approval Procedure

The CPS and the results and recommendations of the independent, trusted third-party shall be submitted to the ACES Program Manager for approval. Authorized ACES CAs shall comply with all requirements of this ACES CP.

The CA and RA must meet all requirements of an approved CPS before commencing operations.

1.6 DEFINITIONS AND ACRONYMS

See Sections 11 and 12.

2. PUBLICATION & REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Authorized ACES CAs shall operate and maintain public repositories to support their PKI operations.

2.1.1 Repository Obligations

A Repository is responsible for maintaining a secure system for storing and retrieving currently valid ACES Certificates, a current copy of this ACES CP and other information relevant to ACES Certificates, and for providing certificates status services for a Relying Party.

The Repository shall implement access controls to prevent unauthorized modification or deletion of information.

Authorized ACES CAs may post certificates and CRLs in additional replicated repositories for performance enhancements. Such repositories may be operated by the Authorized ACES CA or other parties (i.e., state agencies).

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

All CA and subscriber certificates issued by Authorized ACES CAs shall only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties.

Each Authorized ACES CA shall operate a secure online Repository available to Subscribers and Relying Parties that shall have the capability to contain:

- Currently valid ACES Certificates issued by the Authorized ACES CA that have been accepted by the Subscriber
- Certificate Revocation List (CRL) and online certificate status information
- CA certificates issued to and by the Authorized ACES CA
- Other relevant information about ACES certificates

All information to be published in the Repository shall be published immediately after such information is available to the Authorized ACES CA. The Authorized ACES CA will publish ACES certificates immediately upon acceptance of such ACES certificates.

Authorized ACES CA certificates, CRLs, and online certificate status information shall be available for retrieval 24 hours a day, seven days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually.

2.2.2 Publication of CA Information

The following CA information shall be published and publicly available:

- Copy of this ACES CP
- Past and current versions of the Authorized ACES CA's ACES CPS (may be redacted)
- Other information related to the Authorized ACES CA (i.e., FBCA Cross-Certification)
- Annual PKI Compliance Letter
- WebTrust Audit Seals, if applicable
- If the Authorized ACES CA issues ACES SSL Certificates, it shall host test Web pages that allow Application Software Suppliers to test their software with ACES SSL Certificates that chain up to the ACES Root Certificate. At a minimum, the Authorized ACES CA shall host separate Web page, using ACES SSL Certificates, that are (i) valid, (ii) revoked, and (iii) expired. The ACES SSL certificates may be issued to a ".com" or other top level domain for test purposes only.

2.2.3 Interoperability

Authorized ACES CAs shall ensure interoperability with the FBCA Repository

2.3 FREQUENCY OF PUBLICATION

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

Publication requirements for CRLs are provided in Section 4.9 of this ACES CP, Certificate Revocation and Suspension.

2.4 ACCESS CONTROLS ON REPOSITORIES

The Authorized ACES CA shall make publicly available and not impose any access controls on this ACES CP, all CA certificates issued to and by the Authorized ACES CA, and past and current versions of the Authorized ACES CA's CPS (may be redacted), as well as published subscriber certificates and certificate status information.

At a minimum, the Authorized ACES CA repository shall make all current CA certificates and CRLs issued by the CA and CA certificates issued to the CA available to Relying Parties.

For Authorized ACES CAs, the CPS shall detail what information in the repository shall be exempt from automatic availability, and shall also specify to whom, and the conditions under which, the restricted information may be made available.

The Authorized ACES CA shall impose access controls to ensure authentication of Subscribers with respect to their own certificate(s) and personal registration information

that is separately managed from the public certificate and status Repository. These controls shall ensure appropriate protection of all personally identifiable information collected in support of issuance of ACES certificates.

3. IDENTIFICATION & AUTHENTICATION

3.1 NAMING

Authorized ACES CAs shall be able to generate and sign certificates that contain an X.500 Distinguished Name (DN); the X.500 DN may also contain domain component elements. Where DNs are required, subscribers shall have them assigned through the Authorized ACES CAs.

3.1.1 Types of Names

All certificates issued by Authorized ACES CAs shall include a non-NULL subject Distinguished Name (DN) and optional Subject Alternative Name, if marked non-critical, and shall follow the naming requirements at the FBCA medium level of assurance.

3.1.1.1 ACES Unaffiliated Individual Digital Signature and Encryption Certificates

The subject name used for ACES Unaffiliated Individual digital signature and encryption certificates shall contain the Subscriber's authenticated common name and optional Subject Alternative Name, if marked non-critical.

3.1.1.2 ACES Business Representative Digital Signature and Encryption Certificates

Certificates shall assert X.500 Distinguished Name, and optional Subject Alternative Name if marked non-critical.

ACES Business Representative certificates shall assert a name form, subject to requirements set forth below intended to ensure name uniqueness.

3.1.1.3 ACES SSL Server Certificates

Certificates shall assert X.500 Distinguished Name of the server including the identification of the organization and organizational unit sponsoring the server. Additionally, the distinguished name shall assert the registered and verified fully qualified domain name of the server as a Subject Alternative Name and optionally as the common name of the subjectDN. In addition, ACES SSL certificates shall conform to the following:

- The extendedKeyUsage extension shall assert the serverAuthentication value and

shall not assert the anyEKU.

- The *SubjectAltName* field shall contain a *dNSName* containing a Fully Qualified Domain Name (FQDN) of a server;

- Internet Protocol (IP) Addresses shall not be included in the *SubjectAltName* field;

- Wildcard Domain Names are permitted if all sub-domains covered by the wildcard fall within the same application, cloud service, or system accreditation boundary within the scope of the sponsoring Organization.

- Wildcards shall not be used in subdomains that host more than one distinct application platform. The use of third-level Organization wildcards, (e.g., *.[organization].com or *.[agency].gov), shall be prohibited to reduce the likelihood that a certificate will overlap multiple systems or services. Third level wildcards are permitted for DNS names dedicated to a specific application (e.g., *.[application_name].com or *.[application_name].gov).

Before issuing an ACES SSL certificate containing a wildcard, the CA shall ensure the sponsoring organization has a documented procedure for determining that the scope of the certificate does not now and will not infringe on other application servers.3.1.2 Need for Names to Be Meaningful

Names used in the certificates must identify the person or object to which they are assigned in a meaningful way, as provided in Table 3.

ACES Certificate Description	Name Meanings
Authorized ACES CA Digital Signature Certificates	Authorized ACES CAs shall implement the name constraint extension of the X.509 version 3 certificate profile in issuing CA certificates.
ACES Unaffiliated Individual Digital Signature and Encryption Certificates	The authenticated common name should be a combination of first name, middle name and/or initial, and surname.
ACES Business Representative Digital Signature and Encryption Certificates	The authenticated common name should be the combination of first name, middle name and/or initial, and surname and the legal name of the organization and/or unit should also be contained in the DN.
ACES SSL Certificates	The authenticated FQDN shall be included in a SAN The subject DN common name may also contain the authenticated registered domain name of the Application server. .

Table 3. Naming Conventions

When DNs are used, the directory information tree must accurately reflect organizational structures.

When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading. Authorized ACES CAs may supplement any of the name forms for users by including a dnQualifier, serial number, or user id attribute. When any of these attributes are included, they may appear as part of a multi-valued relative distinguished name (RDN) with the common name or as a distinct RDN that follows the RDN containing the common name attribute in order to ensure name space uniqueness requirements are met.

This does not preclude the use of pseudonyms as defined in Section 3.1.3.

3.1.3 Anonymity or Pseudonymity of Subscribers

ACES CAs shall not issue anonymous certificates. Pseudonymous certificates may be issued by ACES CAs to support internal operations. CA certificates issued by ACES CAs shall not contain anonymous or pseudonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting email addresses are specified in RFC 2822 The ACES PMO is responsible for Authorized ACES CA name space control.

3.1.5 Uniqueness of Names

Name uniqueness across the ACES Program must be enforced. Authorized ACES CAs and RAs shall enforce name uniqueness within the X.500 name space for which they have been authorized. When other name forms are used, they too must be allocated such that name uniqueness is ensured. Name uniqueness is not violated when multiple certificates are issued to the same entity.

Authorized ACES CAs shall document, in their respective CPSs, how they will assign subject names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if Joe Smith leaves a CA's community of Subscribers, and a new, different Joe Smith enters the community of Subscribers, how will these two people be provided unique names?).

For distinguished names, name uniqueness is applicable for the entire name rather than a particular attribute.

At a minimum, name uniqueness within an Authorized ACES CA, including subordinate CAs, shall be ensured through a combination of certificate serial number, common name, and Authorized ACES CA issuing the certificate.

The ACES PMO is responsible for ensuring name uniqueness in certificates issued by the Authorized ACES CA.

3.1.6 Recognition, Authentication, and Role of Trademarks

A corporate entity is not guaranteed that its name will contain a trademark if requested. The Authorized ACES CA shall not knowingly issue a certificate including a name that a court of competent jurisdiction has determined infringes the trademark of another. It is not subsequently required to issue that name to the rightful owner if it has already issued one sufficient for identification. An Authorized ACES CA shall not be obligated to research trademarks or resolve trademark disputes.

The ACES PMO is responsible for providing the Authorized ACES CA support in resolving disputes involving names and trademarks.

3.2 INITIAL IDENTITY VALIDATION

The ACES program is operated for the benefit of the government. It is critical to understand the scope of the program and who relies on ACES credentials. Authorized ACES CAs shall maintain a list of ACES Relying Party Applications and up to date contact information for authorized personnel supporting those applications. Before issuing an ACES certificate, the Authorized ACES CA or RA will require the Subscriber to identify at least one Relying Party application that requires an ACES certificate. If the Subscriber identified Relying Party application is not on the current list of ACES Applications, the Authorized ACES CA or RA shall contact the RP and verify it has a government sponsor and a need for ACES certificates, prior to issuing the subscriber requested ACES credential. The newly identified RP shall be added to the monthly report to the ACES PMO.

3.2.1 Method to Prove Possession of Private Key

In all cases where the subject named in a certificate generates its own keys, that subject shall be required to prove possession of the private key that corresponds to the public key in the certificate request.

For signature keys, this may be done by the Subscriber using its private key to sign a value and providing that signed value to the Authorized ACES CA. The Authorized ACES CA shall then validate the signature using the Subscriber's public key.

The Authorized ACES CA CPS shall specify the mechanisms for proving possession of the private key.

In the case where key generation is performed by the Authorized ACES CA or RA either (1) directly on the Subscriber's hardware or software token, or (2) in a key generator that benignly transfer the key to the party's token, then proof of possession is not required.

3.2.2 Authentication of Sponsoring Organization Identity

If the applicant is requesting an ACES Business Representative or SSL Certificate, in addition to verifying the applicant's individual identity and authorization to represent the Sponsoring Organization, the Authorized ACES CA shall also verify the Sponsoring Organization's current operating status. In conducting its review and investigation, the

Authorized ACES CA shall provide validation of information concerning the Sponsoring Organization, including legal company name, type of entity, address (number and street, city, ZIP code), and telephone number using one of the following methods:

1) Communication with a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition.
2) A third party database that is periodically updated and provides identity verification as a main source of business operations.
3) A site visit by the CA or a third party who is acting as an agent of the CA; or
4) An Attestation Letter
5) Or other methods approved by the ACES PMO

3.2.3 Authentication of Individual Identity

If the applicant passes identity proofing verification as specified in the following sections of this ACES CP, Authorized ACES CA shall, at a minimum, record the following transaction data:

- Applicant's name as it appears in the certificate's Common Name field
- Method of application (i.e., online, in-person)
- For each data element accepted for proofing, including electronic forms:
    - Name of document presented for identity proofing
    - Subscriber Identified Relying Party Application
    - Issuing authority
    - Date of issuance
    - Date of expiration
    - All fields verified
    - Source of verification (i.e., which databases used for cross-checks)
    - Method of verification (i.e., online, in-person)
    - Date/time of verification
- Identity of the person performing the verification
- All associated error messages and codes, if any
- Date/time of process completion
- A unique identifying number from the ID of the verifier and from the ID of the applicant.

If the applicant fails identity proofing verification performed by the Authorized ACES CA, the Authorized ACES CA shall notify the applicant of the verification failure via out-of-band notification process linked to the certificate applicant's physical postal address.

The Authorized ACES CAs and/or RAs shall ensure that the applicant's identity information and public key are properly bound.

The subscriber must identify at least one Relying Party application for which the ACES certificate is required at the time of application. This information shall be recorded with the Subscriber's application package. The Authorized ACES CA shall report certificate issuances per Relying Party to the GSA ACES PMO on a monthly basis.

If an applicant is unable to perform face-to-face registration alone, the applicant may be represented by a trusted person already issued a digital certificate by the Authorized ACES CA. The trusted person will present information sufficient for registration at the level of the certificate being requested by the applicant, for both himself/herself and the applicant who the trust person is representing.

An entity certified by a State or Federal organization as being authorized to confirm identities may perform in-person authentication of identity as a Trusted Agent RA, or on behalf of the RA. The certified entity forwards the information collected from the application directly to the Authorized ACES CA or RA for verification of the information a secure manner. If the Trusted Agent performs all or part of the verification of identity, that information shall also be forwarded directly to the ACES CA or RA. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement. Other secure methods may also be acceptable, as approved by the ACES Program Manager.

For human subscribers, this ACES CP allows a certificate to be issued only to a single entity. Certificates shall not be issued that contain a public key whose associated private key is shared.

Only an Authorized ACES RA or US Consular Notary are approved to perform identity proofing for individuals applying for ACES certificates outside the United States.

3.2.3.1 Authentication of Human Subscribers

Authentication of the identity of human subscribers shall be established no more than 30 days before initial certificate issuance.

3.2.3.1.1 Authentication of ACES Unaffiliated Individual Digital Signature and Encryption Certificates

ACES Unaffiliated Individual Digital Signature and Encryption Certificates may be authenticated through an electronically submitted application or by personal presence. In accordance with this ACES CP, the Authorized ACES CA shall verify all of the following identification information supplied by the applicant: first name, middle initial, last name, current address (number and street, city, ZIP code), and home or cellular telephone number.

Applicant identification must be confirmed via an identity-proofing process that incorporates the following factors:

- Submission by the applicant of at least three individual identity items, which must be verified through reference to multiple independent data sources along with cross-checks for consistency, for example:
    - Currently-valid credit card number

  - Alien Registration Number
  - Passport Number
  - Current employer name, address (number and street, city, ZIP code), and telephone number
  - Currently valid state-issued driver's license number or state-issued identification card number
  - Social Security Number
  - Date of birth
  - Place of birth.

- At least one of the above data sources must be based on an antecedent in-person or the equivalent identity verification process, when the application is electronically submitted.
- The use of an out-of-band notification process that is linked to the requesting individual's physical U.S. postal mail address.
- Verification of any additional information contained in the Certificate Application

3.2.3.1.2 Authentication of ACES Business Representative Digital Signature and Encryption Certificates

For ACES Business Representative Digital Signature and Encryption Certificates, identity shall be established by in-person appearance before the Registration Authority or Trusted Agent. Information provided shall be checked to ensure its legitimacy. Credentials required are either one Federal Government-issued Picture I.D., or two non-Federal Government IDs, one of which shall be a photo ID (e.g., a Drivers License).

The Business Representative's identity must be personally verified prior to the certificate being enabled. The applicant shall appear personally before either:

- An Authorized ACES CA
- A trusted Agent or RA approved by the Authorized ACES CA or appointed by name in writing by the Authorized ACES CA
- A person certified by a State or Federal Government as being authorized to confirm identities (such as Notaries Public), who uses a stamp, seal, or other mechanism to authenticate their identity confirmation.
- A US Consular Notary if located outside the United States.

The Authorized ACES CA, RA or Trusted Agent shall verify:

- That the applicant is a duly authorized representative of the Sponsoring Organization as an employee, partner, member, agent, or other association, and
- The Sponsoring Organization's identity as specified in Section 3.2.2

In addition to the requirements for recording transaction data listed above, in Section 3.2.3.1, the process documentation and authentication requirements for ACES Business Representative certificate applicants shall include the following:

- As required by this ACES CP, A signed declaration (by the Authorized ACES CA, RA, or Trusted Agent) that the identity of the Subscriber has been verified, which may be met by establishing how the applicant is known to the verifier
- A declaration of identity signed by the applicant using a handwritten signature; performed in the presence of the individual performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law

The applicant shall personally appear before one of the required identity verifiers at any time prior to application of the Authorized ACES CA's signature to the applicant's certificate, or alternatively, when private keys are delivered to Subscribers via hardware tokens.

3.2.3.2 Authentication of Devices

Some computing and communications components will be named as certificate subjects. In such cases, the component must have a human sponsor who is affiliated with the agency or organization under which the certificate is being issued. The PKI sponsor is responsible for providing the following registration information:

- Registered domain name or IP address
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor using a certificate of equivalent or greater assurance than that being requested (i.e., Medium)
- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1.2

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

For each Fully-Qualified Domain Name listed in an ACES SSL certificate, the CA shall confirm and maintain documented evidence that, as of the date the Certificate was issued, the Sponsor's organization has control over the FQDN and the sponsor is authorized to request the certificate.

Each organization shall have a naming policy for devices that receive an ACES SSL certificate that specifies unique meaningful FQDN names and the CPS shall document how the CA ensures compliance with the sponsoring organization's policy.

Note: FQDNs shall be listed in ACES SSL certificate using dNSNames in the subjectAltName extension and cannot contradict Name Constraints in the issuing CA certificate.

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the CA shall establish and follow a documented procedure to ensure that the wildcard does not fall immediately to the left of an agency or organization name, but is qualified down to a unique application, server, or server farm under control of the sponsor's organization. The device sponsor shall demonstrate that the domain name requested is entirely within the name space to be covered by the wildcard certificate. All requests for device certificates shall be digitally signed by the sponsor.

3.2.3.3 Other Certificates

Nothing in this policy prohibits the GSA ACES PMO from approving production of other certificate types to meet specific needs of participating agencies.

3.2.4 Non-verified Subscriber Information

Subscriber information that is not verified shall not be included in the ACES certificates.

3.2.5 Validation of Authority

Before issuing ACES certificates that assert organizational authority (i.e., Business Representative or SSL certificates), the Authorized ACES CA shall validate the individual's authority to act in the name of the organization.

In accordance with section 3.2.3.2, all requests for device certificates in the name of an organization, shall be digitally signed by the sponsor using a certificate of medium assurance or higher that validates to the ACES Root CA (Federal Common Policy CA). In addition, the CPS shall specify a process by which an organization identifies the individuals who may request certificates that assert organizational authority. If an organization specifies, in writing, the individuals who may request a certificate, then the CA shall not accept any certificate requests that are outside this specification. The CA shall provide an Applicant with a list of the organization's authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for Interoperation

Compliance with this CP and cross-certification with the FBCA enable interoperation with the Federal Public Key Infrastructure. The GSA ACES PMO shall provide oversight of Authorized ACES CAs, by approving the Authorized ACES CA's CPS and supporting documentation.

The MOAs between the GSA ACES PMO and Authorized ACES CAs and between the GSA ACES PMO and the FPKIPA ensure interaction and interoperability with Authorized ACES CAs, authorized Federal Government agencies, and non-government CAs.

3.3 IDENTIFICATION & AUTHENTICATION FOR RE-KEY AND RENEWAL

3.3.1 Identification and Authentication for Routine Re-Key

When an Authorized ACES CA updates its private signature key and thus generates a new public key and certificate, the Authorized ACES CA shall notify the ACES PMO, RAs, and Subscribers, indicating that the CA's public certificate has been changed, in addition to publishing the certificate in the repository and making it publicly available.

Subscribers of Authorized ACES CAs shall identify themselves for the purpose of re-keying through use of their current signature key, except that identity shall be established through initial registration process described in Section 3.2 at least every nine years.

Subscribers' signature private keys and certificates have a maximum lifetime of three years. Subscriber encryption certificates have a maximum lifetime of three years; use of subscriber decryption private keys is unrestricted.

3.3.2 Identification and Authentication for Renewal

Authorized ACES CAs shall accept ACES Certificate renewal requests from their Subscribers within 90 days from the scheduled end of the operational period (expiration date) of the ACES Certificate, provided the ACES Certificate is not revoked, suspended, or expired. ACES Certificates may be renewed in one, two, and up to three-year increments.

Authorized ACES CAs shall authenticate the Subscriber's renewal request using the Subscriber's current signature key for authentication in the renewal process. In the event that subject information and/or the key pair changes, the Authorized ACES CA shall require the Subscriber request a new ACES Certificate. The old certificate (as a result of an update action) may or may not be revoked, but must not be further re-keyed or renewed.

Authorized ACES CAs shall verify the Subscriber has a need to continue to interact with at least one ACES Relying Party Application.

3.3.3 Identification and Authentication for Re-key after Revocation

After a certificate has been suspended, revoked or expired, the applicant is required to go through the initial registration process as described in Section 3.2.

3.4 IDENTIFICATION & AUTHENTICATION FOR REVOCATION REQUEST

Authorized ACES CAs shall provide for the revocation of certificates when requested, at any time and for any reason.

An ACES Certificate revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the ACES Certificate's associated key pair. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised. The identity of the person submitting a revocation request in any other manner shall be authenticated in accordance with Section 4.9. Other revocation request authentication mechanisms may be used as well, including a request in writing signed by the Subscriber and sent via U.S. Postal Service first-class mail, or equivalent.

These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to quickly revoke certificates.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

This section specifies requirements for initial application for certificate issuance.

4.1.1 Application Initiation

The following persons may initiate the ACES Certificate application process:

Potential Subscriber	Authorized Initiator
Unaffiliated Individual	Potential Subscriber only
Business Representative	Sponsoring Organization or potential Subscriber
ACES SSL Server	Sponsor responsible for the component receiving the certificate

Table 4. ACES Certificate Application Process Initiators

4.1.2 Enrollment Process and Responsibilities

Applications for ACES Certificates may be communicated from the applicant to an Authorized ACES CA or an authorized RA, and authorizations to issue ACES Certificates may be communicated from an authorized RA to an Authorized ACES CA:

- Electronically, provided that all communication is secure

- By U.S. Postal Service first-class mail
- In person

All electronic transmissions and communications supporting application and issuance processes shall be authenticated and protected from unauthorized access and modification.

4.1.2.1 Applicant Education and Disclosure

Before enabling the certificates for use by the subscriber (i.e., at application or at acceptance), the Authorized ACES CA shall inform applicants of the advantages and potential risks associated with using ACES Certificates to access Relying Parties electronically, and provide information to Subscribers regarding the use of private keys and digital signatures or encrypted messages created with such keys, and Subscriber obligations as specified in Section 9.6.3.

4.2 CERTIFICATE APPLICATION PROCESSING

An applicant for an ACES Certificate shall complete an ACES Certificate application and provide requested information in a form prescribed by the Authorized ACES CA and this ACES CP. Information in the certificate application shall be verified as accurate before certificates are issued as specified in Section 3.2.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the Subscriber shall meet the requirements specified for Subscriber authentication in Sections 3.2 and 3.3. The components of the Authorized ACES CAs responsible for authenticating the Subscriber's identity in each case are specified in Section 1.3. For CAs that issue ACES SSL certificates, the CPS shall state the CA's practice on processing Certification Authority Authorization (CAA) DNS Resource records for fully Qualified Domain Names.

4.2.2 Approval or Rejection of Certificate Applications

Applications for all ACES Certificates shall be approved only after successful completion of verification and authentication of the identity of the applicant.

Authorized ACES CAs may suspend or end the current applicant registration process, as determined by the Authorized ACES CA, and shall, at a minimum, provide the following verification information to the certificate applicant:

- Indicate failure of identity verification process
- Inform the applicant of the process necessary to resume processing

The ACES Authorized Issuer shall record the following transaction data:

- Applicant's name as it appears in the applicant's request for a certificate
- Method of application (i.e., online, in-person) for each data element accepted for

proofing, including electronic forms

- Name of document presented for identity proofing
- Issuing authority
- Date of issuance
- Date of expiration
- Subscriber identified Relying Party Application
- All fields verified
- Source of verification (i.e., which databases used for cross-checks)
- Method of verification (i.e., online, in-person)
- Date/time of verification
- Names of the individual completing the identity verification
- Fields that failed verification
- Status of current registration process (suspended or ended)
- All identity verification data
- All associated error messages and codes
- Date/time of process completion or suspension

For ACES certificates, the CA shall reject a certificate request if the requested Public Key has a known weak Private Key.

Public key parameters generation and quality checking, shall be conducted in accordance with NIST SP 800-89. Key validity shall be confirmed in accordance with NIST SP 800-56A.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

At the time the Subscriber applies for an ACES certificate, the Authorized ACES CA shall authenticate itself to the applicant prior to collecting any identity information. Upon issuance of an ACES Certificate, the Authorized ACES CA warrants to all Program Participants that:

- The Authorized ACES CA will manage the ACES Certificate in accordance with the requirements in this ACES CP.
- The Authorized ACES CA has complied with all requirements in this ACES CP when identifying the Subscriber and issuing the ACES Certificate.
- There are no misrepresentations of fact in the ACES Certificate known to the Authorized ACES CA and the Authorized ACES CA has verified the information

in the ACES Certificate. It is the responsibility of the Authorized ACES CA to verify the source of the certificate request, and to ensure that Subscriber information submitted in the application process is correct and accurate. Information will be verified to ensure legitimacy as per Section 3.2, Initial Identity Validation.

- Information provided by the Subscriber for inclusion in the ACES Certificate has been accurately transcribed to the ACES Certificate.
- The ACES Certificate meets the material requirements of this ACES CP.
- The Authorized ACES CA shall ensure a permanent record is created with every certificate issuance.

While the Subscriber may do most of the data entry, it is still the responsibility of the Authorized ACES CA to verify that the information is correct and accurate. This may be accomplished either through a system approach linking databases containing personal information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organization. If databases are used to confirm Subscriber attributes, then these databases must be protected from unauthorized access and modification to a level commensurate with the level of assurance specified for the certificates conveying the Subscriber attributes. There must be an auditable chain of custody available for information obtained from databases.

Public keys shall be delivered to the certificate issuer in a way that binds the applicant's verified identification to the public key being certified. This binding shall be accomplished using means that are as secure as the security offered by the keys being certified. The binding shall be accomplished using cryptographic, physical, procedural, and other appropriate methods. The methods used for public key delivery shall be stipulated in the Authorized ACES CA's CPS.

In those cases where public/private key pairs are generated by the Authorized ACES CA on behalf of the Subscriber, the Authorized ACES CA shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber, and that the token is not activated prior to receipt by the proper Subscriber.

4.3.2 Notification to Subscriber of Certificate Issuance

Upon successful completion of the Subscriber identification and authentication process in accordance with this ACES CP, the Authorized ACES CA shall create the requested ACES Certificate, notify the applicant thereof, and make the ACES Certificate available to the applicant. The Authorized ACES CA shall use an out-of-band notification process linked to the ACES Certificate applicant's physical U.S. postal mail address, or equivalent, and deliver the ACES Certificate only to the Subscriber.

4.4 CERTIFICATE ACCEPTANCE

Prior to issuing the ACES Certificate by the Authorized ACES CA, the Subscriber shall indicate and agree to the Subscriber obligations under Section 9.6.3, Subscriber Representations and Warranties.

4.4.1 Conduct Constituting Certificate Acceptance

Prior to issuing the ACES Certificate, the Subscriber shall indicate acceptance or rejection of the ACES Certificate to the Authorized ACES CA. By accepting the ACES Certificate, the Subscriber is warranting that all information and representations made by the Subscriber that are included in the ACES Certificate are true.

4.4.2 Publication of the Certificate by the Authorized ACES CA

As specified in Section 2.2.1, Publication of Certificates and Certificate Status, Authorized ACES CA certificates shall be maintained and published in a repository and made available to the public and Relying Parties.

4.4.3 Notification of Certificate Issuance by the Authorized ACES CA to Other Entities

The Authorized ACES CAs shall notify the ACES PMO upon issuance of a new inter-organization CA cross-certificate or issuance of a new ACES subordinate CA certificate.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The responsibilities of each applicant for an ACES Certificate are to:

- Provide complete and accurate responses to all requests for information made by the Authorized ACES CA (or an authorized RA) during the applicant registration, certificate application, and authentication of identity processes
- Generate a key pair using a FIPS 140 validated software or hardware cryptographic module and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the private key
- Upon issuance of an ACES Certificate naming the applicant as the Subscriber, review the ACES Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate acceptance or rejection of the ACES Certificate
- Use the ACES Certificate and the corresponding private key exclusively for purposes authorized by this Policy and only in a manner consistent with this Policy
- Instruct the issuing Authorized ACES CA (or an authorized RA) to revoke the ACES Certificate promptly upon any actual or suspected loss, disclosure, or

other compromise of the private key, or, in the case of Business Representative, whenever the Subscriber is no longer affiliated with the Sponsoring Organization

- Respond as required to notices issued by the Authorized ACES CA

Subscribers who receive certificates from an Authorized ACES CA shall comply with these ACES CP requirements.

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

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for each application and is not controlled by this ACES CP.

Parties who rely upon the certificates issued under this ACES CP should preserve original signed data, the applications necessary to read and process those data, and the cryptographic applications needed to verify the digital signatures on those data for as long as it may be necessary to verify the signature on that data.

4.6 CERTIFICATE RENEWAL

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate, including the public key.

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

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must meet the requirements specified in Section 6.3.2, Certificate Operational Periods and Key Usage Periods.

Certificates may also be renewed when an Authorized ACES CA re-keys.

4.6.2 Who May Request Renewal

Requests for certificate renewal shall only be accepted from subscribers, sponsoring organizations, or RAs on behalf of subscribers and sponsoring organizations.

Additionally, Authorized ACES CAs may perform renewal of subscriber certificates without a corresponding request, such as when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

Authorized ACES CAs shall accept ACES Certificate renewal requests from their Subscribers within 90 days from the scheduled end of the operational period (expiration date) of the ACES Certificate, provided the ACES Certificate is not revoked, suspended, or expired. ACES Certificates may be renewed in one, two, and three-year increments, in accordance with Section 3.3.2, Identification and Authentication for Renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

Authorized ACES CAs shall notify subscribers of new ACES certificate issuance in accordance with the notification processes specified in Section 4.3.2, Notification to Subscriber of Certificate Issuance.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting acceptance of a renewed certificate shall be in accordance with the processes specified in Section 4.4.1, Conduct Constituting Certificate Acceptance.

4.6.6 Publication of the Renewal Certificate by the Authorized ACES CA

Publication of the renewed Authorized ACES CA certificate shall be in accordance with Section 4.4.2, Publication of the Certificate by the Authorized ACES CA.

4.6.7 Notification of Certificate Issuance by the Authorized ACES CA to Other Entities

Authorized ACES CAs shall provide notification of certificate issuance to other inter-organizational entities in accordance with the notification processes specified in Section 4.4.3, Notification of Certificate Issuance by the Authorized ACES CA to Other Entities.

4.7 CERTIFICATE RE-KEY

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

Subscribers of Authorized ACES CAs shall authenticate themselves for the purpose of re-keying as required in Section 3.3.1, Identification and Authentication for Routine Re-Key.

Re-key of a certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness.

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

4.7.1 Circumstance for Certificate Re-Key

ACES certificate re-keying shall be accomplished through the limitation on certificate renewals. The minimum requirement for all ACES certificate re-keying, with the exception of the Authorized ACES CA certificates, shall be once every three years, in accordance with Section 6.3.2, Certificate Operational Periods and Key Usage Periods.

4.7.2 Who May Request Certification of a New Public Key

ACES subscribers with a currently valid certificate may request certification of a new public key. Authorized ACES CAs, sponsoring organizations, and RAs may request certification of a new public key on behalf of subscribers.

4.7.3 Processing Certificate Re-Key Requests

Before processing certificate re-key requests, the Authorized ACES CA shall identify and authenticate the subscriber in accordance with Section 3.2, Initial Identity Validation, and Section 3.3., Identification & Authentication for Re-Key and Renewal.

4.7.4 Notification of New Certificate Issuance to Subscriber

Authorized ACES CAs shall notify subscribers of new ACES certificate issuance in accordance with the notification processes specified in Section 4.3.2, Notification to Subscriber of Certificate Issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting acceptance of a re-keyed certificate shall be in accordance with the processes specified in Section 4.4.1, Conduct Constituting Certificate Acceptance.

4.7.6 Publication of the Re-Keyed Certificate by the Authorized ACES CA

Publication of the re-keyed Authorized ACES CA certificate shall be in accordance with Section 4.4.2, Publication of the Certificate by the Authorized ACES CA.

4.7.7 Notification of Certificate Issuance by the Authorized ACES CA to Other Entities

Authorized ACES CAs shall provide notification of certificate issuance to other inter-organizational entities in accordance with the notification processes specified in Section 4.4.3, Notification of Certificate Issuance by the Authorized ACES CA to Other Entities.

4.8 MODIFICATION

Certificate modification consists of creating new certificates with subject information (e.g., a name or email address) that differs from the old certificate. For example, an

Authorized ACES CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new certificate may have the same or different subject public key.

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

4.8.1 Circumstance for Certificate Modification

Authorized ACES CAs may modify their own CA certificate or OCSP responder certificate whose characteristics have changed (e.g., assert new policy OID). The new certificate may have the same or a different subject public key.

An Authorized ACES CAs may perform certificate modification for a subscriber whose characteristics have changed (e.g., name change due to marriage). The new certificate shall have a different subject public key.

4.8.2 Who May Request Certificate Modification

Subscribers with a currently valid certificate may request certificate modification. Authorized ACES CAs, sponsoring organizations, and RAs may request certificate modification on behalf of subscribers.

4.8.3 Processing Certificate Modification Requests

Proof of all subject information changes must be provided to the Authorized ACES CA and verified before the modified certificate is issued.

4.8.4 Notification of New Certificate Issuance to Subscriber

Authorized ACES CAs shall notify subscribers of new ACES certificate issuance in accordance with the notification processes specified in Section 4.3.2, Notification to Subscriber of Certificate Issuance.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

Conduct constituting acceptance of a modified certificate shall be in accordance with the processes specified in Section 4.4.1, Conduct Constituting Certificate Acceptance.

4.8.6 Publication of the Modified Certificate by the Authorized ACES CA

Publication of the modified Authorized ACES CA certificate shall be in accordance with Section 4.4.2, Publication of the Certificate by the Authorized ACES CA.

4.8.7 Notification of Certificate Issuance by the Authorized ACES CA to Other Entities

Authorized ACES CAs shall provide notification of certificate issuance to other inter-organizational entities in accordance with the notification processes specified in Section 4.4.3, Notification of Certificate Issuance by the Authorized ACES CA to Other Entities.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

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

For Medium, and Basic Assurance, all CAs shall publish CRLs. Revocation requests must be authenticated. Requests to revoke or suspend a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

Authorized ACES CAs shall publish CRLs and provide certificate status information via the Online Certificate Status Protocol (OCSP) for all revoked and suspended certificates. To the extent practical, the contents of changes in status shall be checked before posting to ensure that all information is correct.

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within the 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 such as control over a domain. This would include evidence that a wild card certificate has been issued with a name where PKI Sponsor does not exercise control of the entire name space associated with the wild card certificate.
- Certificates that contain a deceptive name or are used for unethical purposes such as but not limited to promoting malware or illegal software.
- 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 failure of a CA to adequately adhere to the requirements of this CP or the approved CPS. E.G., there is strong evidence that the CA has failed to comply with the requirements of Section 6.7 of the CP.

In addition, for ACES SSL certificates, a certificate shall be revoked when:

- The CA obtains evidence that the issuing CA (or Subordinate CA) no longer complies with the requirements of section 6.7. In this case, all certificates under an issuing CA or subordinate CA shall be revoked.
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name

4.9.1.1 Permissive Revocation

A Subscriber may request revocation of his/her/its ACES Certificate at any time for any reason. A Sponsoring Organization may request revocation of an ACES Certificate issued to its Employee or Business Representative at any time for any reason.

4.9.1.2 Required Revocation

A Subscriber or a Sponsoring Organization (where applicable), is responsible for promptly requesting revocation of an ACES Certificate:

- When any of the identifying information or affiliation components of any names and other information in the certificate (e.g., privilege attributes asserted) become invalid or are deceptive.
- When the private key, or the media holding the private key, associated with the ACES Certificate is, or is suspected of having been, compromised
- When the individual named as a Business Representative or Employee no longer represents, or is no longer affiliated with, the Sponsoring Organization
- When the Subscriber can be shown to have violated the stipulations of the subscriber agreement
- The Subscriber or other authorized party (as defined in the Authorized ACES CA's CPS) asks for his/her certificate to be revoked
- When the certificate is used for unethical purposes to include but not limited to promoting malware or illegal software.

Failure to request revocation under these circumstances is at the Subscriber's risk.

The Authorized ACES CA shall revoke the certificate:

- If the private key is suspected of compromise
- If the Subscriber can be shown to have violated the stipulations of its Subscriber agreement
- If an Authorized ACES CA learns, or reasonably suspects, that the Subscriber's private key has been compromised
- If the issuing Authorized ACES CA determines that the ACES Certificate was not properly issued in accordance with this Policy and/or the Authorized ACES CA's ACES CPS

Whenever any of the above circumstances occur, the Authorized ACES CAs shall revoke the certificate and include all revoked certificates in all new publications of certificate status information until the certificate expires.

4.9.2 Who Can Request Revocation

The only persons permitted to request revocation of an ACES Certificate issued pursuant to this ACES CP are the Subscriber, the Sponsoring Organization (where applicable), and the issuing Authorized ACES CA or RA.

The CA shall provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA shall publicly disclose the instructions through a readily accessible online means.

4.9.3 Procedure for Revocation Request

An ACES Certificate revocation request should be promptly communicated to the issuing Authorized ACES CA, either directly or through the RA authorized to accept such notices on behalf of the Authorized ACES CA. An ACES Certificate revocation request may be communicated electronically if it is digitally signed with the private key of the Subscriber or the Sponsoring Organization (where applicable). Alternatively, the Subscriber, or Sponsoring Organization (where applicable), may request revocation by contacting the issuing Authorized ACES CA or its RA in person and providing adequate proof of identification in accordance with this ACES CP.

The procedure to request the revocation of a certificate shall identify the certificate to be revoked, identify the reason for revocation, and authenticate the identity of the individual making the request. If the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's or the RA's revocation request must so indicate. If a RA makes a revocation request on behalf of a Subscriber, a formal, signed message format known to the CA shall be employed. All requests shall be authenticated (e.g., digitally or manually signed). For signed requests from the certificate subject, or from an RA, verification of the signature is sufficient.

4.9.4 Revocation Request Grace Period

There is no grace period for an ACES certificate revocation request.

4.9.5 Time within Which Authorized ACES CA Must Process the Revocation Request

The Authorized ACES CAs shall revoke certificates within two (2) business days of receipt of a valid revocation request. The ACES PMO may either grant or deny a revocation exception if requested by the Authorized ACES CA. If the ACES PMO denies an exception, the Authorized ACES CA shall revoke the certificate as soon as possible not to exceed two (2) business days. Revocation requests shall be processed before the

next CRL is published or status made available via OCSP, excepting those requests validated within two hours of publication. Revocation requests validated within two hours of publication shall be processed before the following publication.

4.9.6 Revocation Checking Requirements for Relying Parties

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

4.9.7 CRL Issuance Frequency

For this ACES CP, CRL issuance encompasses both CRL generation and publication.

CRLs shall be published periodically, even if there are not changes to be made, to ensure timeliness of information. CRLs may be issued more frequently than specified below.

Authorized ACES CAs that issue certificates to subscribers or operate online must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 48 hours after issuance time (i.e., the *thisUpdate* time).

For Authorized ACES CAs that are operated in an off-line manner, routine CRLs may be issued less frequently than specified above if the Authorized ACES CA only issues:

- CA Certificates
- (Optionally) CSS certificates, and
- (Optionally) end user certificates solely for the administration of the Authorized ACES CA

However, the interval between routine CRLs shall not exceed 31 days.

All Authorized ACES CAs must meet the requirements specified in Section 4.9.12, Special Requirements Related to Key Compromise, for issuing Emergency CRLs.

4.9.8 Maximum Latency of CRLs

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

4.9.9 Online Revocation/Status Checking Availability

Authorized ACES CAs shall validate online, near-real-time (as current as the latest CRL) the status of all ACES Certificates indicated in an ACES Certificate validation request message via OCSP as defined in RFC 6960. The status information must be updated and available to relying parties within 24 hours of revocation.

The latency of certificate status information distributed by the Authorized ACES CA or their delegated status responders must meet or exceed the requirements for CRL issuance as stated in Section 4.9.7, CRL Issuance Frequency.

All Authorized ACES CAs shall use OCSP and CRLs to distribute status information that also supports the GET method for information retrieval.

For the status of Subscriber Certificates:

- The CA shall update information provided via an Online Certificate Status Protocol.

For the status of Subordinate CA Certificates:

- The CA shall update information provided via an Online Certificate Status Protocol whenever CRLs are generated and at least within 18 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder should not respond with a "good" status. The CA should monitor the responder for such requests as part of its security response procedures. The CA shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA. The CA shall maintain a continuous 24x7 ability to respond internally to a security incident.

In addition, for ACES SSL certificates, OCSP responses must be signed either:

1. by the CA that issued the certificates whose revocation status is being checked, or
2. by a delegated OCSP Responder using a certificate signed by the CA that issued the certificate whose revocation status is being checked.

The OCSP Responder signing certificate shall contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 Online Revocation Checking Requirements

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

4.9.11 Other Forms of Revocation Advertisements Available

Authorized ACES CAs may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the Authorized ACES CA's approved CPS.

- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- The alternative method must meet the issuance and latency requirements for CRLs stated in Section 4.9.7, CRL Issuance Frequency, and Section 4.9.8, Maximum Latency of CRLs.

4.9.12 Special Requirements Related to Key Compromise

For Authorized ACES CAs, when a CA certificate is revoked or a Subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued as specified below:

Assurance Level	Maximum Latency for Emergency CRL Issuance
Basic	24 hours after notification
Medium	18 hours after notification

Table 5. Maximum Latency for Emergency CRL Issuance by Assurance Level

4.9.13 Circumstances for Suspension

A certificate may be placed in suspended status following an unsigned request for certificate revocation, pending authentication of the revocation request.

4.9.14 Who can Request Suspension

See Section 4.9.2, Who Can Request Revocation.

4.9.15 Procedures for Suspension Request

See Section 4.9.3, Procedure for Revocation Request.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 CERTIFICATE STATUS SERVICES

All Authorized ACES CAs shall use OCSP and CRLs to distribute status information. To the extent practical, the contents of changes in status shall be checked before posting to ensure that all information is correct.

4.10.1 Operational Characteristics

Authorized ACES CAs shall validate the online, near-real-time the status of the ACES Certificate indicated in an ACES Certificate validation request message in accordance with OCSP [RFC 6960].

4.10.2 Service Availability

See Section 2.2.1, Publication of Certificates and Certificate Status.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Subscriber key management keys (e.g., encryption, decryption) may be escrowed to provide key recovery. Authorized ACES CAs that support private key escrow for key management keys shall document their key recovery practices and identify that document in their CPS. A copy of the document shall be provided to the ACES PMO for review. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Authorized ACES CAs that support session key encapsulation and recovery shall document the practices and identify that document in their CPS.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Adequate security means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

All authorized users of IT, including contractors, consultants, or other third parties who are specifically granted access to the Authorized ACES Issuer Program, shall comply with relevant CPS, SSP and PPP. The minimum security controls that must be in place prior to authorization of an Authorized ACES CA for processing include the following:

- Technical and/or security evaluation are complete.
- A Risk assessment has been conducted.
- Rules of behavior have been established and signed by users in accordance with requirements set forth in NIST 800-18, and NIST 800-53.
- A Contingency Plan has been developed and tested in accordance with guidelines provided in NIST 800-18, NIST SP 800-34, and NIST 800-53.
- A System Security Plan (SSP) has been developed, updated, and reviewed, in accordance with requirements set forth in NIST 800-18, NIST SP 800-34, and NIST 800-53.
- The system meets the moderate level of controls set forth in latest version of the NIST 800-53 PKI overlay.
- In-place and planned security safeguards appear to be adequate and appropriate for the system, i.e., the level of controls should be consistent with the NIST 800-53 revision 4 Moderate level of controls.
- In-place planned and tested incident response procedures and reporting of security incidents is in accordance with guidelines provided in NIST 800-61 Computer Security Incident Handling Guide.

The Authorized ACES CA shall not publish or disclose in any manner, without the ACES PMO's written consent, the details of any safeguards either designed or developed by the Authorized ACES CA.

For each system, an individual should be the focal point for assuring there is adequate security within the system, including ways to prevent, detect, and recover from security problems. The responsibility for security shall be assigned in writing to an individual trained in the technology used in the system and in providing security for such technology including the management of security controls such as user identification and authentication.

5.1 PHYSICAL CONTROLS

Each Authorized ACES CA, and all associated RAs, CMAs, and Repositories, shall implement appropriate physical security controls and restrict access to the hardware and software (including the server, workstations, and any cryptographic software and hardware modules or tokens) used in connection with providing Authorized ACES CA services at all times to protect against theft, loss, and unauthorized use. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role.

The Authorized ACES CA's physical and environmental security program shall address access controls, water exposures, fire safety, failure of supporting utilities, media storage, waste disposal, off-site backup capabilities, structural collapse, interception of data, and mobile and portable systems, in accordance with Federal regulations.

5.1.1 Site Location and Construction

Authorized ACES CAs shall implement the physical security requirements as follows:

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

5.1.2 Physical Access

The Authorized ACES CA shall provide physical access controls designed to provide protections against unauthorized access to ACES system resources.

5.1.2.1 Physical Access for CA Equipment

Physical security of Authorized ACES CA equipment shall encompass the following:

- Authorized ACES CA and RA equipment shall always be protected from unauthorized access, and especially while the cryptographic module is installed and activated.
- Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the equipment environment.
- Ensure no unauthorized access to the hardware is permitted.
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers.

- Ensure that the physical site is manually or electronically monitored for unauthorized intrusion at all times.
- Ensure that an access log is maintained and inspected periodically
- Require two person physical access control to both the cryptographic module and computer system.
- Restrict the entry and exit of personnel, equipment and media from any area containing a local area network (LAN) server.

Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

If the facility is left unattended, a security check of the facility housing Authorized ACES CA equipment shall be conducted. At a minimum, this check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when open, and secured when closed.
- Any security containers are properly secured.
- Physical security systems (e.g., door locks, vent covers) are functioning properly.
- The area is secured against unauthorized access.

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

5.1.2.2 Physical Access for RA Equipment

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

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment (if implemented), shall meet the CA physical access requirements specified in Section 5.1.2.1, Physical Access for CA Equipment.

5.1.3 Power and Air Conditioning

The Authorized ACES CAs shall provide for backup power sources sufficient to supply uninterruptible operation, or backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. In addition, the CA directories (containing CA issued certificates, CRLs, and certificate status information) shall be provided with uninterrupted power sufficient for a minimum of six hours of operation in the absence of commercial power. Authorized ACES CAs shall employ appropriate mechanisms to ensure availability of repositories as specified in Section 2.2.1, Publication of Certificates and Certificate Status.

5.1.4 Water Exposures

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

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

5.1.5 Fire Prevention and Protection

The Authorized ACES CAs shall provide fire prevention and protection in accordance with Federal regulations, GSA policy, and other supporting GSA security guidelines.

5.1.6 Media Storage

Authorized ACES CA media shall be stored so as to protect them from accidental damage (water, fire, electromagnetic) and shall be protected from unauthorized physical access.

5.1.7 Waste Disposal

The Authorized ACES CAs shall provide waste disposal in accordance with Federal regulations.

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner (e.g., sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable).

5.1.8 Off-site Backup

Systems shall be in place for backing up electronic records that guard against the loss of records information because of equipment defects, human error, or theft. These backup procedures shall be properly documented, understood by IT personnel, and be integrated/coordinated with the organization’s disaster recovery plan.

Backups shall be performed by Authorized ACES CAs and stored offsite not less than once per week. Weekly, monthly and yearly backup of magnetic media shall be rotated and transported to an offsite storage facility. Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the Authorized ACES CA's CPS. At least one full backup copy shall be stored at an off-site location (separate from the Authorized ACES CA equipment). Only the latest full backup need be retained.

Backup media will be stored at a secured alternate data storage site which meets physical, procedural and environmental security requirements commensurate to that of the operational Authorized ACES CA, and which is sufficiently distant from the operating facility to provide adequate protection against major natural disasters (e.g., earthquakes and hurricanes).

5.2 PROCEDURAL CONTROLS

The GSA ACES Program Management Office is responsible and accountable for the operation of ACES.

5.2.1 Trusted Roles

An Authorized ACES CA shall utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards. To increase the likelihood that these roles can be successfully carried out, the functions are distributed among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are defined in terms of four roles. These four roles are employed at the CA, RA, and CSS locations, as appropriate:

Administrator – authorized to install, configure, and maintain the CA; establish and maintain system accounts; configure audit parameters; and generate component keys.

Officer – authorized to request or approve certificate issuance and certificate revocations.

Auditor – authorized to review, maintain, and archive audit logs.

Operator – authorized to perform system backup and recovery.

Some roles may be combined. The roles required for each level of assurance are identified in Section 5.2.4, Separation of Roles.

Administrators do not issue certificates to subscribers.

The Authorized ACES Issuer may divide responsibilities in a different fashion or use different titles for Trusted Roles as long as they meet the requirements for separation of duty and number of persons required per task as specified in sections 5.2.2 and 5.2.4. The CPS shall provide the specific titles and responsibilities used.

5.2.2 Number of Persons Required per Task

Two or more persons are required for the following tasks:

- CA key generation
- CA signing key activation
- CA private key backup

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1, Trusted Roles. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

5.2.3 Identification and Authentication for Each Role

Each user in a trusted role must be assigned a unique user ID and authentication credential and shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity. All user IDs must be revalidated at least annually.

5.2.4 Separation of Roles

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

5.3 PERSONNEL CONTROLS

Each Authorized ACES CA and its RA, CMA, and Repository subcontractors shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in a manner consistent with this ACES CP.

Personnel employed to perform functions pertaining to an Authorized ACES CA shall meet applicable requirements set forth in the ACES CP, Authorized ACES CA CPS, and SSP; and Federal regulations. The Authorized ACES CA shall take appropriate administrative and disciplinary actions against personnel who have performed unauthorized actions involving an Authorized ACES CA or its repository.

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity.

For the Authorized ACES CAs all trusted roles are required to be held by U.S. citizens.

The requirements governing the qualifications, selection, and oversight of individuals who operate, manage, oversee, and audit the Authorized ACES CA shall be set forth in the CPS.

5.3.2 Background Check Procedures

Authorized ACES CA personnel shall, at a minimum, pass a background investigation covering the following areas:

- Employment
- Education
- Place of residence
- Law Enforcement
- References

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree shall be verified.

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

5.3.3 Training Requirements

All Authorized ACES CAs shall provide for the mandatory periodic training in computer security awareness and accepted computer security practices of all employees who are involved with the management, use, or operation of the Authorized ACES CA computer system. All personnel shall receive appropriate security briefings upon arrival and before beginning their assigned duties.

All security awareness and training programs shall be developed and implemented in accordance with Federal laws, regulations, and guidelines (See Appendix A).

All personnel performing duties with respect to the operation of the Authorized ACES CA shall receive training in the following areas:

- CA/RA security principles and mechanisms
- All PKI software versions in use on the CA system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Stipulations of this ACES CP

5.3.4 Retraining Frequency and Requirements

Individuals responsible for PKI roles shall be aware of changes in the Authorized ACES CA operation. Any significant change to operations shall have a training (awareness) plan, and the execution of such plan shall be documented**.** Examples of such changes are software and hardware upgrades, changes in automated security systems, and relocation of equipment.

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

5.3.5 Job Rotation Frequency and Sequence

Any job rotation frequency and sequencing procedures shall provide for continuity and integrity of the Authorized ACES CA services.

5.3.6 Sanctions for Unauthorized Actions

The Authorized ACES CA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or it's RAs that are not authorized in this ACES CP, Authorized ACES CA CPS.

5.3.7 Independent Contractor Requirements

All personnel employed to perform Authorized ACES CA functions are subject to all personnel requirements stipulated in this ACES CP.

Authorized ACES CAs shall establish procedures to ensure that any subcontractors perform in accordance with this ACES CP and the Authorized ACES CA CPS.

5.3.8 Documentation Supplied to Personnel

The Authorized ACES CA shall make available to its CA and RA personnel this ACES CP, relevant portions of the CPS, and any relevant statutes, policies, and guidelines. Documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role.

5.4 AUDIT LOGGING PROCEDURES

Audit logs for all security events on each Authorized ACES CA's system shall be generated. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained securely and in accordance with Section 5.5.2, Retention Period for Archive.

5.4.1 Types of Events Recorded

All security auditing capabilities of the Authorized ACES CA operating system and Authorized ACES CA applications, required by this CP, shall be enabled during installation.

At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event
- The date and time the event occurred
- A success or failure indicator when executing the Authorized ACES CA's signing process
- The identity of the entity and/or operator that caused the event

A message from any source requesting an action by the Authorized ACES CA is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents.

All security auditing capabilities of the Authorized ACES CA operating system and Authorized ACES CA applications required by this CP shall be enabled. As a result, most of the events identified below shall be automatically recorded. Where events cannot be automatically recorded, the Authorized ACES CA shall implement manual procedures to satisfy this requirement.

SECURITY AUDIT:

- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Obtaining a third-party time-stamp

IDENTIFICATION AND AUTHENTICATION:

- Successful and unsuccessful attempts to assume a role
- The value of maximum authentication attempts is changed
- Maximum unsuccessful authentication attempts occur during user login
- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
- An Administrator changes the type of authenticator, e.g., from password to biometrics

LOCAL DATA ENTRY:

All security-relevant data that is entered in the system

REMOTE DATA ENTRY:

All security-relevant messages that are received by the system

DATA EXPORT AND OUTPUT:

All successful and unsuccessful requests for confidential and security-relevant information

KEY GENERATION:

Whenever the CA generates a key (not mandatory for single session or one-time use symmetric keys)

PRIVATE KEY LOAD AND STORAGE:

- The loading of Component private keys
- All access to certificate subject private keys retained within the CA for key recovery purposes

TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:

All changes to the trusted public keys, including additions and deletions

SECRET KEY STORAGE:

The manual entry of secret keys used for authentication

PRIVATE AND SECRET KEY EXPORT:

The export of private and secret keys (keys used for a single session or message are excluded)

CERTIFICATE REGISTRATION:

All certificate requests

CERTIFICATE REVOCATION:

All certificate revocation requests

CERTIFICATE STATUS CHANGE APPROVAL:

The approval or rejection of a certificate status change request

CA CONFIGURATION:

Any security-relevant changes to the configuration of the CA

ACCOUNT ADMINISTRATION:

- Roles and users are added or deleted
- The access control privileges of a user account or a role are modified

CERTIFICATE PROFILE MANAGEMENT:

All changes to the certificate profile

REVOCATION PROFILE MANAGEMENT:

All changes to the revocation profile

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT:

All changes to the certificate revocation list profile

MISCELLANEOUS:

- Appointment of an individual to a trusted role
- Designation of personnel for multiparty control
- Installation of the operating system
- Installation of the CA
- Installing hardware cryptographic modules
- Removing hardware cryptographic modules
- Destruction of cryptographic modules

- System startup
- Logon attempts to CA applications
- Receipt of hardware/software
- Attempts to set passwords
- Attempts to modify passwords
- Backing up CA internal database
- Restoring CA internal database
- File manipulation (e.g., creation, renaming, moving)
- Posting of any material to a repository
- Access to CA internal database
- All certificate compromise notification requests
- Loading tokens with certificates
- Shipment of tokens
- Zeroizing tokens
- Re-key of the CA
- Configuration changes to the CA server involving:
    - Hardware
    - Software
    - Operating system
    - Patches
    - Security profiles

PHYSICAL ACCESS / SITE SECURITY:

- Personnel access to room housing CA
- Access to the CA server
- Known or suspected violations of physical security

ANOMALIES:

- Software error conditions
- Software check integrity failures
- Receipt of improper messages
- Misrouted messages
- Network attacks (suspected or confirmed)
- Equipment failure
- Electrical power outages
- Uninterruptible power supply (UPS) failure
- Obvious and significant network service or access failures
- Violations of certificate policy
- Violations of certification practice statement
- Resetting operating system clock

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed at least once a month.

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 log. All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

A statistically significant set of security audit data generated by Authorized ACES CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. This amount shall be described in the Authorized ACES CA CPS.

The Authorized ACES CA shall implement procedures to ensure that the security audit data are transferred prior to overwriting or overflow of automated security audit log files.

5.4.3 Retention Period for Audit Logs

All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

Audit logs shall be retained onsite for at least two months or until reviewed, as well as being retained in the manner described below and in Section 5.5, Records Archive.

The individual who removes audit logs from the Authorized ACES CA system shall be an official different from the individuals who, in combination, command an Authorized ACES CA signature key.

5.4.4 Protection of Audit Logs

Authorized ACES CA system configuration and procedures must be implemented together to ensure that:

- Only authorized persons have read access to the logs
- Only authorized persons may archive or delete audit logs
- Audit logs are not modified or have an integrity mechanism to ensure they are unalterable.

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from deletion or destruction prior to the end of the audit log retention period (note that deletion requires modification access).

The off-site storage location for audit logs shall be a safe, secure location separate from the Authorized ACES CA equipment.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

The audit collection system may or may not be external to the Authorized ACES CA system. Audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data are protected against loss (e.g., overwriting or overflow of automated log files). 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 GSA shall determine whether to suspend Authorized ACES CA operations until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

There is no requirement to provide notice that an event was audited to the individual, organization, device or application that caused the event.

5.4.8 Vulnerability Assessments

The Authorized ACES CAs will perform routine self-assessments of security controls, specifically checking for evidence of malicious activity.

Practice Note: The security audit data should be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors should check for continuity of the security audit data.

5.5 RECORDS ARCHIVE

5.5.1 Types of Events Archived

The Authorized ACES CA shall retain and archive all data as required by the ACES program. At the end of the ACES program, or at termination of the ACES MOA, the Government will provide information as to disposition of the data. Authorized ACES CA archive records shall be sufficiently detailed to establish the proper operation of the Authorized ACES CA, or the validity of any certificate (including those revoked or expired) issued by the Authorized ACES CA.

At a minimum, the following data shall be recorded for archive in accordance with each assurance level:

- CA accreditation (if applicable)
- Certificate policy
- Certification practice statement

- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Record of CA re-key
- Security audit data (in accordance with Section 5.4.1, Types of Events Recorded)
- Revocation requests
- Subscriber identity authentication data (per Section 3.2.3, Authentication of Individual Identity)
- Documentation of receipt and acceptance of certificates (if applicable).
- Subscriber agreements
- Documentation of loading, shipping, receipt, and zeroizing of tokens
- All CRLs issued and/or published
- Other data or applications to verify archive contents
- Compliance Auditor Reports
- All changes to the Audit parameters, e.g. audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys)
- All routine certificate validation transactions
- Export of private keys (Not mandatory for single session or one-time use symmetric keys)
- All access to certificate subject private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- The approval or rejection of a certificate status change request
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

5.5.2 Retention Period for Archive

The minimum retention period for archive records is 10 years and six months. Applications required to process the archive data shall also be maintained for a period determined by the GSA.

5.5.3 Protection of Archive

The archive media must be protected at least at the level required to maintain and protect all Subscriber information and data from disclosure, modification, or destruction.

No unauthorized user shall be permitted to write to, modify, or delete the archive. The Authorized ACES CA shall maintain a list of people authorized to modify or delete the archive, and make this list available during CP compliance audits.

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

The contents of the archive shall not be released except as determined by the GSA or as required by law; however, records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents.

Archive media shall be stored in a safe, secure storage facility separate from the Authorized ACES CA itself.

5.5.4 Backup Procedures

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

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 KEY CHANGEOVER

To minimize risk from compromise of the Authorized ACES CA's private signing key, that key should be changed often. Upon key changeover, only the new key will be used for certificate signing purposes. The older valid certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also

expired. If the old private key is used to sign CRLs that contain certificates signed with that key, the old key must be retained and protected.

The Authorized ACES CA private keys and subject names must be unique per Authorized ACES CA. An Authorized ACES CA must generate a new key and apply a new subject name when generating new Authorized ACES CA certificates prior to distribution.

The Authorized ACES CA's signing key shall have a validity period as described in Section 6.3.2, Certificate Operational Periods and Key Usage Periods.

> After a CA performs a Key Changeover, the CA may continue to issue CRLs with the old key until all certificates signed with that key have expired. As an alternative, after all certificates signed with that old key have been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates. This final CRL shall be available for all relying parties until the validity period of all issued certificates has past. Once the last CRL has been issued, the old private signing key of the CA may be destroyed.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The ACES PMO shall be notified by the Authorized ACES CAs operating under this policy of any security incident. A security incident or incident is defined as a violation or imminent threat of violation of ACES CP, CPS, subscriber agreements, MOA, or any other document that governs the operations of Authorized ACES CAs. A security incident may include but is not limited to the following:

- Suspected or detected compromise of the Authorized ACES CA systems
- Suspected or detected compromise of a certificate status server (CSS) if:
    - The CSS certificate has a lifetime of more than 72 hours and
    - The CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the id-pkix-ocsp-nocheck extension)
- Physical or electronic penetration of the Authorized ACES CA systems
- Successful denial of service attacks on the Authorized ACES CA components
- Any incident preventing the Authorized ACES CA from issuing a CRL within 48 hours of the issuance of the previous CRL
- Suspected or detected issuance of fraudulent certificates used for unethical purposes such as but not limited to promoting malware or illegal software.
- Any certificate mis-issuance not in compliance with the ACES CP, CPS, or ACES Certificate Profiles.
- Authorized ACES CA private key compromise.
- A known or reasonably known, publicly reported compromise of the Authorized ACES CA.

- Any other issue that the ACES PMO identifies as calling into question the Authorized ACES CA integrity or trustworthiness

The Authorized ACES CA shall re-establish operational capabilities in accordance with GSA policies and guidelines and procedures as set forth in the Authorized ACES CA's CPS.

In the event of a CA or certificate compromise or fraudulent mis-issuance, the Authorized ACES CA shall notify the ACES PMO as soon as possible, but no later than 24 hours from the time the incident was discovered. An initial security incident report shall be submitted to the GSA-ACES@GSA.gov email or communicated directly to the ACES Policy Authority and include the sections identified below.

1. Which Authorized ACES CAs were affected by the incident
2. Authorized ACES CA's interpretation of the incident.
3. Was the incident detected as part of normal operations. If not, explain why.
4. Who detected the incident or perpetrated if known
5. When the incident was discovered
6. Physical location of the incident, if applicable.
7. A partial or complete list of all certificates that were either mis-issued or not compliant with the CP/CPS as a result of the incident.

A final security incident report shall be submitted at a date specified by the ACES PMO to the same location as the initial incident report and include all sections identified below.

1. A complete timeline of events.
2. If a compromise, a detailed description of the exploit and what and how infrastructure was compromised.
3. If the Authorized ACES CA did not detect the incident, why not.
4. What specific remedial measures were taken or will take to address the underlying cause including specific CP/CPS updates.
5. Other information appropriate to understand the incident such as system or vendor documentation or other material.
6. Proof the mis-issued certificates were revoked.
7. Who detected or perpetrated the incident.
8. If requested, log files.
9. Detailed description of how the incident was closed.

In coordination with the Authorized ACES CA, the ACES PMO may conduct the following activities as part of an incident response.

- Communicate with affected parties or directly with affected organizations
- Publish notice of revocation
- Publicly publish a final security incident report on an approved government website.
- Require the Authorized ACES CA to employ, at the Authorized ACES CA expense, a third party investigator to investigate the security incident and prepare a final security incident report.
- Request specific reports at a periodic interval as determined by the ACES PMO

- Specify a due date for the Authorized ACES CA to submit a final security incident report.

The ACES PMO shall notify the Authorized ACES CA, in writing, of its intentions in response to the security incident seven (7) days prior to the action by the ACES PMO except under exceptional circumstances (as defined in the glossary) where the ACES PMO will make reasonable efforts to communicate with the Authorized ACES CA prior to taking action. The Authorized ACES CA may propose an alternate course of action and the ACES PMO may consider reasonable alternatives but reserves the right to reject any proposed course of action not in the government's best interest.

Authorized ACES CAs will notify the ACES PMO of any questionable certificate activity.

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

All Authorized ACES CAs will retain back-up storage media to facilitate restoration to full operation. When computing resources, software, and/or data are corrupted, the Authorized ACES CA shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- If the Authorized ACES CA signature keys are not destroyed**,** CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7, CRL Issuance Frequency.
- If the Authorized ACES CA signature keys are destroyed**,** CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

GSA shall be notified as soon as possible.

5.7.3 Authorized ACES CA Private Key Compromise Procedures

Each Authorized ACES CA must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by an Authorized ACES CA to issue ACES Certificates. Such plan shall include procedures for (and documentation of) revoking all affected ACES Certificates it has issued, and promptly notifying all Subscribers and all Relying Parties.

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

- The GSA shall be immediately informed, as well as any superior or cross-certified CAs and any entities known to be distributed the Authorized ACES CA certificate (e.g., in a root store).
- The Authorized ACES CA shall revoke all affected ACES certificates it has issued.

- A new Authorized ACES CA key pair shall be generated by the Authorized ACES CA in accordance with Section 6.1.1, Key Pair Generation.
- New Authorized ACES CA certificates shall be issued to subordinate CAs in accordance with the CPS.

If the Authorized ACES CA distributed a Trusted Certificate, the Authorized ACES CA shall perform the following operations:

- Generate a new Trusted Certificate.
- Securely distribute the new Trusted Certificate as specified in Section 6.1.4, Authorized ACES CA Public Key Delivery to Relying Parties.
- Initiate procedures to notify subscribers of the compromise.

The GSA shall investigate what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

Authorized ACES CAs must have in place an appropriate disaster recovery/business resumption plan in accordance with guidelines provided by NIST SP 800-34, and NIST SP 800-53. Such plan shall be detailed within the Authorized ACES CA's CPS and other appropriate documentation made available to and approved by GSA.

The Authorized ACES CA shall at the earliest feasible time securely advise the GSA in the event of a disaster where the Authorized ACES CA installation is physically damaged and all copies of the Authorized ACES CA signature keys are destroyed.

Authorized ACES CAs operating under this CP shall have recovery procedures in place to reconstitute the Authorized ACES CA within 72 hours.

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

5.7.5 Customer Service Center

Authorized ACES CAs shall implement and maintain a Customer Service Center to provide assistance and services to Subscribers and Relying Parties, and a system for receiving, recording, responding to, and reporting problems within its own organization and for reporting such problems to GSA. The Authorized ACES CA shall ensure that there is a capability to provide help to users when a security incident occurs in the system.

5.8 AUTHORIZED ACES CA OR RA TERMINATION

An Authorized ACES CA shall perform the following in the event that the Authorized ACES CA ceases operation or its participation as an Authorized ACES CA or is

otherwise terminated:

- All Subscribers, sponsoring organizations, and Relying Parties must be promptly notified of the cessation.
- All ACES Certificates issued by an Authorized ACES CA shall be revoked no later than the time of cessation.

In the event that an Authorized ACES CA terminates operation, the GSA shall ensure that any certificates issued to that CA have been revoked.

Authorized ACES CAs that have ceased issuing new ACES certificates shall either continue to issue CRLs until all certificates issued by that CA have expired, or shall issue a final long term CRL with a nextUpdate time past the validity period of all issued certificates. This final CRL shall be available for all relying parties until the validity period of all issued certificates has past. The Authorized ACES CA is required to continue to conform to all relevant aspects of this CP (e.g., audit logging and archives).

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 Authorized ACES CA Key Pair Generation

Cryptographic keying material used to sign certificates, CRLs or status information by Authorized ACES CAs shall be generated in FIPS 140 Security Level 2 validated cryptographic modules or modules validated under equivalent international standards.

Authorized ACES CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures, either by witnessing the key generation or by examining the signed and documented record of the key generation.

Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the Subscriber, Authorized ACES CA, or RA. If the Authorized ACES CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2, Private Key Delivery to Subscriber, must also be met. Key generation shall be performed using a FIPS-approved method or equivalent international standard.

For Medium and Basic assurance levels, either validated software or validated hardware cryptographic modules shall be used for key generation.

6.1.2 Private Key Delivery to Subscriber

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

When an Authorized ACES CA or RA generates keys on behalf of the Subscriber, the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber.

- The private key must be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
    - For physical delivery on a hardware token, accountability for the location and state of the token must be maintained until the Subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.
    - For shared key applications, organizational identities, and network devices (also see Section 3.2).

The Authorized ACES CA must maintain a record of the subscriber acknowledgement of receipt of the token.

6.1.3 Public Key Delivery to Certificate Issuer

The following requirements apply for Authorized ACES CAs:

- Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity must be delivered securely to the Authorized ACES CA for certificate issuance in a way that ensures that:
    - It has not been changed during transit;
    - The sender possesses the private key that corresponds to the transferred public key; and
    - The sender of the public key is the legitimate user claimed in the certificate application.
- Subscriber public keys shall be delivered to the Authorized ACES CA in a secure manner set forth in the Authorized ACES CA's CPS. If off-line means are used for public key delivery, they shall include identity checking as set forth in this CP and shall also ensure that proof of possession of the corresponding private key is accomplished.
- The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the Authorized ACES CA keys used to sign the certificate.

6.1.4 Authorized ACES CA Public Key Delivery to Relying Parties

When an Authorized ACES CA updates its signature key pair, the Authorized ACES CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in cross-certificates.

Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods for self-signed certificate delivery are:

- Loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms, such as:
  - The Trusted Certificate is loaded onto the token during the Subscriber's appearance at the RA.
  - The Trusted Certificate is loaded onto the token when the RA generates the Subscriber's key pair and loads the private key onto the token, which is then delivered to the Subscriber in accordance with Section 6.1.2.
- Secure distribution of self-signed certificates through secure out-of-band mechanisms
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (N.B. hashes posted in-band along with the certificate are not acceptable as an authentication mechanism).
- Loading certificates from Web sites secured with a currently-valid certificate of equal or greater assurance level than the certificate being downloaded.

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

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

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

6.1.5 Key Sizes

All FIPS-approved algorithms shall be considered acceptable; additional restrictions on key sizes are detailed below:

.

Authorized ACES CAs that generate certificates and CRLs under this policy shall use signature keys of at least 2048 bits for RSA or DSA, and at least 224 bits for ECDSA. Public keys in Authorized ACES CA certificates that expire after12/31/2030 shall be at least 3072 bits for RSA, or at least 156 bits for ECDSA.

Authorized ACES CAs that generate certificates and CRLs under this CP shall use the, SHA-256, or SHA-384 hash algorithm when generating digital signatures. RSA signatures on certificates and CRLs shall be generated using SHA-256 or ECDSA signatures on certificates and CRLs shall be generated using SHA-256 or SHA-384, as appropriate for the key length.

CAs that issue certificates signed with SHA 224 or SHA 256 after December 31, 2010 must not issue certificates signed with SHA-1. Signatures on certificates and CRLs that are issued after 12/31/2030 shall be generated using, at a minimum, SHA-256.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the Authorized ACES CA to sign CRLs.

For Authorized ACES CAs issuing certificates under this CP, end-entity certificates shall contain public keys that are at least 2048 bit for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.
Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require AES for the symmetric key, and at least 2048 bit RSA or 224 bit elliptic curve keys.

6.1.6 Public Key Parameters Generation and Quality Checking

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

Parameter quality checking (including primality testing for prime numbers) shall be performed in accordance with FIPS 186; additional tests may be specified by the GSA.

Elliptic Curve public key parameters shall always be selected from the set specified in Section 7.1.3, Algorithm Object Identifiers.

6.1.7 Key Usage Purposes (as per X509 v3 Key Usage Field)

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate.

CA certificates issued by Authorized ACES CAs shall set two key usage bits: *cRLSign* and/or *keyCertSign*. Where the subject signs OCSP responses, the certificate may also set the *digitalSignature* and/or *nonRepudiation* bits.

> Subscriber certificates shall assert key usages based on the intended application of the key pair. In particular, certificates to be used for digital signatures (including authentication) shall set the *digitalSignature* and/or *nonRepudiation* bits. Certificates asserting digitalSignature shall also assert the extendeKeyUsage value for Client Authentication (1.3.6.1.5.5.7.3.2), certificates asserting nonrepudiation shall also assert the extendedKeyUsage value for Secure Email (1.3.6.1.5.5.7.3.4) and may also assert the value for Document Signing (1.3.6.1.4.1.311.10.3.12). The anyEKU shall not be asserted in any ACES certificate.

Certificates to be used for key or data encryption shall set the *keyEncipherment* and/or *dataEncipherment* bits. Certificates to be used for key agreement shall set the *keyAgreement* bit. For encryption certificates using a key encipherment mechanism, either the *keyEncipherment bit* or the *keyAgreement* bit shall be set to 1 and all other bits shall be 0. Encryption certificates shall also assert the extendedKeyUsage value for Secure Email (1.3.6.1.5.5.7.3.4)

After March 1 2017, ACES SSL certificates shall assert an ExtendedKeyUsage value of Server Authentication (1.3.6.1.5.5.7.3.1) and may optionally assert the Client Authentication (1.3.6.1.5.5.7.3.2). ACES SSL certificates may assert both digitalSignature and keyEncipherment.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERNG CONTROLS

Each Authorized ACES CA, RA, and CMA shall each protect its private key(s) in accordance with the provisions of this CP.

6.2.1 Cryptographic Module Standards and Controls

The Authorized ACES CAs shall use a cryptographic module that meet or exceeds FIPS 140-1 or FIPS 140-2, Security Level 2 overall. Authorized ACES CAs shall use FIPS 140-1 or FIPS 140-2, validated cryptographic modules that adhere, as a minimum, to the following additional requirements:

- Level 3 - 4 (identity-based operator authentication) for “Roles and Services”
- Level 3 (tamper protection and response envelope for covers and doors) for “Physical Security” for CA private key storage in hardware
- Level 2 Hardware for RAs
- Level 1 Hardware or Software for Subscribers

Upon request, Authorized ACES CAs shall provide at least FIPS 140-1 or FIPS 140-2, Level 2 validated cryptographic modules for key pair generation and storage of private keys to application servers.

The installation, removal, and destruction of all cryptographic modules shall be documented.

6.2.2 Private Key Multi-Person Control

A single person shall not be permitted to activate or access any cryptographic module that contains the complete Authorized ACES CA private signing key. Authorized ACES CA signature keys may be backed up only under two-person control. Access to Authorized ACES CA signing keys backed up for disaster recovery shall be under at least two-person control. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of Authorized ACES CA Private Signature Key

Under no circumstances shall an Authorized ACES CA signature key used to sign certificates or CRLs be escrowed.

6.2.3.2 Escrow of Authorized ACES CA Encryption Keys

No stipulation.

6.2.3.3 Escrow of Subscriber Private Signature Keys

Subscriber private signatures keys shall not be escrowed.

6.2.3.4 Escrow of Subscriber Private Encryption Keys

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

6.2.4 Private Key Backup

6.2.4.1 Backup of Authorized ACES CA Private Signature Keys

The Authorized ACES CA private signature keys shall be backed up under the same multi-person control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the Authorized ACES CA private signature key shall be accounted for and protected in the same manner as the original. All access to certificate subject private keys retained within the Authorized ACES CA for key recovery purposes must be documented. Hardware tokens containing Authorized ACES CA private signature keys may be backed up in accordance with the security audit requirements defined in this CP. Backup procedures shall be included in the Authorized ACES CA's CPS.

6.2.4.2 Backup of Subscriber Private Signature Key

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

6.2.4.3 Backup of Subscriber Key Management Private Keys

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

6.2.4.4 Backup of CSS Private Key

CSS private keys may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.

6.2.5 Private Key Archival

Authorized ACES CA private signature keys and subscriber private signatures keys shall not be archived. Authorized ACES CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys, in accordance with this CP.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Authorized ACES CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4.1, Backup of Authorized ACES CA Private Signature Keys. At no time shall the Authorized ACES CA private key exist in plaintext outside the cryptographic module.

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

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

6.2.7 Private Key Storage on a Cryptographic Module

No stipulation beyond that specified in FIPS 140.

6.2.8 Method of Activating Private Keys

Authorized ACES CAs signing key activation requires multi-person control as specified in Section 5.2.2, Number of Persons Required per Task.

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

6.2.9 Method of Deactivating Private Keys

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

6.2.10 Method of Destroying Private Keys

Individuals in trusted roles shall destroy Authorized ACES CA, RA, and status server (e.g., OCSP server) private signature keys when they are no longer needed.

Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a zeroize command. Physical destruction of hardware should not be required.

To ensure future access to encrypted data, subscriber private key management keys should be secured in long-term backups or archived.

6.2.11 Cryptographic Module Rating

See Section 6.2.1, Cryptographic Module Standards and Controls.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Usage Periods

Authorized ACES CAs shall distribute the Federal Common Policy CA as the ACES Trust Anchor or ACES Root CA.. Authorized ACES CAs shall not issue subscriber certificates that extend beyond the end of the CA's certificate.

The Authorized ACES CA shall limit the use of its private keys to a maximum of six years for subscriber certificates and ten years for CRL signing and OCSP responder certificates.

Subscribers' signature private keys and certificates have a maximum lifetime of three years. Subscriber key management certificates have a maximum lifetime of three years; use of subscriber key management private keys is unrestricted.

The validity period of the Subscriber certificate must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1, Identification and Authentication for Routine Re-Key.

6.3.3 Restrictions on Authorized ACES CA's Private Key Use

The private key used by Authorized ACES CAs for issuing ACES Certificates shall be used only for signing such Certificates and, optionally, CRLs or other validation services responses.

A private key held by a CMA, if any, and used for purposes of manufacturing ACES Certificates is considered the Authorized ACES CA's signing key, is held by the CMA as a fiduciary, and shall not be used by the CMA for any other purposes, except as agreed by GSA and the Authorized ACES CA. Any other private key used by a CMA for

purposes associated with its CMA function shall not be used for any other purpose without the express permission of the Authorized ACES CA.

The private key used by each RA employed by an Authorized ACES CA in connection with the issuance of ACES Certificates shall be used only for communications relating to the approval, issuance, or revocation of such certificates.

Under no circumstances shall the Authorized ACES CA signature keys used to support non-repudiation services be escrowed by a third party.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock Authorized ACES CA or Subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Activation data may be user selected, including activation selected by each of the multiple parties holding that activation data). The strength of the activation data shall meet or exceed the requirements for authentication mechanisms stipulated in FIPS 140. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

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

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be:

- Memorized
- Biometric in nature, or
- Recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module

The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective Authorized ACES CA CPS. Passwords shall be encrypted.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

The computer security functions may be provided by the operating system, or through a

combination of operating system, software, and physical safeguards in accordance with Federal laws, regulations, and guidelines.

6.5.1 Specific Computer Security Technical Requirements

For Authorized ACES CAs systems, the following computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications.
- Manage privileges of users to limit users to their assigned roles.
- Generate and archive audit records for all transactions (see Section 5.4, Audit Logging Procedures).
- Enforce domain integrity boundaries for security critical processes.
- Support recovery from key or system failure.
- Enforce multi-factor authentication for all accounts capable of directly causing certificate issuance or implement technical controls operated by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.

For Certificate Status Servers, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications.
- Manage privileges of users to limit users to their assigned roles.
- Enforce domain integrity boundaries for security critical processes.
- Support recovery from key or system failure.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The entire ACES system development life cycle shall be controlled to ensure its integrity at all levels, including the use of best commercial practices. The system development controls are as follows:

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology.
- Hardware and software developed specifically for a particular Authorized ACES CA shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment.

- Where open source software has been utilized, the Authorized ACES CA shall demonstrate that security requirements were achieved through software verification and validation and structured development/life-cycle management.
- Hardware and software procured to operate the Authorized ACES CA shall be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- The Authorized ACES CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not part of the Authorized CA operation. Where the Authorized ACES CA operation supports multiple CAs, the hardware platform may support multiple CAs.
- Proper care shall be taken to prevent malicious software from being loaded onto the Authorized ACES CA equipment. All applications required to perform the operation of the Authorized ACES CA shall be obtained from documented sources. All hardware and software, including RA hardware and software, shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the Authorized ACES CA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the Authorized ACES CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the Authorized ACES CA system. The Authorized ACES CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The Authorized ACES CA shall periodically verify the integrity of the software as specified in the Authorized ACES CA CPS.

6.6.3 Object Reuse

When a storage object (e.g., core area, disk file, etc.) is initially assigned, allocated, or reallocated to a system user, the system shall assure that it has been cleared in accordance with Federal laws, regulations, and guidelines. Authorized ACES CAs' CPSs shall specify procedures for sanitizing electronic media for reuse (e.g., overwrite or degaussing of electronic media) and controlled storage, handling, or destruction of spoiled media, or media that cannot be effectively sanitized for reuse.

All magnetic media used to store sensitive unclassified information shall be purged or destroyed when no longer needed. The Authorized ACES CA system shall ensure that a user is not able to access the prior contents of a resource that has been allocated to that user by the system. Care shall be taken to ensure that the Recycle Bin does not store

deleted files and procedures shall be established to ensure the proper disposal of printed output based on the sensitivity of the data.

6.6.4 Life Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

Authorized ACES CAs shall employ appropriate security measures for CAs, RAs, CSSs, and supporting repository servers to ensure they are guarded against denial of service and intrusion attacks. Unused network ports and services shall be turned off. Any network software present on the Authorized ACES CA equipment shall be necessary to the functioning of the Authorized ACES CA service. The Authorized ACES CA's CPS shall define the network protocols and mechanisms required for the operation of the Authorized ACES CA services.

Authorized ACES CAs shall operate a repository connected to the Internet that provides continuous service (except, when necessary, for brief periods of maintenance or backup).

Any boundary control devices used to protect the network on which Authorized ACES CA equipment is hosted shall deny all but the necessary services to the equipment even if those services are enabled for other devices on the network. Authorized ACES CA servers, routers, and other communication hardware essential for maintaining the operability of the system and its connectivity to the backbone network, as well as any other hardware used in support of production systems, shall be placed in a controlled access location (i.e., behind locked doors).

Remote access to the ACES system shall be restricted to secure methods employing approved I&A as well as intrusion detection and unauthorized access monitoring. Authorized ACES CAs shall indicate if encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. If encryption is used as part of the access controls, provide information about the following:

- The cryptographic methodology (e.g., secret key and public key) used
- If a specific off-the-shelf product is used, the name of the product
- That the product and the implementation method meet Federal standards, and include that information
- Cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving

6.7.1 Interconnections

If the Authorized ACES CA systems interconnect, they shall connect using a secure methodology (such as a firewall) that provides security commensurate with acceptable risk and limit access only to the information needed by the other system. Telnet use must be restricted through firewalls.

Authorized ACES CAs are required to obtain written authorization from GSA prior to connecting with other systems. Authorized ACES CAs shall provide the following information concerning the authorization for the connection to other systems or the sharing of information:

- List of interconnected systems (including Internet.)
- Unique system identifiers, if appropriate
- Name of system(s)
- Organization owning the other system(s)
- Type of interconnection (TCP/IP, Dial, SNA, etc.)
- Discussion of major concerns or considerations in determining interconnection
- Date of authorization
- Sensitivity level of each system
- Interaction among systems
- Security concerns and Rules of Behavior of the other systems that need to be considered in the protection of this system

Authorized ACES CA's CPSs shall provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices, and if additional passwords or tokens are required.

Access to and from other systems will be controlled according to Federal laws and regulations and GSA security policies and guidelines.

6.7.2 Inventory

Authorized ACES CAs shall develop and maintain a comprehensive inventory of Authorized ACES CA IT equipment, hardware and software configurations (including security software protecting the system and information), and major information systems/applications, identifying those systems/applications which process sensitive information in accordance with Federal laws and regulations.

6.8 TIME STAMPING

ACES date/time stamps shall conform to the ITU-T Recommendation X.690 and the X.690 v2, Information Technology – ASN.1 Encoding Rules, 1994.

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1, Types of Events Recorded.

7. CERTIFICATE, CARL/CRL, AND OCSP PROFILES FORMAT

7.1 CERTIFICATE PROFILE

The Authorized ACES CA shall create and maintain ACES Certificates that conform to RFC 5280 and ITU-T Recommendation X.509, The Directory: Authentication Framework, June 1997. All ACES certificates must include a reference to an OID for this Policy within the appropriate field, and contain the required certificate fields as specified in this CP.

At a minimum, Authorized ACES CAs shall issue certificates that comply with the Federal Public Key Infrastructure X.509 Certificate and CRL Extension Profile [FPKI-PROF].

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

CA certificates issued by Authorized ACES CAs shall not include critical private extensions.

Whenever private extensions are used in subscriber certificates, they shall be identified in the Authorized ACES CA's CPS. Critical private extensions shall be interoperable in their community of use.

After March 1, 2017:

1) ACES SSL certificates shall assert the Server Authentication EKU and may assert the Client Authentication EKU.
2) Authorized ACES CAs shall not assert the anyEKU in any ACES certificate.
3) All ACES certificates must contain at least 20 bits of entropy in the serial number.

7.1.3 Algorithm Object Identifiers

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

sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }

ecdsa-with-SH256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }

Where certificates are signed using RSA with PSS padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. RSA signatures with PSS padding may be used with the hash algorithms and OIDs specified below:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

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

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-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }

Where a certificate contains an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }
ansip521r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 35 }

7.1.4 Name Forms

Where required as set forth in Section 3.1.1, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280.

7.1.5 Name Constraints

No Stipulation.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert the OID appropriate to the type of certificate and level of assurance with which it was issued. See Section 1.2, Document Identification, for specific OIDs.

7.1.7 Usage of Policy Constraints Extension

The Authorized ACES CAs may assert policy constraints in CA certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates may contain policy qualifiers identified in RFC 5280.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

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

7.2 CRL PROFILE

When ARLs and CRLs are used to distribute status information, detailed ARL/CRL profiles addressing the use of each extension shall conform to the Federal PKI X.509 Certificate and CRL Extension Profile and RFC 5280.

7.2.1 Version Numbers

The Authorized ACES CAs shall issue X.509 Version two (2) CRLs.

7.2.2 CRL Entry Extensions

CRL extensions shall conform to [FPKI-PROF].

7.3 OCSP PROFILE

Certificate status servers (CSSs) operated under this CP shall sign responses using algorithms designated for CRL signing.

If used, an Authorized ACES CA shall technically constrain an OCSP responder certificate such that id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) is the only EKU asserted. OCSP responder certificates shall contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

8. COMPLIANCE AUDITS AND OTHER ASSESSMENTS

Authorized ACES CAs shall undergo an annual PKI compliance audit to ensure that the requirements of their CPS are being implemented and enforced.

This specification does not impose a requirement for any particular CPS compliance assessment methodology as long as the requirements of the FPKI Compliance Audit Requirements Document[4] [FPKI Audit Requirements] are satisfied. The Authorized ACES CA is responsible for ensuring audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The Authorized ACES CAs and RAs and their subordinate CAs and RAs shall be subject to a periodic CP/CPS PKI compliance audit at least once per year and ensure there is no gap between audit periods. Where a status server is specified in certificates issued by an Authorized ACES CA, the status server shall be subject to the same periodic compliance audit requirements as the corresponding CA. For example, if an OCSP server is specified in the authority information access extension in certificates, that server must be reviewed as part of that Authorized ACES CA's compliance audit.

The GSA and other authorized Federal entities reserve the right to perform periodic and aperiodic compliance audits or inspections of Authorized ACES CA, subordinate CA, or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS, SSP, and Privacy Policies and Procedures (PPP).

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The auditor must demonstrate competence in the field of compliance audits. At the time of the audit, the compliance auditor must be thoroughly familiar with requirements which the Authorized ACES CAs CPS and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition, the auditor must be a Certified Information System Auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor either shall be a private firm that is independent of the Authorized ACES CA being audited and qualified to perform a PKI compliance audit on a CA.

If the Authorized ACES CA chooses to obtain a WebTrust Audit, the ACES PMO requires the CA to retain a WebTrust licensed auditor to perform the audit. The full list of WebTrusted-licensed auditors is available in the appendix.

[4] https://www.idmanagement.gov/IDM/s/article_detail?link=fpki-audit-info

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit of an Authorized ACES CA shall be to verify that the Authorized ACES CA is complying with the requirements of this CP and their CPS. The Authorized ACES CA shall not have an MOA with any other PKI.. The scope of the audit must include all CAs that validate or with a path to the Authorized ACES CA. The audit must document the full PKI hierarchy and contain audit information of all PKI components either controlled or contracted by the Authorized ACES CA. The audit may either be in one complete audit or individual audits for each PKI component, but shall be submitted as one complete package to the ACES PMO.

A full compliance audit for Authorized ACES CAs covers all aspects within the scope identified above.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If the Authorized ACES CA compliance auditor finds discrepancies between how the Authorized ACES CA is designed or is being operated or maintained, the requirements of this CP, any applicable MOAs, and/or the Authorized ACES CA CPS, the following actions shall be performed:

- The compliance auditor shall document the discrepancy.
- The compliance auditor shall notify the parties identified in Section 8.6, Communication of Results, of the discrepancy promptly.
- The Authorized ACES CA shall determine what further notifications or actions are necessary to meet the requirements of this CP, Authorized ACES CA CPS, and any relevant MOA provisions.
- GSA will address any identified deficiencies with the Authorized ACES CA. The Authorized ACES CA shall correct any deficiencies noted during these reviews as specified by GSA, including proposing a remedy and expected time for completion.
- If necessary, disqualify any audit report and require the Authorized ACES CA to perform a new audit at the Authorized ACES CA expense.

8.6 COMMUNICATION OF RESULTS

The results of these audits shall be fully documented. The reports resulting from the PKI compliance audit shall be submitted to the GSA ACES PMO and other government entities as specified by GSA within 30 calendar days of the date of their completion.

The CP/CPS compliance report shall identify the versions of the CP and CPS used in the assessment. The final compliance report or letter must be posted to a publicly-accessible location. If a WebTrust audit is submitted and a WebTrust seal is issued it must also be in a publicly-accessible location. All publicly accessible artifacts shall be provided to the ACES PMO with the annual compliance report.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

The Authorized ACES CA shall not impose any certificate access fees on Subscribers with respect to the content of its own CA Certificate(s) or the status of such ACES Certificate(s).

9.1.3 Revocation or Status Information Access Fee

OCSP and CRLs as specified by URLs within ACES certificates must be freely available for all relying parties.

Fees may be assessed for certificate validation services as set forth in the Authorized ACES CA's GSA ACES MOA.

9.1.4 Fees for Other Services such as Policy Information

The Authorized ACES CA shall not impose fees for access to policy information.

9.1.5 Refund Policy

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

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

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Authorized ACES CA information not requiring protection shall be made publicly available.

9.3.1 Scope of Confidential Information

The Authorized ACES CA shall take steps as required to protect the confidentiality of any GSA, Relying Party, Subscriber, or other Government information provided to the Authorized ACES CA. Such information shall be used only for the purpose of providing Authorized ACES CA Services and carrying out the provisions of this Policy and GSA ACES MOA, and shall not be disclosed in any manner to any person except as may be necessary for the performance of the Authorized ACES CA Services in accordance with the GSA ACES MOA.

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

GSA, Relying Party, Subscriber, and Government information provided to the Authorized ACES CA shall be used only for the purpose of providing Authorized ACES CA Services and carrying out the provisions of this CP and GSA ACES MOA, and shall not be disclosed in any manner to any person except as may be necessary for the performance of the Authorized ACES CA Services in accordance with this CP and the GSA ACES MOA.

9.4 PRIVACY OF PERSONAL INFORMATION

Each Authorized ACES CA that maintains an ACES system shall establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to its security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

9.4.1 Privacy Plan

Each Authorized ACES CA shall promulgate written Privacy Policies and Procedures (PPP) designed to ensure compliance with applicable federal and state privacy regulations, and the ACES MOA. These policies and procedures shall be incorporated into the Authorized ACES CA's CPS.

9.4.2 Information Treated as Private

The Authorized ACES CA shall protect the confidentiality of personal information regarding Subscribers that is collected during the applicant registration, ACES Certificate application, authentication, and certificate status checking processes in accordance with all applicable federal and state privacy regulations, and Appendix J of NIST SP 800-53.

Such information shall be used only for the purpose of providing Authorized ACES CA Services and carrying out the provisions of this CP and the GSA ACES MOA, and shall not be disclosed in any manner to any person without the prior consent of the Subscriber, unless otherwise required by law, except as may be necessary for the performance of the Authorized ACES CA Services in accordance with the ACES MOA.

9.4.3 Information not Deemed Private

Information contained on a single ACES Certificate or related status information shall not be considered confidential, when the information is used in accordance with the purposes of providing Authorized ACES CA Services and carrying out the provisions of this CP and the GSA ACES MOA. However, a compilation of such information about an individual shall be treated as confidential.

9.4.4 Responsibility to Protect Private Information

Each Authorized ACES CA or employee of the Authorized ACES CA to whom information may be made available or disclosed shall be notified in writing by the Authorized ACES CA that information disclosed to such Authorized ACES CA or employee can be used only for the purpose and to the extent authorized in this CP.

In addition, Authorized ACES CAs shall store sensitive information securely, and may be released only in accordance with other stipulations in Section 9.4, Privacy of Personal Information.

9.4.5 Notice and Consent to Use Private Information

Subscriber private information shall not be disclosed in any manner to any person without the prior consent of the Subscriber, unless otherwise required by law, except as may be necessary for the performance of the Authorized ACES CA Services in accordance with this Section 9.4, Privacy of Personal Information.

For purposes of notification of the existence of and granting access to records, the Authorized ACES CA shall permit the parent of any minor, or the legal guardian of any individual declared to be incompetent by a court of competent jurisdiction, to act on behalf of such individual.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The Authorized ACES CA shall not disclose private information to any third party unless authorized by this CP, required by law, Government rule or regulation, or order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

Personal information submitted by Subscribers:

- Must be made available by the Authorized ACES CA to the Subscriber involved following an appropriate request by such Subscriber

- Must be subject to correction and/or revision by such Subscriber
- Must be protected by the Authorized ACES CA in a manner designed to ensure the data's integrity
- Cannot be used or disclosed by the Authorized ACES CA for purposes other than the direct operational support of ACES unless such use is authorized by the Subscriber involved

9.5 INTELLECTUAL PROPERTY RIGHTS

Private keys shall be treated as the sole property of the legitimate holder of the corresponding public key identified in an ACES Certificate. This CP is the property of GSA. Access Certificates for Electronic Services, ACES, and the ACES OIDs are the property of GSA, and may be used only by Authorized ACES CAs in accordance with the provisions of this CP. Any other use of the above without the express written permission of GSA is expressly prohibited.

9.6 REPRESENTATIONS AND WARRANTIES

GSA ACES Policy Authority and Program Management Office will:

- Review periodic compliance audits to ensure that RAs and other components operated by the Authorized ACES CA are operating in compliance with their approved CPSs.
- Review name space control procedures to ensure that distinguished names are uniquely assigned within each Authorized ACES CA.

9.6.1 CA Representations and Warranties

Upon issuance of an ACES Certificate, the Authorized ACES CA warrants to all Program Participants that:

- The Authorized ACES CA will manage the ACES Certificate in accordance with the requirements in this ACES CP.
- The Authorized ACES CA has complied with all requirements in this CP when identifying the Subscriber and issuing the ACES Certificate.
- There are no misrepresentations of fact in the ACES Certificate known to the Authorized ACES CA and the Authorized ACES CA has verified the information in the ACES Certificate. It is the responsibility of the Authorized ACES CA to verify the source of the certificate request, and to ensure that Subscriber information submitted in the application process is correct and accurate. Information will be verified to ensure legitimacy as per Section 3, Identification and Authentication.
- Information provided by the Subscriber for inclusion in the ACES Certificate has been accurately transcribed to the ACES Certificate.
- The ACES Certificate meets the material requirements of this CP.

- The Authorized ACES CA assumes responsibility of all CAs that validate.
- The Authorized ACES CA assumes responsibility of all contracted or subcontracted business operations of the Authorized ACES CA.

9.6.2 RA Representations and Warranties

An RA that performs registration functions in support of an Authorized ACES CA shall also comply with the requirements in the CP.

In addition, RAs supporting Authorized ACES CAs shall conform to the following:

- Maintain operations in conformance to the stipulations of the approved Authorized ACES CA CPS.
- Include only valid and appropriate information in certificate requests, and maintain evidence that due diligence was exercised in validating the information contained in the certificate.
- Ensure that obligations are imposed on subscribers in accordance with Section 9.6.3, Subscriber Representations and Warranties, and that subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

An ACES Subscriber (or human sponsor for device certificates) shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers of Authorized ACES CAs shall agree to the following:

- Provide complete and accurate responses to all requests for information made by the Authorized ACES CA (or an authorized RA) during the applicant registration, certificate application, and authentication of identity processes.
- Generate a key pair using a reasonably trustworthy system, and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the private key.
- Upon issuance of an ACES Certificate naming the applicant as the Subscriber, review the ACES Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate acceptance or rejection of the ACES Certificate.
- Use the ACES Certificate and the corresponding private key exclusively for purposes authorized by this Policy and only in a manner consistent with this Policy.
- Instruct the issuing Authorized ACES CA (or an authorized RA) to revoke the ACES Certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the private key, or, in the case of Business Representatives, and State and Local Governments ACES Certificates, whenever the Subscriber is no longer affiliated with the Sponsoring

Organization.

- Respond as required to notices issued by the Authorized ACES CA.

Subscribers who receive certificates from an Authorized ACES CA shall comply with these CP requirements.

9.6.4 Relying Parties Representations and Warranties

Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for each application and is not controlled by this CP.

Parties who rely upon the certificates issued under this policy should preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data.

Authorized ACES CAs shall maintain a relationship with ACES Relying Party and notify the ACES PMO of the following:

- When authorized Points of Contact for a Relying Party Application change.
- When the need for ACES certificates is no longer required by the Relying Party Application

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

Authorized ACES CAs may not disclaim any responsibilities described in this CP.

9.8 LIMITATIONS OF LIABILITY

Nothing in this CP shall create, alter, or eliminate any other obligation, responsibility, or liability that may be imposed on any Program Participant by virtue of any contract or obligation that is otherwise determined by applicable law.

A Relying Party shall have no recourse against GSA, the Authorized ACES CAs, RAs, certificate manufacturing authority or repository for any claim under any theory of liability (including negligence) arising out of reliance upon an ACES certificate, unless such party shall have agreed to provide such recourse under a contract with the relying party. Each Relying Party assumes all risk of such reliance in the absence of such agreement, except that the Subscriber may have liability under applicable law to the Relying Party with respect to a message bearing his digital signature that is authenticated with an ACES certificate.

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

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP becomes effective when approved by the GSA Policy Authority. This CP has no specified term.

9.10.2 Termination

Termination of this CP is at the discretion of the GSA Policy Authority.

9.10.3 Effect of Termination and Survival

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

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

GSA has established appropriate procedures for communications with Relying Parties and Authorized ACES CA via contracts and MOAs as applicable.

For all other communications, no stipulation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The ACES Policy Authority shall review this CP at least once every year. Corrections, updates, or suggested changes to this CP shall be publicly available. Suggested changes to this CP shall be communicated to the ACES Policy Authority and/or Program Manager; such communication must include:

- A description of the change
- A change justification
- Contact information for the person requesting the change

Notice of all proposed changes to this CP under consideration by GSA that may materially affect users of this CP (other than editorial or typographical corrections, changes to the contact details, or other such minor changes) will be provided to Authorized ACES CAs and Relying Parties, and will be posted on the GSA World Wide

Web site. The Authorized ACES CA shall post notice of such proposed changes and shall advise their Subscribers of such proposed changes.

The ACES Policy Authority and/or Program Manager shall assign new OIDs to certificates as needed and maintain control over the numbering sequence of OIDs within the ACES arc. Authorized ACES CAs requiring new OIDs shall submit a request to the ACES Policy Authority and/or Program Manager.

Any interested person may file comments with GSA within 45 days of original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be given.

Version control shall be maintained by the ACES Policy Authority using date and consecutive version numbers to identify revised versions of the CP, which will be presented on a Change Control Page at the beginning of the CP.

9.12.2 Notification Mechanism and Period

A copy of this CP is available in electronic form on the Internet at http://csrc.nist.gov/groups/ST/crypto_apps_infra/csor/pki_registration.html and via email from the ACES Policy Authority. The Authorized ACES CA shall also make available copies of this CP both online and in hard copy form.

9.12.3 Circumstances under Which OID Must Be Changed

OIDs will be changed if the ACES Policy Authority determines that a change in the CP requires a change in OIDs.

9.13 DISPUTE RESOLUTION PROVISIONS

In the event of any dispute or disagreement between two or more of the Program Participants (Disputing Parties) arising out of or relating to this CP or ACES MOAs, Authorized ACES CA CPS, or Agreements related to this CP, which include Subscriber Agreements, the Disputing Parties shall use their best efforts to settle the dispute or disagreement through negotiations in good faith following notice from one Disputing Party to the other(s).

When one of the Disputing Parties is a Federal entity, the dispute arbitrator shall be the GSA ACES Contract Officer.

Any MOA dispute between Authorized ACES CAs and GSA shall be handled under the terms and conditions of the ACES MOA.

9.14 GOVERNING LAW

The laws of the United States shall govern the enforceability, construction, interpretation, and validity of this CP.

9.15 COMPLIANCE WITH APPLICABLE LAW

Authorized ACES CAs are required to comply with applicable law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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

9.16.4 Enforcement (Attorney Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

9.17.1 Waivers

No stipulation.

10. BIBLIOGRAPHY

Refer to Appendix A, Applicable Standards and Guidelines

11. ACRONYMS AND ABBREVIATIONS

AIS	Automated Information System
CA	Certification Authority
CARL	Certificate Authority Revocation List
CIAO	Critical Infrastructure Assurance Office
CM	Configuration Management
CMA	Certificate Manufacturing Authority
COMSEC	Communications Security
COOP	Continuity of Operations Plan
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standards
FIPS PUB	(US) Federal Information Processing Standard Publication
FPCPF	Federal PKI Common Policy Framework
FPKI	Federal Public Key Infrastructure
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
FPKIMA	Federal PKI Management Authority
FPKIPA	Federal PKI Policy Authority

IATO	Interim Authority to Operate
IETF	Internet Engineering Task Force
IS	Information System
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
IT	Information Technology
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
LAN	Local Area Network
LRA	Local Registration Authority
MOA	Memorandum of Agreement (as used in the context of this CP, between an Agency and the Federal PKI Policy Authority allowing interoperation between the FBCA and Agency Principal CA, or between the ACES PMO and Authorized ACES CA)
NIST	National Institute of Standards and Technology
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OID	Object Identifier
OMB	(US) Office of Management and Budget
PIN	Personal Identification Number
PMO	Program Management Office
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
PPP	Privacy Practices and Procedures

RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
SO	System Owner
SSL	Secure Sockets Layer
SSP	System Security Plan
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WAN	Wide Area Network
WWW	World Wide Web

12. GLOSSARY

Access	Ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
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 certification authority for a certificate, but before the certificate issuance procedure is completed.
Archive	Long-term, physically separate storage.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Audit Data	Chronological record of system activities (i.e., audit trail) to enable the reconstruction and examination of the sequence of events and changes in an event.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioral characteristic of a human being.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies 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. As used in this CP, the term “Certificate” refers to certificates that expressly

	reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
Certificate Manufacturing Authority (CMA)	An entity that is delegated or outsourced the task of actually manufacturing the certificate on behalf of an Authorized ACES CA.
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.
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 online verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Certification	The technical evaluation, made as part of and in support of the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements.
Certification and Accreditation (C&A)	Process of testing all aspects of system security leading to a 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.
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.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to Subscribers.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e.,

	requirements specified in this CP, or requirements specified in a contract for services).
Client (application)	A system entity, usually a computer process acting on behalf of a human user, which makes use of a service provided by a server.
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.
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.
Critical Infrastructure	Those physical and cyber-based systems essential to the minimum operations of the economy and government, including but not limited to telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.
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.
Cryptoperiod	Time span during which each key setting remains in effect.
Data Encryption Standard (DES)	NIST data encryption standard adopted by the US government as FIPS PUB 46, which allows only hardware implementations of the data encryption algorithm.
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 Agency or Organization as defined above and below.
Encryption	The process of transforming text into an unintelligible form, in such a way that the original data either cannot be obtained, or can be obtained only by using a decryption process.
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 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 Agency Principal Certification Authorities and external cross-certified PKIs.
Exceptional Circumstances	In terms of a security incident, a situation where the ACES PMO believes the Authorized ACES CA is compromised as to affect the security posture of a large number the Federal PKI ecosystem.
FPKI Management Authority	The Federal PKI Management Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge and Federal Common Policy Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The Federal PKI Policy Authority is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.
Federal Information Processing Standards (FIPS)	These are Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance to agency waiver procedures.
Firewall	Gateway that limits access between networks in accordance with local security policy.
Government	The U.S. Federal Government and its authorized agencies and entities.
Hardware Token	A sequence of bits or characters, contained in a device such as a smart card, a metal key, or some other physical token, that enables recognition of an entity by a system through personal, equipment, or organizational characters or codes; and the process used to verify the identity of a user and the user's eligibility to access an information system.
Individual Accountability	The principle that requires individual users be held accountable for their actions through technical controls,

	which associate the identity of the user with the time, method, and degree of access to a system.
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.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services, and related resources.
Integrity	Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Interim Authority to Operate (IATO)	When a system does not meet the requirements for accreditation, but the criticality of the system mandates that it become operational, temporary authority to operate may be granted. IATO is contingent upon the implementation of proposed solutions and security actions according to an agreed upon schedule within a specified time period.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Changeover	The procedure used by an Authority to replace its own private key (e.g., due to compromise) and replace current valid certificates issued with old key.
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.
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.

Legal Non-Repudiation	How well possession or control of the private signature key can be established. See Non-Repudiation.
Life Cycle	Stages through which an information system passes, typically characterized as initiation, development, operation, and termination.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the Federal PKI Policy Authority and an Agency allowing interoperability between the Agency Principal CA and the FBCA.
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).
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.
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).
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 Federal PKI Policy Authority.
Principal CA	The Principal CA is a CA designated by an Agency to interoperate with the FBCA. An Agency may designate multiple Principal CAs to interoperate with the FBCA.
Privacy	Restricting access to Subscriber or Relying Party information in accordance with Federal law and Agency policy.
Privacy Practices and Procedures (PPP)	A written statement describing policies and procedures for the protection of individual information collected in order to fulfill the requirements of this CP.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an Authorized ACES 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 Management	The total process of identifying, controlling, and eliminating, or minimizing certain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation, and test, security evaluation of safeguards, and overall security review**.**
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.
Router	A special-purpose computer (or software package) that handles the connection between two or more networks. Routers spend all their time looking at the destination addresses of the packets passing through them and deciding on which route to send them.
Rules of Behavior	Rules that have been established and implemented concerning the use of, security in, and acceptable level of risk for the system.
Secret Key	A "shared secret" used in symmetric cryptography, wherein users are authenticated based on a password, Personal Identification Number (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.
Security Incident or Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices; Examples of incidents include: private key compromise, fraudulent certificate issuance, physical CA compromise, other issues that call into question the Authorized ACES CA integrity or trustworthiness.
Sensitivity	The level of protection that information requires. An information technology environment consists of the system, data, and applications, which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability, which is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organization's mission, and the economic value of the system components.
Separation of Duties	Principle by which roles and responsibilities are divided among individuals so that a single individual cannot subvert a critical process.

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).
Suspend (a certificate)	To temporarily suspend the operational period of a Certificate for a specified time period or from a specified time forward.
Symmetric Key	A key that can be used to encrypt and decrypt the same data.
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System Security Plan (SSP)	Documentation of the management, technical, and operational security controls
Technical non-repudiation	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. See Non-Repudiation
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.
Token	Object that a user possesses for the purpose of I&A. Tokens are characterized as “memory tokens” and “smart tokens.” Memory tokens store but do not process information. Special reader/writer devices control the reading and writing of data to and from the token. Smart tokens incorporate one or more integrated circuit into the token. Smart tokens are typically ‘unlocked’ through the use of a PIN or password.
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 Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Valid Certificate	A certificate that (1) an Authorized ACES CA has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a certificate is not "valid" until it is both issued by an Authorized ACES CA and has been accepted by the Subscriber.
Vulnerability Assessment	An analysis of flaws or weaknesses in security procedures, technical controls, physical controls or other controls that may allow harm to occur to an automated information system.
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.

APPENDIX A: APPLICABLE STANDARDS AND GUIDELINES

ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html
CIMC	Certificate Issuing and Management Components Family of Protection Profiles, version 1.5, August 11, 2011.
FBCA CP	X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001.
FIPS 186-4	Digital Signature Standard, August 2015.
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html
FPKI Audit Requirements	Federal Public Key Infrastructure (FPKI) Compliance Audit Requirements, v2, July 10, 2015
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework,.
NIST SP 800-18	NIST Special Publication 800-34 Rev 1, Guide for Developing Security Plans for Federal Information Systems
NIST SP 800-34	NIST Special Publication 800-34 Rev 1, Contingency Planning Guide for Federal Information Systems,
NIST SP 800-53	NIST Special Publication 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-61	Computer Security Incident Handling Guide
NIST SP 800-131A	NIST Special Publication 800-131A Rev 1, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, November, 2015
RFC 3447	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Jonsson, Kaliski
RFC 6712	Internet X.509 Public Key Infrastructure – HTTP Transfer for the Certificate Management Protocol (CMP), Kause and Peylo, September 2012.
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani, et al.
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Cooper, et al.

RFC 6960	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP, Santesson, et al., June, 2013
WebTrust Licensed Auditors	http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx