Certification Practices Statement
Access Certificates for Electronic Services
IdenTrust Services, LLC

Version 5.3
January 30, 2018

(IdenTrust Services, LLC was formerly known as Digital Signature Trust, LLC)

TABLE OF CONTENTS

SECTION **PAGE**

Revision History

Version	Date	Summary of Changes/Comments
5.0	June 5, 2016	Revise DST to IdenTrust Update contact and address information Remove all references to Federal Employee Certificates Incorporate previously approved amendments
5.1	November 10, 2016	Align current CPS with new ACES CP dated Dec 23, 2015
5.2	September 7, 2017	Align current CPS with new ACES CP v 3.2 dated May 12, 2017 Addition of practices for CAA check for Server Certificates. Changes implemented September 8, 2017. CPS approved by IdenTrust PMS on September 13, 2017.
5.3	January 30, 2018	Updates to reflect updated CA/B Forum Baseline Requirements

SECTION 1: INTRODUCTION

This Certification Practices Statement ("CPS") describes the certification practices of IdenTrust Services, LLC ("IdenTrust"), related to its operations as a Certification Authority ("CA") authorized to issue digital certificates in in accordance with version 3.2 of the Certificate Policy ("CP") dated May 12, 2017 for the Access Certificates for Electronic Services ("ACES") program for the U.S. General Services Administration, Federal Acquisition Service. This ACES CPS covers the operation of systems and management of facilities used to provide public key infrastructure (PKI) services described in the IdenTrust Concept of Operations, which include Certification Authority (CA), Authorized Registration Authority (RA), and repository functionality. This ACES CPS also includes practices satisfying requirements prescribed in the CA/Browser Forum document named *Baseline Requirements for the Issuance and management of Publicly-Trusted Certificates* ("CA/B Forum Baseline Requirements"), which has industry-wide acceptance and has been adopted by browsers as part of the pre-requisites to include a Root CA Certificate in their crypto stores. This document sets out requirements for issuance and management of SSL and Device Certificates and it is available online at: https://www.cabforum.org/documents.html

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 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 the 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.

There were SHA-1 specific policy OIDs defined in the ACES CP for use between January 1, 2011 and December 31, 2013. SHA-1 certificates are no longer valid under the ACES CP or this ACES CPS.

In addition to this ACES CPS, the ACES Certificate Policy (ACES CP) may further specify requirements applicable to a particular project, contract or set of contracts, or issuance of a class of certificates undertaken by IdenTrust.

In particular, this ACES CPS addresses the following:

1) the roles, responsibilities, and relationships among IdenTrust, Trusted Agents, Registration Authorities ("RAs"), Certificate Manufacturing Authorities ("CMAs"), Repositories, Subscribers, Relying Parties, and the Policy Authority (referred to collectively as "Program Participants");
2) obligations and operational responsibilities of the Program Participants; and
3) IdenTrust's policies and practices for the issuance, delivery, management, and use of ACES Certificates to verify digital signatures.

In the event that there is any inconsistency between this ACES CPS, the ACES CP, and Memorandum of Agreement (MOA), and the CA/B Forum Baseline Requirements, the MOA provisions take precedence over the CP, which will take precedence over the CA/B Forum Baseline Requirements, which will take precedence over this ACES CPS, even though this ACES CPS may describe in more detail the policies, practices and procedures implemented by IdenTrust in order to comply with the ACES CP and the ACES MOA and the CA/B Forum Baseline Requirements.

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 the ACES CP and is available to all Relying Parties. Each ACES certificate issued shall assert the appropriate certificate policy OID in the *CertificatePolicies* extension.

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

1) Adobe Approved Trust List Technical Requirements version 1.4

While the 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. IdenTrust provides this detailed Certification Practice Statement (CPS) that states how IdenTrust establishes that assurance in accordance with the ACES CP and the ACES MOA.

1.1.3 Scope

The ACES program exists to facilitate trusted electronic business transactions between non-government individuals for authentication or submitting digitally signed artifacts to Federal, state, local, and other government entities, Federal applications and non-Federal users. This ACES CPS 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 CPS
- 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 CPS 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 this ACES CPS.

1.2 DOCUMENT IDENTIFICATION

The ACES Policies are 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.

This ACES CPS is IdenTrust's ACES CPS version 5.2. This CPS alone is not intended to provide the basis for any contractual obligations. Certificates are differentiated by function (signature or encryption), key storage method (software module or hardware token) and by the certificate subject or holder (unaffiliated individual, business representative, etc.) See Section 1.3. IdenTrust issues ACES certificates under the following certificate policy OIDS:

ACES Policy Certificate Type	**Certificate Policy OID**
ACES Unaffiliated Individual Certificates	2.16.840.1.101.3.2.1.1.1.2
ACES Business Representative Certificates	2.16.840.1.101.3.2.1.1.1.3
ACES Application SSL Server Certificates	2.16.840.1.101.3.2.1.1.1.5

ACES CP Description	**Certificate Policy OID**
IdenTrust's Authorized ACES CA Certificate	2.16.840.1.101.3.2.1.1.1.1
ACES Unaffiliated Individual Digital Signature Certificates	2.16.840.1.101.3.2.1.1.1.2
ACES Unaffiliated Individual Encryption Certificates	2.16.840.1.101.3.2.1.1.1.2
ACES Business Representative Digital Signature Certificates	2.16.840.1.101.3.2.1.1.1.3
ACES Business Representative Encryption Certificates	2.16.840.1.101.3.2.1.1.1.3
ACES Application SSL Server Certificates	2.16.840.1.101.3.2.1.1.1.5
ACES Application SSL Server Certificates	2.16.840.1.101.3.2.1.1.1.5 and CAB Forum subject identity validated (2.23.140.1.2.2)

All ACES Certificates issued by IdenTrust under this ACES CPS include the appropriate OID for the applicable certificate in the *Certificate Policies* field of the Certificate. The foregoing OIDs are placed in certificates only as specifically authorized by the ACES CP. Upon approval by the Federal PKI Policy Authority for cross certification with the Federal Bridge Certification Authority ("FBCA"), ACES certificates issued by IdenTrust will support interoperability between the ACES PKI and another PKI by asserting the appropriate FBCA CP OIDS in the

policyMappings extension. Certificates issued in accordance with other approved federal government certificate policies may assert other OIDs upon approval of the relevant policy authorities.

1.3 COMMUNITY AND APPLICABILITY

The ACES PKI is a bounded public key infrastructure. The ACES CP and this ACES CPS describe the rights and obligations of persons and entities authorized under the ACES CP to fulfill any of the following roles:

- Certificate Service Provider roles
- Certificate Service Provider
    - CA
    - Trusted Agent
    - RA
    - CMA
    - Repository
- End Entity roles
    - Unaffiliated Individual
    - Business Representative
    - Device
    - State and Local Government
- Relying Party role
- Policy Authority role

Requirements for persons and entities authorized to fulfill any of these roles are defined in this Section. A general description of each of these roles and their responsibilities is set forth in Section 2 of this ACES CPS.

Additional obligations are set forth in other provisions of the ACES CP; and in the GSA ACES MOAs, including requirements of this **A**CES CPS, the 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

GSA FAS is the Policy Authority responsible for organizing and administering the ACES CP and ACES MOA.

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 CPS only if such CA first qualifies as an Authorized ACES CA by:

1) Entering into an appropriate MOA with the ACES PMO;
2) Documenting the specific practices and procedures it will implement to satisfy the requirements of the 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 the ACES CP are performed in accordance with the requirements, representations, and warranties of this ACES CPS.
- 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 will submit to an annual PKI compliance audit of all operational aspects related to this ACES CPS including all RA functions whether performed internally or by a third party.

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.

IdenTrust Services, LLC, is a subsidiary of IdenTrust, Inc., and is also subject to oversight by the Office of the Comptroller of the Currency ("OCC") and other state and federal entities. IdenTrust performs Certification Authority functions (e.g., certificate generation, distribution, revocation, etc.) centrally while performing

Registration Authority functions (e.g., subscriber identification and communication) using a decentralized registration process established by IdenTrust in cooperation with its private sector and public sector partners.

To determine any external RA organization's compliance with the ACES CP and ACES CPS, IdenTrust requires that each participating RA organization perform an independent annual audit of such RA organization's IdenTrust approved Registration Practices Statement (RPS) and provide results of the audit to IdenTrust. IdenTrust then reviews the audit results and works directly with the RA should remediation be required.

IdenTrust is qualified to issue certificates identifying the ACES CP (ACES Certificates) having been qualified by GSA by:

a) entering into an appropriate GSA ACES MOA; and

b) documenting in the ACES CPS and other relevant documents the specific practices and procedures implemented to satisfy the requirements of the ACES CP.

1.3.1.3.1 Cross-Certification with the FBCA

IdenTrust has designated a CA within hierarchical PKI's operated by IdenTrust for purposes of cross certification directly with the FBCA (e.g., through the receipt of a cross-certificate) and further designated that CA as the Root CA of IdenTrust under this ACES CPS. Such further designated CA issues either end-entity certificates or CA certificates to other Authorized ACES CAs, or both.

IdenTrust may request that the FBCA cross-certify with more than one CA within the IdenTrust PKI in connection with the ACES CP and the ACES CPS, regardless of the type of PKI architecture (hierarchical or other) deployed. Where the Authorized ACES CA operates a hierarchical PKI, the designated CA may be the ACES Issuer's Root CA.

1.3.1.4 Certificate Status Servers

IdenTrust includes Online Certificate Status Protocol (OCSP) responders to provide online, near real-time status information as current as the latest Certificate Revocation List.

If OCSP responders are provided on behalf of IdenTrust as a Certificate Status Server (CSS), 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 CSSs are within the scope of this ACES CPS.

As an ACES CA, IdenTrust is responsible for the generation and management of Certificates and Certificate Revocation using a variety of mechanisms including but not limited to CRLs and Online Certificate Status Protocol ("OCSP") checking. In addition to the responsibilities above, IdenTrust's service responsibilities also include the processing of Certificate requests and Revocation requests, generation and sending of responses, generation of CRLs and maintenance of OCSP databases, posting of Certificates and CRLs to directories, the designation of Trusted Agents and Registration Authorities and other tasks related to Certificate/CRL management. See Section 2.1.1 for further discussion of the CA's obligations and responsibilities.

1.3.2 Registration Authorities (RAs) and Trusted Agents

IdenTrust performs the role and functions of the RA. IdenTrust may also receive assistance in performing its registration authority functions from third parties (including government agencies) who agree to be subject to and bound by the approved methods in the ACES CP with respect to registration services, referred to herein as "Authorized RAs." IdenTrust employs Trusted Agents who are authorized to assist in processing Subscriber

identification information during the registration process.

Trusted Agents perform their registration functions without use of automated RA interfaces with the IdenTrust CA system.

In the event that RAs are deployed IdenTrust will ensure that audits include all RA functions whether performed internally or by a third party.

1.3.3 Subscribers

IdenTrust issues ACES Certificates to the following classes of Subscribers:

a) Members of the general public (Unaffiliated Individuals);

b) Individuals authorized to act on behalf of business entities (i.e., Sponsoring Organizations) recognized by IdenTrust, such as employees, officers, and agents of a Sponsoring Organization (Business Representatives); and

c) Application Servers.

All subordinate CA Certificates issued by IdenTrust for ACES are used and controlled by IdenTrust. IdenTrust does not issue Subordinate CA Certificates to external parties at this time.

A PKI Sponsor is a natural person who applies for a Device Certificate but is not the Subscriber. The PKI Sponsor is responsible for registering application and/or Servers with the Trusted Agent or LRA. This individual is employed by or the authorized agent for the Sponsoring Organization who has express authority to represent the organization for the Device Certificate. The PKI Sponsor is also responsible for the operation and control of an application or Server (device), and assumes the obligations of Subscriber for the certificate associated with the device, including but not limited to:

- A duty to protect the Private Key of the Device at all times;
- Sign and submit, or approve an Device Certificate request on behalf of the organization; and
- Sign and submit a Subscriber Agreement on behalf of the organization, and/or acknowledge and agree to the certificate terms of use on behalf of the organization when the organization is an affiliate of the CA.

1.3.4 Relying Parties

Relying Parties are those persons and entities which fulfil the duties and obligations of Relying Parties as set forth in the ACES CP and this ACES CPS, including but not limited to those duties and obligations related to determining the validity of an ACES Certificate issued under this ACES CPS prior to each instance of their reliance on such ACES Certificate. The only purpose for which Relying Parties can rely on ACES Certificates issued under this ACES CPS is the verification of digital signatures made with such ACES Certificates. 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.

Entities that become Relying Parties are subject to the terms of the ACES CP and this ACES CPS applicable to Relying Parties. Government operated applications wishing to accept ACES Certificates are bound by the terms of the ACES CP and this ACES CPS.

Except to the extent expressly provided for under this ACES CPS and subject to all disclaimers and limitations set forth therein, IdenTrust shall have no liability to any Relying Party with respect to any ACES Certificate issued under this ACES CPS.

1.3.5 Other Participants

IdenTrust may require the services of other security, community, and application authorities. In this case this ACES CPS will identify the parties, define the services, and designate the mechanisms used to support these services.

1.3.5.1 Certificate Manufacturing Authorities (CMAs)

IdenTrust performs the role and functions of CMA. IdenTrust may also receive assistance in performing its CMA functions from contracting third parties who agree to be subject to and bound by the ACES CP with respect to CMA services.

1.3.5.2 Repositories

IdenTrust performs the role and functions of Repository. IdenTrust may also receive assistance in performing its Repository functions from contracting third parties who agree to be subject to and bound by the ACES CP with respect to Repository services; however, IdenTrust remains responsible for the performance of these services in accordance with the ACES CP and ACES MOA.

1.3.5.3 Applications Servers

IdenTrust issues Application Secure Sockets Layer (SSL) Server Certificates to federal, state, and local governmental agencies and to other organizations for the purposes described below.

1.3.5.3.1 ACES Application Secure Sockets Layer (SSL) Server Certificates

IdenTrust issues ACES Application SSL Server Certificates for use on federal, state and local Agency Servers and other organizations to allow mutual authentication and/or trusted SSL communications between citizens and government Agencies. These certificates are issued to the agency or organization server where the common name is the registered Domain Name of the Webserver. IdenTrust does not and will not issue SSL Certificates to reserved IP addresses or internal server names. IdenTrust does not issue ACES SSL wildcard Certificates at this time.

After December 31, 2015, the Fully Qualified Domain Name of the Agency's Web server shall be contained in the subjectAltName extension of these certificates. Certificates shall allow for server authentication through the extended KeyUsage extension.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

All ACES end-entity certificates are software certificates; however, IdenTrust does allow subscribers to purchase optional hardware to store their certificates, if desired. Note that storage on optional hardware does not change or in any way impact the assurance level of the certificate.

The following table summarizes the functional uses of ACES Certificates:

ACES Certificate Type	Subscriber	Purpose	Use of Certificate

ACES Certificate Type	Subscriber	Purpose	Use of Certificate
IdenTrust CA Certificate	N/A	Establish and generate the CA certificates	To enable the authorized CA to issue subscriber certificates and to issue certificates to subordinate CAs within the IdenTrust ACES CA PKI
Unaffiliated Individual Certificate (Basic and Medium)	Unaffiliated Individual	Digital Signature	To enable an Unaffiliated Individual ACES Subscriber to authenticate himself/herself 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)	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.
Application 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 FPKI: Note: no longer required after December 2015

Effective January 1, 2011, IdenTrust will continue to issue ACES certificates containing ACES SHA-1 certificate policy OIDs and using SHA-1 Digital Signatures; however such SHA-1 Digital signature use will be deprecated. All ACES digital signatures with a validity date beyond January 1, 2014 will be created with SHA-2 (see Section 6.1.5) and include SHA-2 certificate policy OIDs.

As such, use of SHA1 certificates issued under this policy should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.

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 and this ACES CPS.

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.

The 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. IdenTrust offers ACES Unaffiliated, ACES Business Representative Certificates and ACES SSL Application 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

1.5.1.1 ACES CP Administrator

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

1.5.1.2 IdenTrust CPS Administrator

IdenTrust's Change and Risk Management Committee ("CRMC") reviews CPs and approves CPSs. The CRMC manages the audit and risk assessment function for IdenTrust's CA operations to ensure that the risks are accurately identified, that necessary mitigating activities are identified, and that individual projects should proceed. The Chair of the CRMC represents IdenTrust at meetings of the Audit Committee. The CRMC is comprised of representatives from functional units across the organization.

Attn: PMA Chair
IdenTrust Services, LLC
5225 Wiley Post Way
Salt Lake City, UT 84116
Email: helpdesk@IdenTrust.com

1.5.2 Contact Information

1.5.2.1 ACES CP Contact

Questions regarding the ACES CP shall be directed to:

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

1.5.2.2 IdenTrust CPS Contact

IdenTrust, Inc.
ACES Program Manager
5225 Wiley Post Way
Salt Lake City, UT 84116
helpdesk@IdenTrust.com

1.5.2.3 IdenTrust Service Center

The IdenTrust Customer Service Center is available between 7 a.m. and 6 p.m. Mountain Standard Time (MST), Monday through Friday, excluding Federal holidays. The IdenTrust Customer Service Center assists subscribers with certificate- and key-related issues. Such issues include, but are not limited to, problems with key generation and certificate installation. Problems and inquiries received that are not certificate-related are directed to the relevant government agency for resolution with the subscriber. Those concerns can include, but are not limited to, problems with accessing information and inquiries of a general nature. For questions concerning ACES certificates, IdenTrust operations or this ACES CPS, please contact:

Toll-free US: 1 (888) 882-1104
Outside of the US: +1 (801) 384-3511
Fax: (801) 384-3610

Otherwise, assistance is available at the Web site above, 24 hours per day, including Federal holidays, to individual subscribers, business representatives, and individuals authorized to act on behalf of agency applications.

1.5.3 Person Determining CPS Suitability for the ACES CP

1.5.3.1 ACES CP Contact

This ACES CPS must conform to the 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.

1.5.3.2 IdenTrust CPS Contact

Attn: ACES Program Manager
5225 Wiley Post Way
Salt Lake City, UT 84116

1.5.4 CPS Approval Procedure

This ACES 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 ACES CPS before commencing operations.

1.6 DEFINITIONS AND ACRONYMS

See Glossary and Appendix B: Acronyms and Abbreviations

SECTION 2: GENERAL PROVISIONS

2.1 OBLIGATIONS

This section provides a general description of the roles and responsibilities of the ACES Program Participants operating under the ACES CP and this ACES CPS: IdenTrust, RAs, CMAs, Repositories, Subscribers, Relying Parties, and the Policy Authority. Additional obligations are set forth in other provisions of this ACES CPS, IdenTrust's ACES MOA, the System Security Plan (the "SSP"), Privacy Practices and Procedures (the "PPP"), Agreements with Relying Parties, Subscriber Agreements and other agreements with Program Participants.

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 the ACES CP, and other information relevant to ACES Certificates, and for providing information regarding the status of ACES Certificates as valid or invalid that can be determined by a Relying Party.

Repositories retained under contract with IdenTrust to perform Repository services on behalf of IdenTrust are required to comply with the provisions of this ACES CPS and the ACES CP.

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 Status

ACES Certificates issued by IdenTrust contain pointers to locations where certificate-related information is published including CRLs, as specified by the ACES CP. IdenTrust's secure online Repository is available 24 X 7 to Subscribers and Relying Parties at IdenTrust's Repository which contains:

1) all currently valid ACES Certificates issued by IdenTrust that have been accepted by Subscribers; and
2) Authority Revocation Lists / Certificate Revocation Lists (ARLs/CRLs), as specified by the ACES MOA and the ACES Policy Office.
3) CA certificates issued to and by IdenTrust
4) other relevant information about ACES Certificates.

Online certificate status information is available through IdenTrust's ACES validation services via the following locations:

CRL Distribution:
http://validation.identrust.com/crl/acesca2.crl

AIA:
http://validation.identrust.com/certs/acesca2.p7c

OCSP:
http://aces.ocsp.identrust.com

IdenTrust operates and maintains CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less. IdenTrust Root CA Certificates, CRLs, and online ACES Certificate status information are available for retrieval 24 hours a day, seven days a week, with a minimum of 99% availability overall per year and scheduled down-time does not exceed 0.5% annually, excluding network outages.

2.2.2 Publication of CA Information

All information to be published in the repository shall be published immediately after such information is available to IdenTrust. IdenTrust will publish ACES Certificates immediately upon acceptance of such ACES Certificates. Information relating to the status of an ACES Certificate will be published in accordance with the IdenTrust ACES MOA.

The IdenTrust website for ACES contains links to:

1) IdenTrust ACES Certificate for its signing key
2) Past and current versions of the IdenTrust ACES CPSs
3) A copy of the ACES CP correlating to the IdenTrust ACES CPS
4) Annual PKI Compliance Letter
5) WebTrust Audit Seals, if applicable
6) IdenTrust issues ACES SSL Certificates and as such hosts test Web pages that allow Application Software Suppliers to test their software with ACES SSL Certificates that chain up to the ACES Root Certificate. And hosts a 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.

Links are accessible at https://www.identrust.com/certificates/aces.html.

2.3 FREQUENCY OF PUBLICATION

This ACES CPS 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 CPS, Certificate Revocation and Suspension.

2.4 ACCESS CONTROLS ON REPOSITORIES

IdenTrust does not impose any access controls on the ACES CP, IdenTrust's ACES Certificate for its signing key, and past and current versions of this ACES CPS as well as subscriber certificates and status information and can be accessed via links located at https://www.identrust.com/certificates/aces.html.

IdenTrust does, however, impose access controls to ensure authentication of Subscribers with respect to their own certificate(s) and the status of such certificate(s) and personal registration information, which is separately managed from the public certificate and status repository.

Information in the IdenTrust ACES repository is protected in accordance with IdenTrust's Privacy Policies and Procedures (PPP), available at the IdenTrust website at https://www.identrust.com/privacy.html.

SECTION 3: IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

IdenTrust-issued certificates contain an X.500 distinguished name for the subscriber consisting of either the X.501 distinguished name specifying a geo-political name or an Internet domain component name. When domain component naming is used, IdenTrust reserves the right to issue certificates utilizing domain component naming to honor contract obligations or where practical or required for proper application usage for distinguished names in the following manner: dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*]; dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*]; etc.

3.1.1 Types of Names

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

3.1.1.1 ACES Unaffiliated Individual Signature and Encryption Certificates

The subject name used for ACES Unaffiliated Individual Certificates shall be the Subscriber's authenticated common name. The Subscriber's email address shall be used for the Subject Alternative Name (SAN).

3.1.1.2 ACES Business Representative Digital Signature and Encryption Certificates

ACES Business Representative Certificates shall assert X.500 Distinguished Name, and a Subject Alternative Name (SAN). Where required, IdenTrust may 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 IdenTrust, which such assignments shall be made by IdenTrust in accordance with Section 3.1.5. ACES Business Representative Digital Signature Certificates shall assert an alternate name form subject to requirements set forth below intended to ensure name uniqueness. The Subscriber's email address shall be used for the Subject Alternative Name (SAN).

3.1.1.4 ACES Application 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 fully qualified domain name of the server as a Subject Alternative Name (SAN) and optionally as the common

name of the subjectDN. In addition, ACES SSL certificates issued by IdenTrust conform to the following, noting that IdenTrust does not issue ACES SSL wildcard Certificates at this time.

- 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).

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 described below.

3.1.2.1 ACES IdenTrust Digital Signature CA Certificates

IdenTrust implements the name constraint extension of the X.509 version 3 certificate profile in issuing cross certificates in accordance with the FBCA CP cross-certification requirements.

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. IdenTrust 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 structures.

3.1.2.2 ACES Unaffiliated Individual Signature and Encryption Certificates

In the case of Unaffiliated Individuals, the authenticated common name (cn) should be:

(i) a combination of first name and/or initials and surname.

3.1.2.3 ACES Business Representative Signature and Encryption Certificates

In the case of Business Representatives, the authenticated common name (cn) should be:

(i) the combination of (a) first name and, optionally, an initial (b) and surname; and
(ii) reflect the legal name of the organization in the Organizational Unit (ou) information contained in the DN.

3.1.2.5 Agency Application SSL Server Certificates

In the case of Agency Application Servers, the following applies:

(i) the authenticated FQDN is included in a Subject Alternate Name (SAN); and
(ii) the common name (cn) may also include the application server name.

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

3.1.3 Anonymity or Pseudonymity of Subscribers

IdenTrust does not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are contained in the applicable certificate profile, and are established by the GSA/FTS Center for Information Security. The ACES Program Management Office is responsible for Agency CA name space control.

3.1.5 Uniqueness of Names

Name uniqueness across the ACES Program is enforced by IdenTrust's CA. IdenTrust and Authorized 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 across the ACES system is ensured.

IdenTrust uses the following name forms and allocates names within the Subscriber community to guarantee name uniqueness among current and past Subscribers for all Subscriber certificates:

Name uniqueness is made possible through the use of an additional naming attribute as part the SubjectDN: of the subscriber. This attribute is 0.9.2342.19200300.100.1.1, which is an experimental OID for the Attribute UID. Whenever IdenTrust issues a certificate, it calculates a 128-bit Globally Unique ID (GUID) or Universal Unique Identifier (UUID). The GUID/UUID consists of three variables:

- The IP Address of the generator—"the CA system" (4 bytes);
- Time (8 bytes); and
- Sequence number (4 bytes).

The GUID/UUID value, along with the common name of the Subscriber, guarantees uniqueness of the Certificate in the Repository. The GUID/UUID is converted to a string of hexadecimal numbers, e.g., D01E411A000000E1A341CAC00000001.

These unique entries in the Repository may be found using a search of multi-valued naming attributes. For example, an agency may search for a Subject DN using a Repository search for a subscriber entry using "0.9.2342.19200300.100.1.1 = D01E4733000000F3150C2F10000000D8 + cn = John G Man" as the search criteria, which will return a single user entry regardless of the number of "John G Man" subscribers in the Repository.

There are various other methods of using a GUID/UUID to achieve name uniqueness, which IdenTrust reserves the right to use in other implementations with Program Participants of ACES. For instance, IdenTrust also can append the GUID/UUID to the commonName for the Certificate subject. An example X.500 subject common name might be "John A. Doe:0B5FOQAAANX[OPutAAAAIA—" where '0B5FOQAAANX[OPutAAAAIA—'

constitutes a modified base-64 encoding of a UUID. This UUID is then appended, following a colon, to the Subscriber's name to create a unique identifier.

As other methods and standard practices of guaranteeing name uniqueness emerge, IdenTrust may implement these as well; in order to increase application interoperability of certificates.

Device certificates under the ACES program are guaranteed to be unique due to the usage of agency-based application naming of the Subject DN or, in the case of Agency SSL server certificates, the use of a Fully Qualified Domain Name as the Common name of the certificate after verification of its registration and with the FQDN registrar. These Device Certificates include the authenticated name of the electronic device including the dNSName containing the FQDN or public IP address containing the IP address of a Server and if applicable, the name of the Organization. Device Certificates issued on the basis of IP address cannot be issued after 2016. As of that effective date, IdenTrust will not issue a certificate with an expiry date later than November 1, 2015 with a subjectAlternativeName extension or Subject commonName field containing a reserved IP Address or internal Server name.

3.1.6 Recognition, Authentication, and Role of Trademarks

A corporate entity is not guaranteed that its name will contain a trademark if requested. IdenTrust 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. IdenTrust shall not be obligated to research trademarks or resolve trademark disputes.

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. IdenTrust maintains 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 IdenTrust or an RA will require the Subscriber to identify at least one Relying Party application to be accessed with the Subscribers ACES certificate. If the Subscriber-identified Relying Party application is not on the IdenTrust then-current list of ACES Relying Party applications, then (a) prior to issuing the subscriber-requested ACES credential IdenTrust will contact the Relying Party to verify it has a government sponsor and a need for ACES certificates and (b) the Relying Party shall be added to the IdenTrust list of Relying Party applications and will be reported in the monthly report to the ACES PMO.

3.2.1 Possession of Key Pair

Potential Subscribers are required to demonstrate proof of possession of the Private Key that corresponds to the public key in a Certificate request, and IdenTrust is required to verify that the applicant possesses the private key corresponding to the public key submitted with the application for a certificate. IdenTrust verifies that a certificate applicant possesses the private key corresponding to the public key submitted with the application in accordance with secure protocols generally-accepted by the CA industry, such as that described in the IETF PKIX Certificate Management Protocol (e.g., by verifying that the request, or at least a portion thereof, was signed with the applicant's corresponding private key--so that the private key can be verified by the signature and public key contained in the request). See also Section 6.1.3.

3.2.1.1 Hardware Tokens

When hardware tokens are required for private key storage, IdenTrust maintains a record of receipt of the token by the subject. IdenTrust delivers a hardware cryptographic module and a shared secret (see Section 3.1.7.2) directly to the Subscriber or via an Authorized RA or Trusted Agent. Using a pair of shared secrets (1 mutual, 1 exclusive – refer to Section 3.2.1.2), the Subscriber authenticates to IdenTrust. For token-based Signing Certificates, the key pair is generated on the token but only the public key is submitted to IdenTrust for certificate creation. Once created the Signing Certificate is delivered in accordance with Section 4.3. (Certificate Issuance). In accordance with Sections 4.12 (Key Escrow and Recovery) and 6.2.5 (Private Key Archival), generation of the private key corresponding to the token-based Encryption Certificate is performed on the server side by the CA system (to archive the private key for key recovery purposes). The private key is securely delivered to and installed on the Hardware Token via a password-protected PKCS#12-based mechanism.

3.2.1.2 Use of Shared Secrets

IdenTrust uses two classes of shared secrets:

1) Mutually Shared Secret – where the contents of the secret are known to both IdenTrust (or an Authorized Local Registration Agent) and the Subscriber
2) Exclusive Shared Secret – where only the Subscriber knows the content.

When IdenTrust uses a mutually shared secret (e.g., a password or PIN) as a mechanism in the verification method, IdenTrust ensures that the applicant and IdenTrust (or an Authorized RA) are the only recipients of this shared secret.

When IdenTrust uses an exclusive shared secret (e.g., Account Password) as a mechanism in the verification method, IdenTrust ensures that the applicant knows the secret. This is achieved through cryptographic protocols without disclosing the secret to IdenTrust.

3.2.2 Authentication of Sponsoring Organization Identity

If the applicant is requesting a Business Representative ACES Certificate, in addition to verifying the applicant's individual identity and authorization to represent the Sponsoring Organization, IdenTrust is required to verify the Sponsoring Organization's current operating status. In conducting its review and investigation, IdenTrust validates the Sponsoring Organization's legal name, type of entity, address (number and street, city, ZIP code) and telephone number.

The procedure for verifying organization validity is to verify through an independent, third-party source that the organization has been in existence for more than one year. IdenTrust will request identifying information about the organization from the applicant such as the name and address of the organization and the state of its incorporation or organization. IdenTrust will verify the information provided by the applicant using business registration and information databases maintained by third parties such as secretaries of state and commercial vendors. An alternative method of conducting authentication of organization identity will involve a combination of written and oral communication between IdenTrust and an authorized organizational representative.

The authorized organizational representative will make certain representations and warranties regarding the organization's validity and authority. He or she also can attest to the relationship of other employees, representatives or agents of the organization. An authorized organizational representative may also designate a Trusted Agent for the organization authorized to approve potential Subscribers and confirm their relationship

with the organization. An alternative method for employees, representatives or agents to establish their identity and provide evidence of organizational affiliation is through an authorized IdenTrust Trusted Agent. The individual presents a current (i.e., unexpired) picture badge issued by the organization (such badge must have the individual's photo, name, organization name, and expiration date).

If any required information for an SSL Certificate is not obtained during the application process, IdenTrust will repeat the procedures documented in this section and in Section 3.2.3.2 (Authentication of Devices) to obtain the remaining required information requested for inclusion by the applicant from a reliable, independent, third-party database as defined in this section. The information obtained for SSL Certificates must include a FQDN verified by practices as described in Section 3.2.3.2.1.

LRAs or Trusted Agents verify the existence and name of a Sponsoring Organization in one of the following ways:

A reference to a source unrelated to the prospective Sponsoring Organization such as:

- A secretary of state or other Governmental registry;
- Commercial database of business information;
- A third party database that is periodically updated, which IdenTrust has evaluated;
- Presentation to LRA of a copy of a document issued by a Government Agency attesting to the Sponsoring Organization's legal existence, together with reasonable proof of the authenticity of that document. Documents submitted for this purpose must be "fair on their face", i.e., bear no apparent indication of forgery, fraud, tampering, etc.;
- In the case of an organization that is not registered with a state regulatory Agency (such as a partnership or unincorporated association), a copy of the partnership agreement, association rules, assumed name registration, or other document attesting to the organization's existence;
- LRA may independently obtain (without reference to the data provided by the Applicant or PKI Sponsor for a certificate) the name, address, and telephone number of the organization, which are verified through a telephone call with a representative of the organization made to the telephone number independently obtained by LRA or Trusted Agent;
- A site visit by an LRA or a third party who is acting as an agent for IdenTrust; or
- An attestation letter by an authorized representative (e.g., a supervisor, administrative officer, information security officer, certificate coordinator, etc.) of the Applicant/PKI Sponsor's employer that has been verified in accordance with this section, or by a person or entity certified by a Government Agency as being authorized to confirm organization identities, provided that the attestation letter is checked to ensure legitimacy.

IdenTrust will verify the information provided by the Applicant using business registration and information databases maintained by third parties such as secretaries of state and commercial vendors. Should a third party vendor be utilized to confirm information provided manually or electronically IdenTrust or the Authorized RA will evaluate the third-party source by these required criteria;

1) Data it contains that will be relied upon has been independently verified
2) The database distinguishes between self-reported data and data reported by independent information sources; and
3) Changes in the data that will be relied upon will be reflected in the database in no more than 12 months;

In addition, the following criteria will be taken into account while reviewing the information taken from the third-party source:

1) The age of the information provided;
2) The frequency of updates to the third party database;
3) The data provided and purpose of the data collection;
4) The public accessibility of the data availability; and
5) The relative difficulty in falsifying or altering the data.

Any documents received for the manual verification process will be inspected by the LRA for signs of alteration or falsification. The contents of the request will also need to be verified for quality and accuracy.

The authorized organizational representative will make certain representations and warranties regarding the organization's validity and authority. He or she also can attest to the relationship of other employees, representatives or agents of the organization. An authorized organizational representative may also designate a Trusted Agent for the organization authorized to approve potential Subscribers and confirm their relationship with the organization. An alternative method for employees, representatives or agents to establish their identity and provide evidence of organizational affiliation is through an authorized IdenTrust Trusted Agent. The individual presents a current (i.e., unexpired) picture badge issued by the organization (such badge must have the individual's photo, name, organization name, and expiration date).

3.2.3 Authentication of Individual Identity

If applicant passes identity proofing verification, IdenTrust, records, at a minimum, the following transaction data:

- Identity of the person performing the identification
- Applicant's name as it appears in the certificate's Common Name feld
- Subscriber-identified Relying Party Application
- Method of application (i.e., on-line, 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
    - All fields verified
    - Source of verification (i.e., which sources are used for cross-checks)
    - Method of verification (i.e., on-line, in-person)
    - Date/time of verification
- Names of contractors, subcontractors or entities providing identification services, if any
- All associated error messages and codes

- Date/time of process completion
- A unique identifying number from the ID of the verifier and from the ID of the applicant
- Names (IDs) of contractor's/subcontractor's/entity's processes, if any.

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

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

Verification of Email Address

Email verification when required can be done in two ways; electronically and manually through a list submitted by a Trusted Agent. If the application for a Certificate requires email verification the application cannot be approved until the specified steps for electronic or manual of verification is complete.

Electronic Verification of Email

When an Applicant/PKI Sponsor submits an application through a secure online form, an automated email is sent to the Applicant/PKI Sponsor's email address provided in the application. Within that automated email message there is a link that guides the Applicant/PKI Sponsor to a server-authenticated SSL/TLS secured web site and instructions to provide out-of-band information, including an Account Password. This Account Password was created during the application by the Applicant/PKI Sponsor and it is secure only to the Applicant/PKI Sponsor. When the Applicant/PKI Sponsor provides and submits the Account Password created during the application accurately the verification of the email address is completed and the verification status is automatically updated within the Applicant/PKI Sponsor's application record.

Manual Verification of Email

When a Trusted Agent provides the list of authorized Applicants/PKI Sponsors, the email address is validated by the Trusted Agent based on the internal knowledge of the Sponsoring Organization. The Trusted Agent may use internal databases and directories to ensure the email accuracy.

Applicants Outside of the U.S.

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

The certificate retrieval process utilized by IdenTrust ensures that authentication of the identity of human subscribers is 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

IdenTrust does not issue ACES Unaffiliated Individual Encryption certificates at this time.

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

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

a) 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; and
    - Social Security Number
    - Date of birth
    - Place of birth.
b) 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;
c) The use of an out-of-band notification process that is linked to the requesting individual's physical U.S. postal mail address; or equivalent, and
d) Verification of the information contained in the Certificate Application.

3.2.3.1.2 Authentication of ACES Business Representative Digital Signature and Encryption Certificates

IdenTrust does not issue ACES Business Representative Encryption certificates at this time.

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 ID, or two Non-Federal Government IDs, one of which shall be a photo ID (e.g., Driver's 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 employee of IdenTrust;
- A Trusted Agent personally approved by IdenTrust or appointed by name in writing to IdenTrust;
- 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 U.S. Consular Notary if located outside the United States.

IdenTrust, the Authorized RA or the Trusted Agent shall verify:

a) that the applicant is a duly authorized representative of the Sponsoring Organization as an employee, partner, member, agent, or other association; and
b) the Sponsoring Organization's identity as specified in Section 3.2.2.

The process documentation and authentication requirements shall include the following:

- A signed declaration by that person that he or she verified the identity of the Subscriber as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy
- The date and time of the verification
- A declaration of identity signed by the applicant using a handwritten signature. This shall be performed in the presence of the person performing the identity authentication, using a format that declares under penalty of perjury under the local law.

The applicant shall personally appear before one of the required identity verifiers at any time prior to application of the 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 (i.e., routers, firewalls and servers) 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 sponsor is responsible for providing the following registration information:

- Equipment identification- Registered domain name/service name (DNS name), device component serial number, 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 Authorized RA to communicate with the sponsor when required

The registration information shall be verified according to the procedures set forth below in this Section.

3.2.3.2.1 Verification of Authorization by Domain Name Registrant

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.

IdenTrust maintains a policy for devices that receive an ACES SSL certificate that specifies unique meaningful FQDN names, for which an abbreviated process is detailed in this ACES CPS.

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.

All registration information is verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods as described in the ACES CP 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 Sections 3.2.3.1.2 and 3.2.3.1

The LRA confirms the validity of the ACES SSL certificate application via a signed email, according to the following procedures:

1) Each sponsor applying for an ACES SSL certificate must be an ACES Business Affiliated certificate holder and provide an email address named in the ACES Affiliated certificate during the registration process.
2) Upon receipt of an electronically submitted registration for an ACES SSL certificate, IdenTrust will email the ACES SSL sponsor at the email address provided in the ACES SSL registration application, requesting a confirmation email that is signed using that sponsor's ACES Business Affiliated Certificate.
3) The application cannot be approved without receipt of the signed email confirmation.

IdenTrust verifies that the PKI Sponsor has the right to issue or has control of the Fully-Qualified Domain Name(s) from the SAN extension and public IP address(es) listed in the Certificate application by following the steps listed below.

The LRA confirms the rights by the Domain Registrant by doing the following:

1) The domain(s) supplied by the PKI Sponsor is placed into a search engine (e.g. WHOIS) and the LRA records the contact information for the Domain Name Registrant.

2) Once the Domain Name Registrant is identified from a database record he or she are contacted via email to confirm the information provided by the PKI Sponsor to confirm or deny the right of the PKI Sponsor to be issued the certificate for the Domain Name(s) for which the PKI Sponsor has applied. It is through this process that IdenTrust ensures that SSL Certificates are issued with the consent of the owner of each FQDN contained within the Certificate. During this exchange the Domain Name Registrant will have the opportunity to name other potential PKI Sponsor(s).

If the PKI Sponsor applies for a domain that is a two-letter country code (ccTLD), this confirmation will be sought from the Domain Name level to which the ccTLD applies.

For certificate requests where the domain provided indicates the Domain Name Registrant has used a private, anonymous or proxy registration services the RA follows these steps:

The LRA will attempt to contact the domain issuance service to obtain the domain point of contact (POC) contact information. The LRA upon contacting the domain issuance services will request that the Domain services via email contact the Domain Name Registrant and request that they email the RA confirming that he or she is the current domain administrator and that the PKI Sponsor has authorization to request a certificate for said domain. After that confirmation has been received, the LRA will check the email string from the domain administrator for accuracy to confirm or deny the PKI Sponsor's right to apply for a Server Certificate for that domain. Once these steps have been completed the LRA will record and file the records of communication that occurred amongst IdenTrust, the domain registrar and the Domain Name registrant before approving the issuance of the Certificate.

In cases where the registered domain holder cannot be contacted, the LRA will:

- Rely on a verified legal opinion or a verified accountant letter to the effect that the PKI Sponsor has the exclusive right to use the specified Domain Name(s) in identifying itself on the internet; and

- Rely on a practical demonstration by the PKI Sponsor establishing that it controls the Domain Name(s) by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing the PKI Sponsor's FQDN(s).

During this procedure the Domain Name registrant will be asked if they would like to provide a list of individuals authorized to apply for a certificate for that Domain Name and/or any additional FQDNs verified

under their control. Individuals that apply for FQDNs provided by the Domain Name registrant that are not named on such a list will not be authorized to request a certificate.

Documentation of these steps is maintained in the IdenTrust certificate registration system.

3.2.3.2.2 Verification of DBA or Tradename

If the PKI Sponsors want to include a DBA or Tradename the PKI Sponsor must first prove that they have the right to use that name. In order to fulfill this requirement an LRA must request one piece of evidence from the following list that confirms ownership of the DBA or Tradename during the verification process:

- A letter/official legal document, phone call to an independently verified number, or an email from the domain registered to a Government Agency in the jurisdiction of the PKI sponsor's organization legal creation, existence, or recognition that validates the ownership of the DBA or tradename;
- A letter/official legal document, phone call to an independently verified phone number or an email from the domain registered to a verifiable third-party source that validates the ownership of the DBA or tradename;
- A letter/official legal document, phone call to an independently verified phone number, or an email from the domain registered to a Government Agency responsible for the management of such DBAs or tradenames; and/or
- An attestation letter accompanied by documentary support that validates the ownership of the DBA or tradename.

All information obtained by this process will be uploaded and retained electronically to the PKI Sponsor's application. If the information is obtained through a phone call, the

LRA must document in the application the telephone number, the source it was obtained and verified through, and the name and title of the phone call recipient.

3.2.3.2.3 Verification of the Country Code

The LRA will also verify the country associated with the Subject by choosing one of the following processes:

- Verifying the ccTLD with the Domain Name Registrar listed by the PKI Sponsor through verification processes conducted by the LRA of the PKI Sponsor and the organization in Sections 3.2.2 and 3.2.3.
- PKI Sponsors requesting a Certificate that will contain the countryName field and the other Subject Identity Information will be verified by the LRA using the processes listed in 3.2.2 and 3.2.3.

In addition to completing the identification and authentication, the Certificate request must be checked against the following:

3.2.3.2.4 Verification of the Certificate Request

When evaluating the authenticity of a certificate request, the LRA evaluates the affiliation of the PKI Sponsors to the Sponsoring Organization. IdenTrust does not issue ACES business affiliated or SSL Certificates to individual Subscribers without an association to an organization. An Individual defined as a sole proprietorship is eligible with proper verification. This association may be verified through a phone call from an LRA to the organization to confirm the information provided on the application.

In order to verify the authenticity of an SSL Certificate request for a Sponsoring Organization the LRA contacts the PKI Sponsor via the company/organization telephone number independently verified through a third-party data base. The LRA will request to speak to the PKI Sponsor at the organization telephone number and upon confirming identity, will request to verify the validity of the request.

3.2.3.2.5 Verification against High Risk and Denied Request Lists

To ensure that requests for ACES SSL Certificates are properly verified, IdenTrust and Authorized RAs conduct two additional checks when necessary:

1) IdenTrust and Authorized RAs maintains internal lists of prior denied applications identified as posing a risk; and
2) IdenTrust and Authorized RAs will check high risk domain requests against an authoritative third party list prior to issuance.

Information returned from such checks is used during the application process by an LRA within IdenTrust or an Authorized RA when identifying potentially illegitimate Certificate requests. If an Authorized RA is elected to perform verification processes, IdenTrust will verify that the processes used to identify high risk requests and prior denied requests provide a level of assurance that is equal to or greater than the level of assurance provided by the process described below.

3.2.3.2.6 High Risk Request Procedure

To prevent potential phishing, fraudulent use and to take further precautions against potential Compromise, IdenTrust and the Authorized RA maintains a list of prior High

Risk Requests and checks a third-party authority list specifying current High Risk Domain Names. This list is used by LRAs to identify potential risks.

Should an LRA identify an application with any potential risk posed to IdenTrust or a Domain Name listed on the third-party authority list, it will be flagged and brought to the attention of management to complete further internal verification. To prevent high-risk issuance of an ACES SSL Certificate this internal verification will require one or more the following pieces of evidence:

- A call to the Sponsoring Organization;
- Request further documentation from the Sponsoring Organization;
- Careful examination of the FQDN to confirm whether the intent of the Domain Registrant is to imitate or mislead customers of an FQDN on the High Risk FQDN List in order to commit fraudulent or phishing activities (e.g., www.g00gle.com, www.1dentrust.com, etc.) and specific filters that are established at the system level to deny initial applications (e.g., non-US ASCII characters);
- Manual review of all documents and information provided; and/or
- Other verifiable proof as deemed necessary by Authorized RA or IdenTrust management.

3.2.3.2.7 Denied Request Procedure

ACES SSL applications that cannot pass this review, will not be issued an ACES SSL Certificate. If the SSL Certificate application does not pass review, it will be added to a list of previously denied applications and kept for verification purposes of future SSL Certificate applications.

3.2.3.2.8 Verification of gTLD Domains

IdenTrust does not issue SSL Certificates containing general top level domain names (gTLDs) that are not currently approved or in the process of being approved by the Internet Corporation for Assigned Names and Numbers (ICANN). FQDNs containing a gTLD that has not been approved will be rejected in the application process until ICANN finalizes the approval of the gTLD. IdenTrust does not issue SSL Certificates for reserved IP addresses or internal server names and will not issue them for the gTLD domains not approved on these

grounds. IdenTrust has never issued an SSL Certificate to internal names including those that may contain an unassigned gTLD.

3.2.3.3 Other Certificates

Nothing in this policy prohibits the GSA ACES PMO from approving production of other certificates 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

Authority of representatives of Participant CAs, and RAs is established using the procedures described in Section 3.2.2.

Certificates that assert affiliation are issued only after verification of applicant affiliation with an authoritative source within the subscribing organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a reliable means of communication.

Once a subscribing organization has been authenticated (see Section 3.2.2) and has entered into a subscribing organization authorization agreement naming a subscriber as an authorizing official, the authorizing official may appoint and remove other authorizing officials (or sponsors) who are authorized to approve affiliation of applicants and devices, and to request certificate lifecycle events for the subscribing organization, e.g., request suspension of a subscriber's certificate or request revocation of a subscriber's certificate in the event organization-individual affiliation is broken. IdenTrust maintains a list of subscribing organization authorizing officials.

In accordance with Section 3.2.3.2, all requests for device certificates in the name of an organization, are confirmed via a digitally signed email from the sponsor of the ACES SSL certificate, using an ACES Business Affiliated certificate which validates to the ACES Root CA (Federal Common Policy CA).

In addition, IdenTrust complies with the procedures detailed in the ACES CPS Section 3.2.3.2 to confirm that the sponsor submitting the ACES SSL certificate application is associated with and authorized by the organization named in the ACES SSL certificate application. IdenTrust keeps a list of individuals who are authorized by the organization to request a certificate and reconfirms authority when an ACES SSL certificate application is received. IdenTrust will provide an Applicant with a list of the organization's authorized certificate requesters upon the Applicant's verified written request.

CAs and RAs may rely on TAs to provide documentary proof that I&A has been performed according to Section 3.2.3. CAs and RAs may rely on internal TAs to provide documentary proof that identification and authentication has been performed according to Section 3.2.3, and to indicate subscribing organization authorization to affiliate an applicant or device with the subscribing organization.

In the instance where an applicant applies for an affiliated certificate and there is no internal TA, the applicant is provided a subscribing organization authorization agreement and instructed to have it signed by an officer or individual of the subscribing organization able to agree to and bind the subscribing organization to its duties and obligations as described in the agreement. If organization identity has not already been established, the LRA verifies organization identity according to the processes identified in Section 3.2.2 prior to approving issuance of the affiliated certificate.

Certificates issued to subscribers do not assert authority to act on behalf of the subscribing organization in any implied capacity.

Authorization for SSL Certificates shall be through an authorized contact listed with the domain name registrar, a person with control over the domain name, or through communication with the applicant using a reliable method per the CA/B Forum Baseline Requirements.

3.2.6 Criteria for Interoperation

To ensure PKI interoperability, IdenTrust:

- Operates a PKI that has undergone a successful compliance audit pursuant to Section 8 of this ACES CPS;
- Issues Certificates with profiles as described in Section 7.1; and
- Makes ACES PKI Certificate Status information available to Relying Parties in accordance with Section 2 of this ACES CPS,

  CRL Distribution:
  http://validation.identrust.com/crl/acesca2.crl

  AIA:
  http://validation.identrust.com/certs/acesca2.p7c

  OCSP:
  http://aces.ocsp.identrust.com

3.3 IDENTIFICATION & AUTHENTICATION FOR RE-KEY AND RENEWAL

The procedures for accomplishing Certificate Renewal, Update, and Routine Re-Key are contained in Section 3.3.

3.3.1 Identification and Authentication for Routine Certificate Re-key

Subscribers shall identify themselves for the purpose of Re-keying through use of their current signature key. Routine Re-key will occur at certificate renewal, which will occur no more than three (3) years, based on certificate validity period, from the most recent key issuance. If it has been more than nine (9) years since a subscriber was identified or any personally identifying information has changed, identity shall be established through the initial registration process described in Section 3.1.

For SSL Certificates, the PKI Sponsor will follow the same steps for verifying the information in their Certificate for the SSL Certificate. PKI Sponsors may also opt to add, remove or edit FQDNs during Re-key. If the contents of the SSL Certificate have changed (the FQDN(s) and Organization information) the RA will request verification information in accordance with the verification processes set forth in Section 3.1 before the Re-key process can be completed.

Updating a certificate means creating a new certificate that has a different key, a different serial number, and different information in some fields than the old certificate. In the event that subject information and/or the key pair change, the Subscriber is required to 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, renewed, or updated. If an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to

IdenTrust, an Authorized RA, a Trusted Agent, or other designated agent in order for an updated certificate having the new name to be issued. If an individual's authorizations or privileges change, the Authorized RA, Trusted Agent or other designated agent will verify those authorizations, and if any authorizations have reduced, the old certificate must be revoked.

A certificate that has not been Re-keyed or updated by the end of its operational period shall reflect an expired status.

IdenTrust shall Re-key or update ACES Certificates issued to Relying Parties only after completing successful identity proofing verification in accordance with the requirements for identity proofing specified in Section 3.2.3

3.3.2 Identification and Authentication for Renewal

IdenTrust accepts ACES Certificate renewal requests from Subscribers within 90 days prior to the scheduled end of the operational period (expiration date) of the ACES Certificate, provided that the Certificate is not revoked, suspended, or expired. Identity proofing for an ACES Certificate renewal (signing and encryption) is limited to a 9-year period. For example, if it has been less than nine (9) years (i.e., one 3-year term and two 3-year renewal) since a subscriber was identified as required in Section 3.2, then IdenTrust will authenticate a Subscriber's electronic request for a new certificate for a 3-year term using the currently valid certificate issued to the subscriber by the CA. Each new certificate issued as the result of a renewal will include a new Key Pair.

During the registration process, IdenTrust requires that the Subscriber designate at least one ACES Relying Party Application with which the Subscriber will interact.

3.3.3 Identification and Authentication for Re-key or Renewal after Revocation

Applicants without a valid ACES Certificate (e.g., where an ACE Certificate has been revoked, suspended, or expired) shall be re-authenticated by IdenTrust or an Authorized RA or Trusted Agent through a new ACES Certificate application, as described in Section 3.2 just as with an initial applicant registration, and shall be issued a new ACES Certificate.

3.4 IDENTIFICATION & AUTHENTICATION FOR REVOCATION REQUEST

IdenTrust may revoke certificates when requested, at any time for any reason. In accordance with the ACES CP, 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. The identity of the person submitting a Revocation request in any other manner shall be authenticated in accordance with Section 4.9. Revocation requests authenticated on the basis of the ACES Certificate's associated key pair shall always be accepted as valid. Other Revocation request authentication mechanisms may be used as well, including a request in writing and signed by the Subscriber and sent to IdenTrust 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.

SECTION 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	PKI sponsor responsible for the component receiving the certificate

4.1.1.1 Application Form

An applicant for an ACES Certificate shall complete an ACES Certificate application and provide requested information in a form prescribed by IdenTrust and the ACES CP.

4.1.2 Enrollment Process and Responsibilities

Most applicant registrations are initiated through a Web interface on IdenTrust's website even though some require in-person identity proofing at some point during the certificate application process. (Applications may also be initiated and processed through an external hosted Web interface using IdenTrust's secure registration messaging protocol as or a bulk loading process described in Section 4.1.3.) The applicant for a certificate must complete a registration form and acknowledge his or her agreement with and acceptance of the Subscriber Obligations identified in Section 4.5.1.

A Sponsoring Organization or Federal Agency may enter into an agreement with IdenTrust to host its own registration process and interface with IdenTrust's Certificate Manufacturing Architecture via IdenTrust's secure registration messaging protocol for the creation, delivery and management of certificates. The Sponsoring Organization or Federal Agency will be contractually bound to adhere to the applicable provisions of ACES CP and this ACES CPS and to provide registration services in strict accordance with the practices set forth in this Section 4.

4.1.2.1 Applicant Education and Disclosure

At the time of application for a IdenTrust-issued ACES Certificate, applicants are advised of the advantages and potential risks associated with using ACES Certificates to access Relying Parties electronically and Subscribers are provided with information regarding the use of private keys and digital signatures or encrypted messages created with such keys, and other Subscriber obligations as specified in Section 9.6.3 of this ACES CPS.

4.1.3 Enrollment Process / Bulk Loading

A Sponsoring Organization or Federal Agency may enter into an agreement with IdenTrust to process Business Representative Certificates in bulk. The Sponsoring Organization or Federal Agency and IdenTrust appoint Trusted Agent(s) to assist with processing of requests for certificate issuance. IdenTrust's Trusted Agents are identified and authenticated in accordance with Sections 3.2.2 and 3.2.3 Trusted Agents must enter into an agreement and have or obtain an ACES medium assurance certificate to perform and communicate Subscriber identity verification in accordance with the applicable CP. The Trusted Agent performs in-person identification of applicants and collects the information required by Sections 3.2.2 and 3.2.3. The Trusted Agent gathers certificate application information, including name, address, phone number, e-mail address and organization name into a bulk certificate issuance request, which is digitally signed by the Authorized RA or Trusted Agent and securely delivered to IdenTrust for processing.

Printed records, signed declarations and biometric records are either maintained by the Authorized RA or Trusted Agent, or are sealed in a tamper-evident package and delivered to IdenTrust or an Authorized RA for safekeeping. The requirement for recording a biometric of the applicant may be satisfied by providing passport-style photographs to the Trusted Agent. The Trusted Agent verifies the photographs against the appearance of the applicant and the biometrics on the presented credentials and securely incorporates the biometric as a component of the tamper-evident package. Authentication by a Trusted Agent does not relieve IdenTrust or its Authorized RAs of responsibility to verify identifying information by checking official records or maintain records of biometrics.

4.2 CERTIFICATE APPLICATION PROCESSING

Verification of the information provided by the Subscriber must be confirmed by IdenTrust or an Authorized RA or Trusted Agent as accurate before a certificate can be issued.

4.2.1 Performing Identification and Authentication Functions

The applicant's identity and authorization to obtain a certificate, along with applicant's possession of a functioning public/private key pair, are verified during the identity verification process as specified in Section 3.2. Roles or authorizations of the Subscriber that are intended for inclusion in the certificate are also verified, if applicable.

For issuance of 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.

Effective September 8, 2017, IdenTrust and RAs will include checking of CAA records to process validation of FQDNs in Server Certificate applications.

4.2.2 Approval or Rejection of Certificate Applications

A certificate application is approved only when all verification processes are successfully completed to confirm the identity and affiliation (when required) of the applicant.

IdenTrust terminates an applicant registration process if:

- The applicant's identity cannot be established in accordance with identity-proofing requirements;
- Not all forms necessary to establish identity or authorization are submitted on a timely basis
- IdenTrust is unable to verify or process the applicant's payment information (where payment information is required).
- For SSL Certificates, the PKI Sponsor is unable to establish or provide verifiable evidence to IdenTrust or the Authorized RA that they are authorized to request the Certificate for the FQDN from the Domain Administrator or a CAA record is found but 'identrust.com' is not listed as one of the trusted CA domain names.

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.

Upon application rejection, IdenTrust provides the following verification information to the certificate applicant as follows:

- Indicates a failure of identity verification process, and
- Informs the applicant of the process necessary to resume processing of the application.

Upon application rejection, IdenTrust records the following transaction data:

- Applicant's name as it appears in the applicant's request for a certificate
- Method of application (i.e., on-line, 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., on-line, in-person)
- Date/time of verification
- Names of contractors, subcontractors, or entities providing identification services, if any
- 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
- Names (IDs) of contractor's/subcontractor's/entity's processes, if any.

For SSL Certificate requests in addition to the list above the rejection transaction record will include:

- The FDQN requested;
    - Whether or not "identrust.com" was listed as one the trusted CA Domain Names in the CAA record; and
- Whether or not the Domain Name was on the denied or High Risk Request lists.

4.2.3 Time to Process Certificate Applications

Certificate applications will be processed in 3-5 days assuming accurate paperwork is received.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

At the time the subscriber applies for an ACES certificate, IdenTrust authenticates itself to the applicant prior to collecting any identity information by using a digital certificate that identifies IdenTrust's web server and initiates a secure, authenticated (Secure Socket Layer – https://) session with the applicant. Upon issuance of an ACES Certificate, IdenTrust warrants to all Program Participants that:

a) Upon receiving a request for a certificate, IdenTrust issued and will manage the ACES Certificate in accordance with the requirements in the ACES CP.

b) IdenTrust has complied with all requirements in the ACES CP when identifying the Subscriber and issuing the ACES Certificate;

c) It is the responsibility of IdenTrust 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.

d) There are no misrepresentations of fact in the ACES Certificate known to IdenTrust and IdenTrust has verified the information in the ACES Certificate per Section 3.2.

e) Information provided by the Subscriber for inclusion in the ACES Certificate has been accurately transcribed to the ACES Certificate; and

The ACES Certificate meets the material requirements of the ACES CP. The issuance of a subordinate CA Certificate for ACES Certificates verifies:

There are no misrepresentations of fact in the ACES subordinate CA Certificate known to IdenTrust and IdenTrust has verified the information in the ACES subordinate CA Certificate at the time of Issuance as based on the profiles created for that Certificate and in a scripted ceremony as described in Section 6.1.1.1.

IdenTrust maintains a permanent record for every subordinate CA Certificate issuance.

For SSL Certificates, the issuance of a Device Certificate verifies:

1) The PKI Sponsor has the right to use the Domain Name or public IP address at the time of application and verification;

2) The PKI Sponsor was authorized to obtain that certificate from the Domain Name Administrator at the time of application and verification;

3) The information included on the certificate is accurate at the time of application and verification;

4) The information included on the certificate is not misleading;

5) The identity of the PKI Sponsor has been verified according to these identification and authentication policies;

6) The PKI Sponsor has signed and is bound by the Subscriber Agreement;

7) IdenTrust will maintain a publicly accessible Repository for verification of the status of the SSL Certificate; and

8) IdenTrust will revoke the SSL Certificate for any of the reasons listed in Section 4.9.

9) The IdenTrust certificate registration system creates a permanent record for every SSL certificate issuance.

While the Subscriber may do most of the initial data entry, it is still the responsibility of IdenTrust or an Authorized RA or Trusted Agent to verify that the information is correct and accurate. Applicant information is verified either by an in-person review, through a system approach of linked databases containing personnel

information, through personal contact with the Subscriber's sponsoring organization and other means and placed in a customer information file used to track the applicant through the certificate enrollment process.

Databases used to confirm Subscriber attributes are protected from unauthorized modification to a level commensurate with the level of assurance specified for the certificates conveying the Subscriber attributes.

Binding of public keys delivered to IdenTrust with the subscriber's identity is accomplished using means that are as secure as the security offered by the keys being certified. The binding is accomplished using a combination of cryptographic, procedural and other appropriate controls and methods. The methods used for public key delivery are described in Section 6.1.3.

For the handling and delivery of public and private keys, see Sections 3.2..1.1 (Hardware Tokens) 6.1.2, 6.1.3 and 6.1.4. Once a certificate has been approved for issuance, the Subscriber is given an activation code (i.e., a mutually shared secret) and a Uniform Resource Locator (URL) address at which to enter the activation code and their Account Password (i.e., an exclusive shared secret) created during registration in order to retrieve the certificate(s).

Only the Subscriber may generate key pairs for Signing Certificates and the resulting certificate containing the public key is delivered (in PKCS#7 or Raw Certificate format) to the Subscriber by IdenTrust (or an Authorized RA or Trusted Agent) via a secure protocol. Possession of the associated private key is verified after installing the Signing Certificate via a Web interface. IdenTrust generates key pairs for Encryption Certificates and the corresponding certificate is then delivered to the Subscriber via a password-protected PKCS#12 file that the Subscriber manually installs. (this process may optionally be automated via the Web interface on supported platforms.)

IdenTrust's own public key certificate for ACES is made available in a downloadable PKCS#7 file, which is accessible through a link on IdenTrust's ACES website. Other trustworthy means of distributing IdenTrust's CA certificate ("Trusted Certificate") exist and may be used by IdenTrust.

4.3.2 Notification to Subscriber of Certificate Issuance

IdenTrust creates the requested ACES Certificate after the following have occurred: successful completion of the Subscriber identification and authentication process in accordance with the ACES CP, and notification to the applicant thereof through an out-of-band notification process linked to the ACES Certificate applicant's confirmed physical U.S. postal mail address, or equivalent.

4.4 CERTIFICATE ACCEPTANCE

As a condition to issuing the ACES Certificate, certificate applicants are required to indicate acceptance or rejection of the ACES Certificate to IdenTrust and agree to the Subscriber obligations under Section 4.5.1. 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.

4.4.1 Conduct Constituting Certificate Acceptance

Program Participants are advised that they may reject the certificate by promptly notifying IdenTrust. In addition to being advised that downloading the certificate constitutes their acceptance of the certificate, Subscribers must also agree in a Subscriber Agreement that by using the ACES certificate (and failing to notify IdenTrust of any errors, defects or problems) they expressly accept the certificate and its contents. Upon certificate issuance, Subscribers are provided with the contents of the certificate in a human-readable form for their review. IdenTrust records the act of certificate acceptance in accordance with Section 4.5.1.

4.4.2 Publication of the Certificate by the Authorized ACES CA

Sub-CA Certificates are published in the Repository upon Issuance.

The publication of Subscriber Certificates is optional and it is implemented based on the CA particular needs.

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

IdenTrust notifies the ACES PMO when it has issued any new ACES subordinate CA Certificate.

When IdenTrust Re-keys by updating its private signature key and thus generates a new public key, it will notify all CAs, Authorized RAs, and subscribers that rely on its CA certificate that it has changed its keys. IdenTrust will generate a key rollover certificate, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Where distribution of a new self-signed certificate to current users is required, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Through a combination of online processes and printed forms, each applicant for an ACES Certificate shall:

- provide complete and accurate responses to all requests for information made by IdenTrust (or a Trusted Agent or 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;
- promise to protect a private keys at all times, in accordance with the applicable Subscriber Agreement, this ACES CPS, the ACES CP and any other obligations that the Subscriber may otherwise have;
- use the ACES Certificate and the corresponding private key exclusively for purposes authorized by the ACES CP and only in a manner consistent with the ACES CP;
- instruct IdenTrust (or an Authorized RA or employer) 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 ACES Certificates, whenever the Subscriber is no longer affiliated with the Sponsoring Organization; and
- respond as required to notices issued by IdenTrust or its authorized agents.

Subscribers who receive certificates from IdenTrust shall comply with these requirements as well as those in the ACES CP. Additional information concerning the rights and obligations of Subscribers may be found in Sections 1.3, 3.1 and 4.1 of this ACES CPS.

4.5.2 Relying Party Public Key and Certificate Usage

The ACES CP is binding on each Relying Party and governs its performance with respect to its application for, use of, and reliance on ACES Certificates.

a) Acceptance of Certificates. Each Relying Party will validate ACES Certificates issued by all Authorized CAs;

b) Certificate Validation. Each Relying Party will validate every ACES Certificate it relies upon with the Authorized CA that issued the certificate; and

c) Reliance. A Relying Party may rely on a valid ACES Certificate for purposes of verifying the digital signature only if:

- the ACES Certificate was used and relied upon to authenticate a Subscriber's digital signature for an application bound by the ACES CP;
- prior to reliance, the Relying Party (1) verified the digital signature by reference to the public key in the ACES Certificate, and (2) checked the status of the ACES Certificate by generating an appropriate status request via a current CRL, OCSP, or other comparable validation method, as approved by GSA, and (3) a check of the certificate's status indicated that the certificate was valid; and
- the reliance was reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of reliance.

Relying Parties are responsible for deciding whether or how to check the validity of ACES Certificates by checking the appropriate certificate status information. A Relying Party may use information in the ACES Certificates (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

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 the ACES CP or this ACES CPS. Relying Parties who rely on stale CRLs do so at their own risk. See Section 4.9 (Certificate Revocation and Suspension).

Parties who rely upon the certificates issued under the ACES CP or this ACES CPS 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.

4.6 CERTIFICATE RENEWAL

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

Where a valid certificate has 90 days or less until the date of its expiration, then using such certificate as the basis the subscriber of such certificate can apply for a new certificate via an online request for a renewal. In the event that an application for renewal is not approved, then renewal of the certificate that was the basis of such renewal request is not possible.

4.6.1 Circumstance for Certificate Renewal

Provided a subscriber has a valid certificate with 90 days or less until the date of its expiration, such subscriber can request a renewal of such certificate.

Certificates may also be renewed when IdenTrust Re-keys a sub CA.

4.6.2 Who May Request Renewal

IdenTrust only accepts requests for certificate renewal from subscribers; provided, however, IdenTrust may perform renewal of subscriber certificates without a corresponding request in certain circumstances, such as when the CA is Re-keyed.

4.6.3 Processing Certificate Renewal Requests

The Subscriber requests a renewal by accessing an online website, which requires presentment of the expiring certificate to authenticate the request. Following successful authentication, the request is submitted to the CA or RA for approval.

Subscribers will authenticate themselves for the purpose of renewal as required in Section 3.3.2, Identification and Authentication for Renewal.

Requests for renewal must be refused where IdenTrust has previously received and authenticated a notice of compromise of the Private Key corresponding to the certificate that is the basis of such request.

4.6.4 Notification of New Certificate Issuance to Subscriber

IdenTrust notifies 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

IdenTrust publishes renewed certificates in accordance with Section 4.4.2, Publication of the Certificate of this ACES CPS.

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

IdenTrust provides 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 a new certificate with a different Public Key (and serial number) while retaining the remaining contents of the previously issued certificate that describes 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.

Re-key of a Certificate does not violate the requirement for name uniqueness.

After a Re-key, the initial certificate may or may not be revoked, but must not be further Re-keyed, renewed, or modified.

In the event a request for a Rekey is not approved, then Re-key is not possible.

4.7.1 Circumstance for Certificate Re-Key

Provided a subscriber has a valid certificate, such subscriber can request a Re-key of such certificate.

A request for a Re-key must be made via an online request and validated by presentment of the certificate to be Re-keyed. Re-key requests are processed according to the same processes and limitations as applied to certificate renewals as described in Section 4.6.1 Circumstance for Certificate Renewal. In the event that the certificate cannot be validated via online presentment, and/or if a change to subject information is required, then a new certificate must be requested.

Subscribers will authenticate themselves for the purpose of Re-key requests as required in Section 3.3.1, Identification and Authentication for Routine Re-Key.

The minimum requirement for all ACES certificate Re-keying, with the exception of the IdenTrust sub-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 a Re-key using such certificate as the basis for such request.

IdenTrust, sponsoring organizations, and RAs may request certification of a new public key on behalf of subscribers.

4.7.3 Processing Certificate Re-Key Requests

Requests for certificate Re-key are processed according to the same processes and limitations as applied to certificate renewals as described in Section 4.6.3 Processing Certificate Renewal Requests.

Subscribers will authenticate themselves for the purpose of renewal as required in Section 3.3.1, Identification and Authentication for Re-Key.

Requests for a certificate Re-key must be refused where IdenTrust has previously received and authenticated a notice of compromise of the Private Key corresponding to the certificate that is the basis of such request.

4.7.4 Notification of New Certificate Issuance to Subscriber

IdenTrust notifies 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 IdenTrust sub CA certificates 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

IdenTrust provides 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

IdenTrust does not allow modification of an existing Subscriber certificate. In a case where Subscriber information has changed (such as address, a name change due to marriage, addition of a degree, etc.) the Subscriber is required to apply for a new certificate and is subject to all identity verification procedures as described in Section 3 Identification and Authentication.

4.8.1 Circumstance for Certificate Modification

IdenTrust may modify its 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.

Not applicable for Subscriber certificates.

4.8.2 Who May Request Certificate Modification

Subscribers requiring modification of their existing certificate must apply for a new certificate.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the Authorized ACES CA

In the event of a change to an IdenTrust ACES sub-CA certificate IdenTrust publishes modified IdenTrust certificate 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

In the event of a change to an IdenTrust ACES sub-CA certificate, IdenTrust provides 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

4.9.1 Circumstances for Revocation

An ACES certificate is revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid.

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:

a) When any of the identifying information, affiliation components or attributes contained in the certificate become invalid;

b) When the private key, or the media holding the private key, associated with the ACES Certificate is, or is suspected of having been, compromised; or if it is an SSL Certificate, no longer complies with the CA/B Forum Baseline Requirements;

c) IdenTrust obtains evidence that the Certificate was misused;

d) When the individual named as a Business Representative no longer represents, or is no longer affiliated with, the Sponsoring Organization;

e) The Subscriber or other authorized party, as defined in an applicable agreement (e.g., Bulk Submission Agreement), asks for his/her certificate to be revoked.

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

IdenTrust will revoke the certificate:

a) If the private key is suspected of compromise;

b) If the Subscriber can be shown to have violated the stipulations of its Subscriber agreement;

c) If IdenTrust learns, or reasonably suspects, that the Subscriber's private key has been compromised;

d) If IdenTrust determines that the ACES Certificate contains a deceptive name or is used for unethical purposes such as, but not limited to, promoting malware or illegal software;

e) If IdenTrust determines that the ACES Certificate was not properly issued in accordance with the ACES CP and/or this ACES CPS; or

f) Other circumstances requiring revocation exist (e.g., the binding in the certificate between subject attributes and the subject's public key are no longer considered valid).

IdenTrust may also revoke a certificate:

a) upon failure of the subscriber (or the sponsoring organization, where applicable) to meet its obligations under the ACES CP, this ACES CPS, or an applicable agreement, regulation, or law;

b) upon a determination that the certificate has become unreliable or that material information in the application for a certificate or in the certificate itself has changed or has become false or misleading (e.g., the subscriber changes his or her name);

c) upon a determination that a the certificate has been used for unethical purposes to include, but not limited to, promoting malware or illegal software.

d) a governmental authority has lawfully ordered IdenTrust to revoke the certificate; or

e) there are any other grounds for revocation. An agreement with a sponsoring organization or participating agency may limit or extend these circumstances for revocation.

Whenever any of the above circumstances occur, IdenTrust will revoke the certificate and include all revoked certificates in all new publications of certificate status information until the certificate expires.

Specific Circumstances for ACES SSL Certificates and Revocation:

a) IdenTrust is made aware of any circumstances indicated that the use of a FQDN or public IP address in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or service agreement between the Domain Name Registrant and the PKI Sponsor has been terminated, or the Domain Name Registrant has failed to Renew the Domain Name); or

b) The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

c) IdenTrust is made aware that an ACES SSL Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name.

d) 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.

Note: IdenTrust does not issue ACES SSL Wildcard Certificates at the time of this publication.

4.9.2 Who Can Request Revocation

The only persons permitted to request revocation or suspension of an ACES Certificate issued pursuant to the ACES CP are the Subscriber, the Sponsoring Organization or Federal Agency (where applicable), IdenTrust, and the Authorized RA or Trusted Agent who performed identity verification.

4.9.3 Procedure for Revocation/Suspension Request

An ACES Certificate revocation or suspension request should be promptly communicated to IdenTrust, either directly to IdenTrust or through an Authorized RA or Trusted Agent authorized to accept such notices on behalf of IdenTrust. 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 IdenTrust or its Authorized RA or Trusted Agent in person and providing adequate proof of identification in accordance with

the 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 revocation request must so indicate. If an Authorized RA or Trusted Agent 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; for signed requests (e.g. digitally or manually signed) from the certificate subject, or from an Authorized RA, verification of the signature is sufficient.

Upon receiving a revocation request, IdenTrust places the certificate on suspended status and unless prohibited by law, notifies the subscriber of the request. IdenTrust assists the requester in identifying the specific certificate(s) to be revoked by supplying a list of all certificates issued to the requester, as appropriate. IdenTrust then verifies the revocation request through procedures similar to those originally used for certificate issuance. If IdenTrust is able to adequately confirm that the person making the revocation request is authorized to do so, the certificate is revoked and the repository is updated. Except as prohibited by law, the subscriber is notified of the certificate's status using an out-of-band notification process linked to the subscriber's physical postal mail address.

Revocation or suspension of a certificate shall take effect immediately upon receipt of a valid revocation request. Information about a revoked certificate shall remain in the status information until the certificate expires.

Device certificates can be revoked by additional methods. The PKI Sponsor can revoke the certificate once they authenticate and request a revocation on a secure online web page using a Server-Authenticated SSL/TLS Encrypted Session and the account number and account password used by the PKI Sponsor during initial registration. If the PKI Sponsor no longer has the account number or cannot remember the account password, then identifying information of the PKI Sponsor obtained during registration can be used to authenticate the PKI Sponsor's request (e.g., the PKI Sponsor can be called at the phone number previously established during registration.) Device certificates can also be revoked after a conclusive investigation of certificate that is initiated by a report received by the problem reporting page that is conducted in accordance with procedures described below. In addition, a digitally signed request from the PKI Sponsor that enables the LRA to link the PKI Sponsor to the certificate, using the electronic records in the Authorized Registration Authority or CA system, is considered valid.

Certificate Problem Reporting, Investigation and Response

IdenTrust provides Subscribers, Relying Parties, application software suppliers and other third parties with clear instructions and contact information for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, Compromise, misuse, inappropriate conduct, or any other matter related to the ACES Certificates. These instructions are available online at the IdenTrust website in the support section at www.IdenTrust.com. This page lists a telephone number to contact help desk representatives during business hours and an email contact to ensure reporting will be received 24/7.

Once a report is received either by email or telephone, a help desk representatives will file a ticket for the report including the details provided by the contact. The help desk representative will provide the following information for the report when possible:

- Account number;
- Name and Contact Information of the Individual/Organization Reporting the Certificate;
- Subscriber, Organization, Domain and/or PKI Sponsor name;

- Nature of the Issue (illegal activity, Private Key Compromise, etc.); and
- When the issue was discovered.

Once a ticket is filed the help desk representative will forward that ticket information including the details and ticket number, via email, to the appropriate level of management or the Security Office. Upon creating a record of the contact the following considerations are assessed to determine the appropriate action:

- The nature of the alleged problem;
- The number of Certificate problem reports received about a particular Certificate or Subscriber; and
- The entity making the complaint (for example, a complaint from a law enforcement official that a web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that he/she didn't receive the good they ordered); and relevant legislation.

Upon review, the Security Office, or an appropriate level of management, will determine whether revocation, suspension, or other action is warranted. If it is determined that revocation or suspension is necessary, security or management will send an official request to a help desk representative or an LRA to execute the specified action accordingly. When deemed necessary based on the content of the report and the findings by security and management, IdenTrust will forward the complaint to law enforcement.

All email contact associated with the case must be saved and documented by the help desk representative.

To respond to high-priority Certificate problem reports IdenTrust maintains the Certificate problem reports support page 24/7 whether by telephone contact during office hours or email contact during evening, weekend or holiday hours.

4.9.4 Revocation Request Grace Period

There is no grace period for an ACES revocation request.

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

IdenTrust will revoke a certificate within two (2) business days of receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

IdenTrust shall have no liability if a Relying Party does not obtain an OCSP response indicating that the certificate is valid (in accordance with Sections 4.9.9 and 4.9.10) or fails to check the most recent ARL/CRL for certificate revocation.

4.9.7 CRL Issuance Frequency

When CRLs are used to distribute status information:

- They shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information;
- Superseded certificate status information shall be removed from the repository system upon posting of the latest certificate status information;

- The issuance frequency for CRLs shall be at least once every 18 hours and for ARLs every 24 hours, although IdenTrust may issue CRLs more frequently;
- Certificate status information shall be published not later than the next scheduled update, and
- CRL issuance for reasons of loss or compromise of private key shall take place within 18 hours of notification.

When a CA certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL is issued within six hours for all subscriber certificates that CA has issued and an ARL is issued within six hours of notification for that CA.

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

IdenTrust makes certificate validation available via CRL checking and Online Revocation/Status Checking (OCSP) that also supports the GET Method for retrieval of validation information for Certificates issued in accordance with the CA/B Forum Baseline Requirements.

IdenTrust validates online, near-real-time (as current as the last CRL) the status of all ACES Certificates indicated in an ACES Certificate validation request message, via OCSP as defined in RFC 6960.

The certificate status available via OCSP is at least as current as the certificate status available via CRL lists.

IdenTrust CRL and OCSP services resources are sufficient to provide a response time of ten seconds or less under normal operating conditions.

The OCSP Responder signing certificate contains an extension of type id-pkix-ocsp- nocheck, as defined by RFC 6960.

Upon receipt of a signed Certificate Validation Request message from an agency application, IdenTrust:

1) Verifies the signature on the Certificate Validation Request,
2) Generates and returns a signed Certificate Status Response message, and
3) Indicates the certificate status as one of the following:
    a) Valid. Indicates that the certificate is usable (other validation methods such as OCSP would indicate a certificate status of “good”).

        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.

    b) Invalid. Indicates that the certificate either has been revoked or is beyond its operational period.
        i) CRL-based validation would show the certificate on the CRL as “revoked” and would supply a reason
        ii) Flag where all reasons except “certificateHold” constitutes an Invalid certificate, in accordance with RFC 5280 and its successors.

iii) OCSP-based validation would indicate a "revoked" state and that the certificate has been revoked (and not marked as temporarily “on hold”), in accordance with RFC 6960 or its successors).

iv) Suspended. Indicates that the certificate has been placed in suspended status pending validation of a revocation request. See Section 4.5.

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.

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.

IdenTrust maintains an online 24x7 publicly accessible Repository that application software providers can use to automatically check the current status of all unexpired and revoked Certificates issued by the IdenTrust and maintains a continuous 24x7 ability to respond internally to a security incident.

Suspension of certificates can be determined by one or both of the methods below:

1) CRL-based validation would show the certificate on the CRL as “revoked” with a reasonFlag of “certificateHold,” in accordance with RFC 5280 and its successors.

2) OCSP-based validation would indicate a "revoked" state and that the certificate is temporarily “on hold,” in accordance with RFC 6960 and its successors.

If the OCSP responder receives a request for status of an SSL Certificate that has not been issued, the responder will reply with an “unknown” status.

4.9.10 Online Revocation Checking Requirements

Each Relying Party will validate every ACES Certificate it relies upon, with such validation to be conducted by such Relying Party in conformity with the terms of the ACES CP and this ACES CPS. See Section 4.9.7 for CRL checking requirements.

4.9.11 Other Forms of Revocation Advertisements Available

IdenTrust reserves the right to make other forms of revocation advertisement available to Relying Parties and in such cases will, at a minimum, adhere to all requirements pertaining to CRL issuance and latency.

Each Relying Party will validate every ACES Certificate it relies upon, with such validation to be conducted by such Relying Party in conformity with the terms of the ACES CP and this ACES CPS.

4.9.12 Special Requirements Related to Key Compromise

If or when an IdenTrust 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:

CRL Issuance Table

Assurance Level	Maximum Latency for Emergency CRL Issuance
Basic	24 hours after notification
Medium (all policies)	18 hours after notification

See Section 4.9.5 for additional information regarding latency of CRL publishing following notification of revocation.

4.9.13 Circumstances for Suspension

All Certificates, except for SSL Certificates, 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.

4.9.15 Procedure for Suspension Request

See Section 4.9.3.

4.9.16 Limits on Suspension Period

There are no limits on the period of time a certificate may be in a suspended status.

4.10 CERTIFICATE STATUS SERVICES

IdenTrust uses OCSP and ARLs/CRLs to distribute status information as specified by the ACES CP. To the extent practical, the contents of changes in status shall be checked before posting to ensure that all information is correct.
Revocation entries on the ARLs/CRLs or OCSP Response will not be removed until after the Expiry Date of a revoked Certificate.

4.11 END OF SUBSCRIPTION

Each Certificate issued under this ACES CPS includes within it a date identifying a day on which the Certificate expires, and such Certificate expires at the end of such day unless earlier revoked per the terms the applicable CA-Subscriber agreement.

4.12 KEY ESCROW AND RECOVERY

IdenTrust only offers keyEncipherment for SSL certificates. Encryption is not offered for Subscriber certificates; therefore IdenTrust does not currently maintain a Key Recovery Policy document for the ACES program.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable. IdenTrust does not offer encryption certificates at this time.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

4.12.2.1 Circumstances for private key recovery

Not applicable

4.12.2.2 Key Recovery Roles: Who can request private key recovery

Not applicable

4.12.2.2.1 Key Recovery Agent

Not applicable

4.12.2.2.2 Key Recovery Officials

Not applicable

4.12.2.2.3 Internal Requestors

Not applicable

4.12.2.2.4 External Requestors

Not applicable

4.12.2.3 Procedure for Private Key Recovery Request

Not applicable

4.12.2.3.1 Automated Self-Recovery

Not applicable

4.12.2.3.2 Recovery via KRA

Not applicable

SECTION 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

IdenTrust and its associated Trusted Agents, Authorized RAs, CMAs, and Repositories shall establish and maintain security controls to assure adequate security for all information processed, transmitted, or stored in the IdenTrust CA the in accordance with the ACES CP, this CPS, the SSP and the PPP.

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.

IdenTrust is required to have the following minimum security controls in place:

- Technical and/or security evaluation complete
- Risk assessment conducted
- Rules of behavior established and signed by users

- Contingency Plan developed and tested
- Security Plan developed, updated, and reviewed
- System meets the moderate level of controls set forth in latest set forth in NIST SP 800-53 Rev. 4, tailored in accordance with NIST SP 800-171, Rev. 1
- In-place and planned security safeguards appear to be adequate and appropriate for the system and consistent with NIST 800-53 revision 4 Moderate level of controls as described above. No party may use any software, program, routine, query, device or manual process in an attempt to: bypass security measures (including attempting to probe, scan or test vulnerabilities to breach security); access data for which they are unauthorized to access; interfere with the proper working of IdenTrust's CA systems; or impose a disproportionately large load on (i.e., overload or crash) the infrastructure supporting IdenTrust's systems (e.g., DOS/DDOS attacks, viruses, etc.). The unauthorized use of any robot, spider, software, routine, meta-search, automated query to monitor, copy or make any other unauthorized uses of IdenTrust's systems is strictly prohibited and will be prosecuted to the fullest extent allowed by law. IdenTrust reserves the right to block any activity that it interprets as a runaway application, attack or other event that might be an attempt to bring down IdenTrust's ACES PKI infrastructure and systems.

System Security Plan

IdenTrust has prepared and maintains a System Security Plan (SSP) in accordance with requirements set forth in NIST SP 800-18 Rev. 1, NIST SP 800-34 Rev. 1, and NIST SP 800-53 Rev. 4, and the ACES MOA.

Risk Management

IdenTrust conducts periodic risk assessments and maintain its ACES systems at the level of residual risk in accordance with, NIST SP 800-34 Rev. 1, NIST SP 800-53 Rev 4 and the associated ACES MOA.

Rules of Behavior

The SSP includes the rules of conduct that will be used to instruct IdenTrust's officers and employees in compliance requirements and penalties for noncompliance. IdenTrust's rules of behavior are developed and implemented in accordance with requirements set forth in NIST SP 800-18 Rev. 1, NIST SP 800-34 Rev. 1 and NIST SP 800-53 Rev. 4 and the ACES MOA.

Contingency Plan

IdenTrust develops, implements, maintains, and periodically tests its contingency plan for its ACES system in accordance with guidelines provided in NIST SP 800-34 Rev. 1 and NIST SP 800-53 Rev 4.

Incident Response Capability

IdenTrust is able to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. A security incident is defined to be any adverse event that threatens the security of information resources. Adverse events include compromises of integrity, denial of service, compromises of confidentiality, loss of accountability, or damage to any part of the system.

Incident response procedures and reporting of security incidents shall be in accordance with guidelines provided in NIST 800-61 Computer Security Incident Handling Guide Rev. 2.

Physical Security

For each system, an individual should be a 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. This person shall be made explicitly responsible for making physical security checks.

5.1 PHYSICAL CONTROLS

IdenTrust's physical and environmental security program addresses all access control items as specified in the ACES CP, in that IdenTrust confirms each respective datacenter provider for protection against these possibilities. In addition, IdenTrust has a documented business continuity plan and security incident response plans that provide contingencies in case any one of the named disasters does occur.

IdenTrust, and all associated Trusted Agents, Authorized RAs, CMAs, and Repositories, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing IdenTrust services. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section 5.2.1.

The IdenTrust security program includes an annual risk assessment conducted by Security Officers and other trusted personnel as directed by the Risk Management Committee. This program includes identifying foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate data or Certificate management processes. It also assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate data and Certificate management processes. In addition, it assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that IdenTrust has in place to counter such threats.

5.1.1 Site Location and Construction

IdenTrust implements the physical security requirements that include:

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

5.1.2 Physical Access

IdenTrust provides physical access controls designed to provide protections against unauthorized access to ACES system resources.

5.1.2.1 Physical Access for CA Equipment

IdenTrust implements physical security of CA equipment to encompass the following:

- 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 are commensurate with the level of threat in the equipment environment.

- The physical requirements are intended to ensure no unauthorized access to the hardware is permitted, to ensure all removable media and paper containing sensitive plain-text information is stored in secure containers, to ensure that the physical site is manually or electronically monitored for unauthorized intrusion at all times, to ensure that an access log is maintained and inspected periodically, and to require two-person physical access control to both the cryptographic module and computer system.
- Physical access controls shall restrict the entry and exit of personnel, equipment and media from any area containing a local area network (LAN) server.

IdenTrust's CA system is housed in an enclosed secure data center, the perimeter of which is access-controlled through a keycard system. In addition, the perimeter of the building is secured with surveillance cameras 24 hours a day, 7 days a week.

To enter the building, personnel must pass through doors requiring keycard access and a PIN number. The entryway of the building is also monitored with surveillance cameras. To gain access to the offices and work area, a keycard is required. All keycard accesses in the facility are logged and copies of logs gaining entry to the IdenTrust secure room, discussed below, are provided to and retained by IdenTrust.

In addition to other layers of security implemented in the facility, an additional layer of security protects the secure room containing the CA equipment. Limited to authorized personnel, access to this room can only be gained by two individuals acting together, each of whom must be authenticated through a two-factor biometric-controlled door system. This secure computer room is monitored at all times with surveillance cameras. Finally, all CA and repository equipment is located in secure, locked computer cabinets and require physical or electronic keys for access.

Removable cryptographic modules are inactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers.

- Activation information and cryptographic modules are stored in separate containers

IdenTrust's CA facility is manned on a 24-x-7 basis. A log identifying the person guarding/monitory the facility is maintained. During surveillance and security checks of the facility housing IdenTrust's CA system, IdenTrust verifies that:

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

5.1.2.2 Physical Access for RA Equipment

The IdenTrust office, entries, and the room where the RA equipment is located are video-recorded. The IdenTrust Security Office performs periodic checks and reviews of the security integrity of the facilities to ensure that alarms, access points, video cameras, storage containers, access logging, etc., are operational and/or functioning correctly. A record is kept that describes the types of checks performed, the times, and the persons who performed them. Records are kept for no less than one year and reviewed with external auditors annually as part of the WebTrust for Certification Authorities audit.

IdenTrust personnel require programmable electronic access cards to access the IdenTrust office space and the RA room. Access cards for personnel working in IdenTrust's offices are granted only upon authorization from the IdenTrust Security Office.

Employees are prohibited from permitting unknown or unauthorized persons to gain access to the RA room. Authorization to enter must be obtained in advance from Operations Management. Visitors are allowed within the LRA room only after properly identifying themselves and the purposes for their visits. Visitors are not allowed to roam without escorts. All entry to the RA Room is logged, either electronically or manually, with the respective dates and times of access.

Cryptomodules used to access RA workstations require Activation Data that is memorized and not written down. When not in use, modules are locked or under control of their primary users.

5.1.2.3 Physical Access for CSS Equipment

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

5.1.3 Power and Air Conditioning

IdenTrust's data center has been designed to augment the security and safety of the facility. The building is constructed to withstand earthquake, fire, moisture and heat. Air conditioning is provided in a fully redundant fashion around the perimeter of the computer room. Air conditioning and water pipes are separated from the rest of the computer room. Environmental sensors signal an operator console that is staffed 24 hours a day, 7 days a week.

Communications are provided through two separate access points to the building. The facility maintains its own UPS and backup generator, which are tested routinely. Flood exposure is minimal to non-existent at the site.

More detail can be found in the SSP which addresses the following in more detail: access controls, fire safety, failure of supporting utilities, structural collapse, interception of data, mobile and portable systems in accordance with Federal regulations.

5.1.4 Water Exposures

The subflooring is equipped with water sensors. Water pipes are separated from the rest of the computer room. Environmental sensors signal an operator console that is staffed 24 hours a day, 7 days a week. More detail can be found in the SSP which addresses the following in more detail: access controls, fire safety, failure of supporting utilities, structural collapse, interception of data, mobile and portable systems in accordance with Federal regulations.

5.1.5 Fire Prevention and Protection

IdenTrust houses its information processing facilities in a building designed to serve as a hardened data and control center for a major natural gas company in the Intermountain West. As such, the building is equipped with advanced fire response aspects including:

- Fire-retardant construction materials;
- Advanced chemical, smoke, and heat-based detection systems;

- Water-based sprinkler fire suppression in business suites;
- Inergen inert atmospheric gas fire suppression in the secure room;
- 24x7 onsite operators with fire control console/panel access; and
- Seismic separation between the secure room and office space, which also serves as an interstitial gap to thwart fire spread.

In addition, computer rooms (such as the secure room where CA, CSA, CMS and RA Systems are housed) are equipped with riot doors, fire doors, and other doors resistant to forcible entry.

A description of the IdenTrust disaster recovery plan in the event a fire disaster should occur is contained in Section 5.7.4.

5.1.6 Media Storage

- All media is backed up, stored, transported, and disposed of in accordance with Federal requirements.
- CA media is stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from IdenTrust's sites of operation.

5.1.7 Waste Disposal

IdenTrust policy prohibits any media from leaving organizational control that does contain or has contained sensitive data. Such media is destroyed as described below when it reaches end-of-life.

After it is no longer needed, all sensitive information is securely destroyed using procedures that are approved by the Security Office and are consistent with Federal regulations, GSA policy, and other supporting GSA security guidelines. Employees are prohibited from destroying or disposing of potentially important records or information without specific advance management approval.

All outdated or unnecessary copies of printed sensitive information are shredded using in-office equipment, or disposed of in a secure waste receptacle that is shredded onsite by a bonded company that specializes in disposing of sensitive information and under the direct observation of a Trusted Role employee.

When sensitive CA information is erased from a disk, tape, or other magnetic storage media, the erasure is followed by a repeated overwrite operation, using approved secure-delete programs. This prevents the information from later being scavenged. Alternatively, degaussers, shredders, and/or other equipment and procedures approved by the Security Office are employed.

The Security Office is contacted for assistance in disposing of media and equipment no longer being used by the CA, RA and Repository systems. Such media and equipment are stored at a level of security appropriate to the level of sensitivity of information contained in the media and equipment until they can be effectively sanitized or destroyed. Key materials, for example, are stored in a safe within the IdenTrust Secure Room, as described in Section 5.1.2.1.

Cryptographic modules remain in locked safes within the Secure Room; sensitive backup tapes remain in the offsite secure location's vault prior to destruction. All cryptographic modules are zeroized after the keys on them are no longer needed. If zeroization procedures fail, then they are physically destroyed. Destruction techniques vary depending on the medium in question. Methods of destruction include:

☐ Incinerating cryptographic modules, hard disks, and similar items

- ☐ Crushing cryptographic modules, hard disks, and similar items
- ☐ Shredding, cutting, stretching, and/or otherwise destroying magnetic tapes
- ☐ Shredding paper

5.1.8 Off-Site Backup

Systems are 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 are properly documented; understood by IT personnel; and integrated and coordinated with IdenTrust's disaster recovery plan.

Backups are performed by IdenTrust and stored off-site not less than once per week. Weekly, monthly and yearly backup of magnetic media shall be rotated and transported to an off-site storage facility. Full system backups, sufficient to recover from system failure, are made on a weekly basis. At least one full backup copy is stored at an offsite location (separate from IdenTrust equipment). A minimum of the latest full backup is retained.

Backup media is stored at a secured alternate data storage site which meets physical and environmental security requirements commensurate to that of the operational 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

There are four primary trusted roles—Administrator, Officer, Auditor and Operator--further defined in Section 5.2.2.

5.2.1 Trusted Roles

IdenTrust 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. Trusted roles defined in the ACES CP include:

1) *Administrator* – authorized to install, configure, and maintain the CA; establish and maintain system accounts; configure profiles, including certificate profiles, and audit parameters; and generate and back up CA and other component keys. Administrators do not issue certificates to subscribers.
2) *Officer* – authorized to register new subscribers, verify the identity of subscribers and the accuracy of information included in certificates, request or approve certificates, certificate revocations and key recovery operations.
3) *Auditor* – authorized to review, maintain and archive audit logs and perform or oversee internal compliance audits to ensure that the CA system and associated RA systems are operating in accordance with this CPS.
4) *Operator* – responsible for the routine operation of the CA equipment and operations, authorized to perform system backup and recovery and change recording media.

Under no circumstances shall the incumbent of a CA role perform its own auditor function.

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

The Authorized ACES CA or RA 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.

5.2.1.1 IdenTrust Trust Roles Definition

All employees, contractors, and consultants of IdenTrust, CAs, RAs and LRAs who have access to or control over cryptographic operations that may materially affect the Issuance, use, Suspension, or Revocation of Certificates, including access to restricted operations of IdenTrust's CA, CSA, RA, LRA Systems and Repository are, for purposes of this ACES CPS, considered as serving in a Trusted Role. Such personnel include, but are not limited to system administration personnel, system operators, engineering personnel, and operations managers who oversee CA, RA or LRA operations. The functions and duties performed by these persons are also separated and distributed by way of practices consistent with the requirements of Section 5.2.4 below, so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI (see Section 5.2.4). Oversight of IdenTrust's Trusted Roles is performed by the Risk Management Committee, Operations Management, the Human Resources Department, and Executive Management.

IdenTrust maintains a list of Individuals performing each Trusted Role. The list is maintained by the CIO and, for audit purposes, the Security Office has an updated copy of the list.

The following table maps the ACES CP Trusted Roles to IdenTrust-internally-defined roles in Sections 5.2.1.1-5.2.1.6. A TA does not necessarily need to be Trusted Roles, but is included here for role clarity.

	IdenTrust Defined Roles								
ACES - CP Role	CA Administrator	Int and Ext RA Administrator	LRA	Help Desk	Security Officer	Operations Manager	System Administrator	Trusted Agent	PKI Consultant
Administrator	X	X							
Officer			X	X					
Auditor					X	X			
Operator	X						X		
Other Role(s)								X	X

5.2.1.2 IdenTrust CA Administrator Role Definition

Within IdenTrust, the ACES Administrator functions are primarily handled by the IdenTrust CA Administrator, as well as RA Administers, both external and internal. This section provides specifics related to each of this role definitions.

IdenTrust CA Administrator Definition

The ACES CA Administrator is a Trusted Role. The CA Administrator's responsibilities and operating procedures, as they relate to CA Operations, are as follows:

- Installation and configuration of the CA software;
- Installation and configuration of Repository software;
- Installation and configuration of the RA software (Internal RA Administrator only);
- Establishing and maintaining CA system accounts;
- Configuration of CRL parameters;
- Configuration of Certificate Profiles;
- Cross-Certificate, Root CA and Sub CA Key management (performed under two person control); and
- Cross-Certification paperwork and workflow of the Root CA and subordinate CAs by the other Bridges.

The CA Administrator ensures the ACES CA Keys will not be used to sign Certificates except in the following cases:

- Self-Signed Certificate to represent the Root CA itself;
- Certificates for Participant CAs and Sub CAs;
- Cross-Certificates;
- Certificates for infrastructure purposes (e.g., administrative role Certificates, internal CA operational Device Certificates, and OCSP Response verification Certificates) and;
- Certificates that are issued solely for the purpose of testing products with Certificates that are issued by the Root CA.

CA Administrators do not Issue to Subscribers.

IdenTrust maintains redundancy in the role of CA Administrators. At least two CA Administrators are maintained in case a primary CA Administrator is on vacation, sick, or otherwise not available.

Within IdenTrust, CA Administrators also carry out the responsibilities of the Certificate Status Authority Administrator. The CSA Administrator responsibilities and operating procedures performed by IdenTrust CA Administrators, as they relate to CSA Operation, are as follow Certification Status Authority ("CSA") Roles as follows:

- Installation, configuration, and maintenance of the CSA software;
- Generating and backing up CSA Keys (performed under two person control);
- Management of CSA Key and Certificate lifecycle, including renewal of OCSP Responder Certificates (performed under two person control);
- Establishing and maintaining system accounts and configuring audit parameters; and
- Operation of the CSA equipment.

Registration Authority ("RA") Administrator Definition

The RAs operating under this policy are subject to the stipulations of the ACES CP and this ACES CPS. In cases where the RA is external to IdenTrust, the RA is obligated by contract and policy to comply with the ACES CP and this ACES CPS.

IdenTrust Internal RA Administrator

The responsibility for RA operations within IdenTrust is carried out by the CA Administrator and, in the case of specific implementations, PKI Consultants. All RAs are required to comply with all RA requirements as outlined in the ACES CP and this ACES CPS.

External RA Administrator

The RA Administrator of an External RA is a Trusted Role with duties for the RA that are similar to those of the CA Administrator for IdenTrust, including the following responsibilities and operating procedures:

Installation, configuration, and maintenance of software on the RA System;

- Generating and managing Keys and the Certificate lifecycle of the RA System; and
- Secure operation and management of the RA System, including patch management, backup, system logging and physical and logical security.

5.2.1.3 IdenTrust Officer Role

Within IdenTrust, the CA Officer responsibilities are performed by an LRA. CA Certificates generation responsibility is also shared by Help Desk Representatives.

Local Registration Authority ("LRA") Role Definition

An LRA is a Trusted Role and performs the roles, responsibilities and operating procedures, as they relate to RA Operations, are as follows:

- Confirming identity via review and approval of documents submitted by TAs and Licensed Notaries;
- Entering Subscriber information, verifying correctness, and approving requests;
- Securely communicating requests to and responses from the CA system;
- Receiving and distributing Certificates;
- Authentication of identity upon request for Revocation and executing Revocation;
- Archival of Subscriber authentication information (i.e., copies of paper forms, etc.);
- Operation of the LRA Systems and Cryptomodules; and,
- Generation of Cross-Certificate, the External Root CA and Subordinate CA's, Re-Keying and Revocation (performed under two person control).

Help Desk Representative Role Definition

IdenTrust's Help Desk Representatives perform the following duties:

- Troubleshooting of Certificate lifecycle events problems;
- Maintaining Subscriber account information within the RA System;
- Initiating Revocation processes;
- Initiating Suspension processes;
- Initiating escalation of suspected Private Key compromise, or other reasons for potential Certificate Revocation;
- Generation of the ACES Root CA Certificate, Sub CA or Participant CA Certificates, CA Certificate Re-Key, and Revocation of CA Certificates (all CA Certificate lifecycle events performed under two person control); and
- Generation of the CMS Certificates and Revocation of CMS Certificates (all CMS Certificate lifecycle events performed under two person control).

5.2.1.4 IdenTrust Audit Role Definition

Within the IdenTrust organization, the Security Officer fulfils the internal Audit function and the Operations Manager provides audit oversight. IdenTrust is also subject to client-conducted audits, as well as external compliance audits, as required by various certificate policies.

Security Officer Role Definition

IdenTrust's Security Office is comprised of a number of Security Officers responsible for reviewing the audit logs recorded by CA, CSA and RA Systems and actions of administrators and operators during the performance of some of their duties. The Security Office operates under the oversight of the IdenTrust Security Officer and the IdenTrust CIO.

A Security Officer reviews logs for events such as the following:

- Requests to and responses from the CA system;
- The Issuance of Certificates;
- Repeated failed actions;
- Requests for privileged information;
- Attempted access of system files, IdenTrust databases or the External RA database;
- Receipt of improper messages;
- Suspicious modifications;
- Performance of archive and delete functions of the audit log and other archive data as described in Sections 5.4 and 5.5 of this document; and
- Administrative functions such as compromise reporting.

The Security Officer performs, or oversees, internal compliance audits to ensure that CA, CSA, RA and LRA Systems are operating in accordance with this ACES CPS, ACES CP and any Memorandum of Agreement ("MOA") applicable to the operation of the IdenTrust ACES PKI. For ACES SSL Certificates, the Security Officer also performs quarterly self-audits to monitor Certificate Issuance quality in accordance with Section 8.1 of this ACES CPS.

Operations Manager Role Definition

A list of IdenTrust Operations Managers (i.e., CIO and other Operations designees below the CIO) is kept at all times as approved and authorized by the Chief Executive Officer (CEO). The Operations Manager performs the following duties:

- Provides internal audit oversight, and works closely with external auditors as needed;
- Handles approval/removal of Network, System and CA Administrators as well as Help Desk Representatives and LRAs;
- Acts as custodian of Activation Data for administrative Cryptomodules used with CA software;
- Works closely with the Security Officer to review requests for privileged information or sensitive system-related requests; and
- Participates as an active member of the Risk Management Committee.

5.2.1.5 IdenTrust Operator Role Definition

Within IdenTrust, the ACES Operator functions are divided between the IdenTrust CA Administrator and the IdenTrust System Administrator.

IdenTrust CA Administrator

See Section 5.2.1.2 for details regarding which tasks specific to the CA Operator role are performed by the IdenTrust CA Administrator.

IdenTrust Systems Administrator

IdenTrust's System Administrator role is aligned with the ACES Operator role. The IdenTrust System Administrators are responsible for the following:

- Installation and configuration of operating systems, and databases;
- Installation and configuration of applications and initial setup of new accounts;
- Performance of system backups, software upgrades, patches, and system recoverability;
- Secure storage and distribution of backups and upgrades to an off-site location;
- Performing the daily incremental database backups; and
- Administrative functions such as time services and maintaining the database.

5.2.1.6 Other Roles

Trusted Agent ("TA")

The Trusted Agent is not a Trusted Role (see Section 1.3.5). TAs differs from LRAs in that they do not have privileged access to the CA system to take action to Approve, Reject or Revoke Certificates.

PKI Consultant

PKI Consultants are IdenTrust employees who coordinate the processes needed to securely on-board new CAs, RAs and LRAs. PKI Consultant responsibilities include:

- Installation and configuration of RA software connecting to CA system and IdenTrust RA System administration;
- Helping distribute Cryptomodules containing RA System Keys; and
- Configuring RA System access rights to CA-provided services.

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 act in the role of 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

The requirements for vetting personnel in Trusted Roles are found below in Sections 5.3.1 and 5.3.2. Identification and authentication for logical and physical access to CA system resources is described in this Section 5.2.3. In accordance with IdenTrust's security policies, IdenTrust CA personnel must first authenticate themselves before they are: (i) included in the access list for any component of the CA system; (ii) included in the access list for physical access to a component of the CA system; (iii) Issued a Certificate for the performance of their Trusted Role; (iv) given an account on a computer connected to the CA system; or (v) otherwise granted physical or logical access to a component of the CA system.

Each of these access methods (Certificates and system accounts) are: (i) directly attributable to the Individual; (ii) password protected; (iii) not shared; and (iv) restricted to actions authorized for that role through the use of

CA software, operating system and procedural controls. If accessed across shared networks, CA operations are secured, using Cryptomodules, strong system authentication, and AES encrypted SSH connections.

5.2.4 Separation of Roles

Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role.

IdenTrust utilizes software and hardware to identify and authenticate its users and ensures that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles.

CA systems identify and authenticate users through the use of access controls and policies. Such controls and policies include safeguards against a user assuming more than one of the roles of Officer, Administrator or Auditor. Additional Separation of Duties controls are discussed in Section 5.2.1 above.

CA, RA and CSA systems also identify and authenticate users and ensure through the use of access controls and policy that no user identity can assume more than one identity in the system.

5.3 PERSONNEL CONTROLS

IdenTrust and its Authorized RA, Trusted Agents, 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 the ACES CP, this ACES CPS, SSP and Federal regulations.

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling Trusted Roles as defined in this ACES CPS shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. Administrators, Officers, Auditors and Operators are selected to fulfill Trusted Roles based on their experience, training and ability. Administrators, Officers, Auditors and Operators are required to demonstrate knowledge and proficiency about: (i) IdenTrust's security principles and mechanisms; (ii) security awareness; (iii) PKI software versions in use on the CA system; (iv) PKI duties they are expected to perform; and (v) disaster recovery and business continuity procedures

5.3.2 Background Screening Check Procedures

All persons accessing IdenTrust's ACES computer systems shall undergo background investigations. Minimum requirements for background investigations and national security clearances shall be based upon position and duties. Individuals shall be screened prior to being authorized for system access and periodically thereafter.

Background screening for personnel appointed in a Trusted Role, at a minimum, must pass a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence (3 Years);
- Law Enforcement; and
- References.

The period of investigation shall cover at least the last five years for each area, excepting the residence check which shall 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 U.S. Executive Order 12968 August 1995, or equivalent.

If the person has been in the work-force for less than 5 years, the employment verification shall consist of the periods during which the person has been in the work-force. At a minimum, the background check will be refreshed every ten years.

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

In some instances, individuals may be given the ability to bypass some significant technical and operational controls in order to perform system administration and maintenance functions (e.g., LAN administrators or systems programmers). Such individuals shall be screened commensurate with the risk and magnitude of harm they could cause. Such screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter.

Least Privilege

Users must be restricted to data files, processing capability, or peripherals, and type of access (read, write, execute, delete) to the minimum necessary for the efficient completion of their job responsibilities. IdenTrust's physical access controls are designed and/or configured to provide least privilege.

Individual Accountability

IdenTrust's physical access controls are designed and/or configured to provide individual accountability. Individual accountability requires the linking of activities on IdenTrust's ACES system to specific individuals, and therefore, requires the system to internally maintain the identity of all active users. IdenTrust allows only one user per account, and users never share user IDs or passwords. The following is a description of how the access control mechanism supports individual accountability and audit trails:

5.3.3 Training Requirements

IdenTrust requires mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of systems used to administer ACES CA and RA services. 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 and GSA security policy and supporting security guidelines.

All personnel performing duties with respect to the operation of IdenTrust's CA system 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
- Understanding common threats to the information verification process (including phishing and other social engineering tactics), for SSL Certificates, understanding the requirements for identification and

authentication of SSL Certificate issuance and passing an examination administered by IdenTrust or the Authorized Registration Authority covering those requirements

5.3.4 Retraining Frequency and Requirements

Individuals responsible for PKI roles shall be aware of changes in CA operation.

Any significant change to CA operations shall have a training (awareness) plan, and the execution of such plan shall be documented**.** Examples of such changes are CA software or hardware upgrade, 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 IdenTrust's services; otherwise, IdenTrust compensates for this control through cross-training including experience in all essential areas.

5.3.6 Sanctions for Unauthorized Actions

IdenTrust shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving IdenTrust or its repository not authorized in the ACES CP, this ACES CPS, or the ACES MOA.

5.3.7 Independent Contractor Requirements

Persons and legal entities, if any, contracted by IdenTrust to perform functions for IdenTrust pertaining to the ACES CP and this ACES CPS shall meet applicable requirements set forth in the ACES CP, this ACES CPS, SSP, and ACES MOA as determined by the GSA.

5.3.8 Documentation Supplied to Personnel

IdenTrust provides documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role. IdenTrust makes available to its CA and Authorized RA personnel the certificate policies it supports, relevant parts of this ACES CPS, and any relevant statutes, policies or Contracts**.**

IdenTrust maintains an inventory of items that comprise its ACES system which is managed under the CM Plan and includes hardware, software, communications, and documentation relating to the ACES Program, and a record of the location of software, including:

- Vendor-supplied documentation for hardware
- Vendor-supplied documentation for software
- General support system(s) security plan(s)
- Security architecture
- Security standard operating procedures
- Testing procedures and results

- Standard operating procedures
- Emergency procedures
- Contingency plans
- Interface specification for both internal and external interfaces of the system
- Memoranda of understanding with interfacing systems
- Disaster recovery plans
- User rules of behavior
- User manuals
- Risk assessment
- Backup procedures
- Authorized processing documents and statement.

5.4 SECURITY AUDIT LOGGING PROCEDURES

Audit logs for all security events on each IdenTrust's system are generated. Where possible, the data in security audit logs is automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used.

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 IdenTrust's CA operating system and PKI CA applications required by the ACES CP are enabled. IdenTrust meets the applicable requirements for audit records and auditing capabilities for the assurance level of the certificates it issues, as are set forth in the Audit Events Table (Appendix C to this ACES CPS).

IdenTrust's ACES system is able to create, maintain, and protect from modification, unauthorized access, or destruction an audit trail of accesses to the resources it protects in accordance with Federal law, regulations, guidelines, as well as GSA security policy and supporting security guidelines. IdenTrust's ACES system protects audit data from destruction and provides other audit options for use when the standard audit mechanism is unable to record events. Audit records shall be reviewed frequently for signs of unauthorized activity or other security vulnerabilities. Events recorded include those that occur to the routers, firewalls and other network equipment at each host; within applications and databases, and at all physical security check points.

IdenTrust staff members manually record all significant events that are not logged by the equipment.

Access to the audit data and on-line audit logs shall be strictly limited. There shall be separation of duties between security personnel who administer the access control function and those who administer the audit trail. The audit data shall be protected by the system so that read access to it is limited to authorized users. IdenTrust shall ensure that only authorized users and/or programs can enable or disable the audit mechanism and only authorized staff shall be able to retrieve audit trail information and archive it. Unauthorized attempts

to change, circumvent, or otherwise violate security features shall be detectable and reported within a known time by the system.

For each recorded event, the audit trail includes the following information:

- Type of event
- Date and time of the event
- Success or failure of the action
- Terminal identification
- Unique user identification

The system's own journalizing or logging capability should always be used to monitor all communications activity with the host, to determine system/network usage, identify user difficulties and uncover intrusion attempts. The security administrator will review reports to determine if there have been repeated unsuccessful attempts to login to the network. System audit trails and suspected or confirmed computer security violations shall be monitored and appropriate corrective action shall be taken where necessary. Records shall also be maintained of system anomalies, such as software error conditions, software check integrity failures, receipt of improper messages, misrouted messages, and uninterruptible power supply failures.

The duration of storage of audit data is adequate to ensure recognition of security incidents and subsequent analysis of their occurrence, and will be a minimum of 30 days.

Refer to table of auditable events provided in Appendix C: Auditable Events Table.

5.4.2 Frequency of Processing Log

IdenTrust reviews its audit logs at least once a month. Such reviews involve verifying that the log has not been tampered with and briefly inspecting log entries, with a more thorough investigation of any alerts or irregularities in the logs.

A statistically significant set of security audit data generated by IdenTrust 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. All significant events are explained in an audit log summary. Actions taken as a result of these reviews are documented. IdenTrust implements procedures to ensure that the security audit data is 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, are retained and made available during compliance audits. The security audit logs for each auditable event defined in this section are maintained in accordance with Records Archive, Section 5.5. Refer to table of auditable events provided in Appendix C: Auditable Events Table.

Audit logs are retained onsite for at least two months as well as being retained in the manner described in Section 5.5.

Only persons with a then-current designation as an Auditor shall be permitted to remove audit logs from IdenTrust systems.

5.4.4 Protection of Audit Logs

The IdenTrust CA system configuration and procedures are implemented together to ensure that:

- Only authorized people have read access to the logs;
- Only authorized people may archive or delete audit logs; and
- 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).

Only persons with a then-current designation as an Auditor shall be permitted to remove audit logs from IdenTrust systems.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries are backed up at least monthly and a copy of the audit log is sent off-site at least on a monthly basis.

5.4.6 Audit Collection System (Internal vs. External)

Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the GSA shall determine whether to suspend CA operations until the problem is remedied.

Archives are produced by IdenTrust backup operators on a periodic basis (daily, weekly, and monthly) and given to an external courier service for secure delivery to a secure off-site storage facility.

5.4.7 Notification to Event-Causing Subject

Not applicable.

5.4.8 Vulnerability Assessments

IdenTrust performs routine self-assessments of security controls and specifically checks for evidence of malicious activity.

The Security Officers, System Administrators, and other operating personnel monitor attempts to violate the integrity of CA systems, including the equipment, physical location, and personnel. The audit logs are checked for anomalies that may indicate violations, and are reviewed by the Security Office for events including but not limited to repeated failed actions, attempts to acquire privileged access, requests for privileged information, attempted access of system files, and unauthenticated responses. The Security Office also checks for continuity of the security audit data. Reviews of the security audit logs are conducted by the Security Office in accordance with Section 5.5.1.

5.5 RECORDS ARCHIVE

5.5.1 Types of Events Archived

The data and files which must be archived by or on behalf of IdenTrust include ACES certificate application information, certificate issuance and transaction data.

The following minimum data shall be recorded for archive:

- CA accreditation
- Certificate Policy
- Certification Practice Statement
- Contractual obligations and other agreements concerning operations of the CA
- 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 as per Section 3.3.2
- Documentation of receipt and acceptance of certificates
- Subscriber agreements
- Export of private keys
- Documentation of loading, shipping, receipt and zeroizing of tokens
- All ARLs and 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
    - All certificates issued or published
    - All changes to the certificate profile
    - All changes to the revocation profile
    - All changes to the revocation list profile
    - All changes to the trusted public keys
- 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)
- Subscriber private encryption keys that are archived/escrowed in accordance with this ACES CPS.
- 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 the ACES CP
- Violations of this ACES CPS
- All audit logs
- Documentation required by compliance auditors

5.5.2 Retention Period for Archive

IdenTrust follows industry best practices including guidelines provided by the National Archives and Records Administration (NARA). The minimum retention period for archive records is 10 years and 6 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 IdenTrust management group maintains responsibility of all off-site backups of archive data. The archive data is sealed in tamper evident containers and stored off site away from the CA. It is the IdenTrust management group's responsibility to maintain the archives in a secure and protected manner. No other group has access to the archives, and only the IdenTrust management group has the authority to request an archive from the remote site.

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. IdenTrust shall maintain a list of people authorized to modify or delete the archive, and make this list available during CP compliance audits.

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 CA system itself.

5.5.4 Backup Procedures

IdenTrust retains and archives all data through the term of the IdenTrust ACES MOA. IdenTrust archive records must be maintained for 10 years and six months from the date of record origination and shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by IdenTrust.

5.5.5 Requirements for Time-Stamping of Records

Refer to Section 6.8

5.5.6 Archive Collection System

Archive information is collected internally and stored externally as described in Section 5.5.4.

5.5.7 Procedures to Obtain and Verify Archive Information

Upon proper request (see Sections 9.3 and 9.4), IdenTrust will create, package and send copies of archive information. Archived information is provided and verified using the formats and media explained in Section 5.5.3. Access to archive data is restricted to authorized personnel in accordance with Sections 9.3 and 9.4.

Archive data is retrieved from secure storage using defined procedures for accessing archived material. The request procedure requires two IdenTrust Trusted Role employees who are previously authorized for this procedure. One such employee requests the material, and the other provides management approval, using processes established in conjunction with the offsite facility.

Material is delivered to a predefined destination by a bonded carrier employed by the storage facility. Identification of the receiving party is checked, the delivery receipt is signed by the receiving party and physical custody of the archive material is transferred back to IdenTrust. The materials are stored in the secure room until they can be reviewed and/or copied in a forensically sound manner for the requestor. The original archive materials are then returned to the archive storage facility.

5.6 KEY CHANGEOVER

IdenTrust provides for the extension and/or continuation of its self-signed root certificates prior to their expiration through a key rollover process involving signing the new public key with the old private key, and vice versa. 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 CA's signing key will have a validity period as described in Section 6.3.2, Certificate Operational Periods and Key Usage Periods.

IdenTrust ACES CA private keys and subject names are unique. IdenTrust will generate a new key and apply a new subject name when generating new IdenTrust ACES certificates prior to distribution.

IdenTrust will notify all appropriate parties per Section 4.4.3.

After a CA performs a Key Changeover, the CA will 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 will 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

The ACES CP defines a security incident or incident 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. For the purposes of this ACES CPS, IdenTrust covers this statement and also defines procedures in line with the IdenTrust Security Incident Response Guide (SIRG).

5.7.1 Incident and Compromise Handling Procedures

An incident may include, but is not limited to the following conditions and IdenTrust will notify the ACES PMO should any of these conditions occur:

- Suspected or detected compromise of the Authorized ACES CA systems

- Suspected or detected ACES CA private key compromise
- 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 IdenTrust's systems
- Successful denial of service attacks on IdenTrust's CA components
- Any incident preventing IdenTrust 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. In addition, IdenTrust will provide information requested by the ACES PMO, relative to any other issue that the ACES PMO identifies as calling into question the integrity or trustworthiness of the IdenTrust CA.

In the event of a CA or certificate compromise or fraudulent mis-issuance, IdenTrust will 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.

In response, 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 IdenTrust prior to taking action. IdenTrust 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.

IdenTrust will notify the ACES PMO of any questionable certificate activity.

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

IdenTrust retains back-up storage media to facilitate restoration to full operation. If CA equipment is damaged or rendered inoperative, but IdenTrust's CA signature keys are not destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

- Before returning to operation, ensure that the system's integrity has been restored.
- If IdenTrust's 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 IdenTrust's 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.

IdenTrust will re-establish operational capabilities in accordance with GSA policies and guidelines and procedures as set forth in this ACES CPS.

5.7.3 Authorized ACES CA Private Key Compromise Procedures

IdenTrust has developed a key compromise plan to address the procedures that will be followed in the event of

a compromise of the private signing key used by IdenTrust to issue ACES Certificates. The plan includes procedures for (and documentation of) revoking all affected ACES Certificates it has issued, and promptly notifying all Subscribers and all Relying Parties.

If IdenTrust signature keys are compromised or lost (such that compromise is possible even though not certain), IdenTrust shall:

- Notify the GSA and Federal PKI Policy Authority of the compromise and revoke any cross certificates that exist;
- Revoke all ACES certificates it has issued;
- Generate a new IdenTrust key pair in at least a FIPS 140-1 Level 3 cryptographic hardware in accordance with Sections 6.1 and 6.2;
- Issue new CA certificates to subordinate CAs in accordance with the applicable ACES CPS.

If the private key in IdenTrust's self-signed CA Root Certificate is compromised, IdenTrust will:

- Generate a new signing key pair and corresponding CA Certificate;
- Initiate procedures to notify subscribers of the compromise; and
- Securely distribute the new CA Certificate.
- Optionally, IdenTrust may renew current certificates under the new signing key. (see Section 3.2.1)

If the IdenTrust's CA private key appears as the subject public key in certificates issued by other CAs, IdenTrust will notify the issuer(s) of these certificates within 24 hours.

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

In the event that IdenTrust's Public Key is revoked due to compromise, IdenTrust shall reestablish revocation capabilities as quickly as possible by revoking subordinate certificates and signing a CRL with the private key that has been compromised. IdenTrust will then set up a new CA hierarchy and reissue certificates. Revocation information will continue to be available through CRLs/ARLs within the Repository and IdenTrust's Standard OCSP responder obtained though the AIA extension of Subscriber certificates. Any affected cross-certificate would have to be revoked by the CA issuing the cross-certificate.

5.7.4 Business Continuity Capabilities after a Disaster

IdenTrust has a disaster recovery/business resumption plan in place that allows IdenTrust to reconstitute the CA within 72 hours of catastrophic failure, which IdenTrust has made available to the GSA. IdenTrust's business continuity and disaster recovery plans allow for other non-essential systems to be brought into operation later than 72 hours. If for any reason IdenTrust cannot issue a CRL within 72 hours after the time specified in the next update field of its currently valid CRL, it will notify GSA and any applicable Agency policy authorities where appropriate.

If for any reason the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, IdenTrust will notify GSA and any applicable policy authorities. Relying parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operation with new certificates.

5.7.5 Customer Service Center

IdenTrust implements and maintains an ACES Customer Service Center to provide assistance and services to Subscribers and Relying Parties, and a system for receiving, recording, responding to and reporting ACES problems within its own organization.. IdenTrust 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

In the event that IdenTrust ceases operation or its participation as an Authorized CA in ACES or is otherwise terminated:

a) all Subscribers, sponsoring organizations, and Relying Parties must be promptly notified of the cessation;

b) all ACES Certificates issued by IdenTrust shall be revoked no later than the time of cessation;

In the event that the IdenTrust ACES CA ceases to issue new ACES certificates, IdenTrust will either continue to issue CRLs until all ACES certificates issued by IdenTrust have expired, or IdenTrust will 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. In addition, IdenTrust will continue to conform to all relevant aspects of the ACES CP and this ACES CPS (e.g., audit logging and archives).

In the event that IdenTrust terminates operation, the GSA shall ensure that any certificates issued to IdenTrust have been revoked.

The services under IdenTrust's ACES MOA and ACES CP are vital to the Government and must be continued without interruption. Upon the ACES PMO written notice, IdenTrust will engage in good faith negotiations with the ACES PMO to establish a plan relating to phase-out of the operations of IdenTrust in the event of a termination of the ACES MOA. In the event of a termination of the ACES MOA, IdenTrust shall provide phase-in coordination (i.e., coordinating the orderly transition to Government-provided services such that the level and quality of transitioning services are not degraded, to the extent possible) and exercise its best efforts and cooperate to effect an orderly and efficient transition to a successor.

In the event of ACES PMO providing written notice of the IdenTrust ACES MOA expiration, IdenTrust shall continue performance under the then-existing terms and conditions (including price) of the IdenTrust ACES MOA for a period of up to 48 hours. Should the ACES PMO, having provided such notice of expiration, but not having elected initially to extend the IdenTrust's ACES MOA, provide written notice within such 48 hours of a desire to extend IdenTrust's ACES MOA, IdenTrust, shall continue to perform under the IdenTrust ACES MOA for up to 72 hours so that IdenTrust and the ACES PMO might, if mutually agreeable, execute a new memoranda of agreement to replace the IdenTrust ACES MOA.

SECTION 6: TECHNICAL SECURITY CONTROLS

IdenTrust, and all Authorized RAs, CMAs, and Repositories, shall implement appropriate technical security controls in accordance with GSA security policy and supporting security guidelines. When a FIPS 140-2 validated HSM or Cryptomodule is used, the module will be used in FIPS approved mode.

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 by IdenTrust to sign certificates, CRLs or status information shall be generated in a FIPS-140 Security Level 2 validated cryptographic module or modules validated under equivalent international standards. IdenTrust cryptographic modules meet or exceed FIPS 140-1 Level 3.

The CA Key generation ceremonies are performed in the Secure Room. The ceremony is scripted, video-recorded and witnessed. The ceremony is performed by personnel in Trusted Roles who use different security Keys at the appropriate time depending on whether Key generation, Certificate generation or a Cryptomodule backup/cloning operation is being performed. The scripts and video recording are made available to independent third party auditors during the annual audit for examination.

CA key pair generation occurs only under multiparty control and verifiable audit trail is created during key generation to establish that security requirements for procedures were followed. The key generation record documents any failures or anomalies in the key generation process, and any corrective actions taken. The documentation also demonstrates that appropriate role separation was used during key generation.

6.1.1.2 Subscriber Key Pair Generation

Key pairs for all Program Participants must be generated in such a way that the private signature key is not known by other than the authorized user of the key pair, except under circumstances addressed in Section 6.1.2. RA, and CMA keys must be generated in hardware tokens.

Cryptographic modules must meet or exceed FIPS 140-1 or FIPS 140-2, Security Level 2 overall, and cryptographic modules must adhere, as a minimum, to the following requirements referencing FIPS PUB 140-1 or 140-2: (a) Level 3 - 4 (identity-based operator authentication) for 'Roles and Services'.

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

In those cases where public/private key pairs are generated by IdenTrust on behalf of the Subscriber, IdenTrust shall implement procedures to ensure that the token is not activated by an unauthorized entity. (Subscriber private signature keys will not be generated by IdenTrust.)

Delivery of the Subscriber encryption private key (or, if the Subscriber generates the encryption key pair, delivery by the Subscriber to the Agency) shall be in accordance with the requirements of the ACES CP and this ACES CPS.

Key pairs for Subscribers can be generated in either hardware or software. For subscribers, software or hardware shall be used to generate pseudo-random numbers, key pairs, and symmetric keys. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved method.

6.1.2 Private Key Delivery to Subscriber

IdenTrust does not generate private signature keys for Subscribers. Delivery of private encryption keys is performed in accordance with Section 6.2.3 of this ACES CPS.

6.1.3 Public Key Delivery to Issuer (IdenTrust)

As part of the ACES Certificate application process, the Subscriber's public key must be transferred to the Authorized RA or IdenTrust in a way that ensures that:

1) it has not been changed during transit;

2) the sender possesses the private key that corresponds to the transferred public key; and

3) the sender of the public key is the legitimate user claimed in the certificate application.

Once IdenTrust, or an Authorized RA or Trusted Agent, has confirmed the identity of the Subscriber in accordance with Section 3.1 and approved certificate issuance, IdenTrust or the Authorized RA or Trusted Agent sends the Subscriber an activation code. The activation code is used in conjunction with a secure SSL session between IdenTrust and the Subscriber during which the public/private key pair and the certificate are generated. This process ensures that the public key is sufficiently bound to the subscriber's identity. Proof of possession of the private key is demonstrated through the certificate request and downloading process, which will not work if the subscriber does not have a functioning public/private key pair. (see Section 3.2.1)

6.1.4 Authorized ACES CA Public Key Delivery to Relying Parties

IdenTrust ensures that Subscribers and Relying Parties receive and maintain the ACES Sub CA Public Keys in a trustworthy fashion. Public Keys for CAs are contained within CA Certificates. Methods for delivery of CA Certificates include:

1) CA Certificates may be delivered to Subscribers during the Certificate retrieval process for their own Subscriber Certificates during the Server-Authenticated SSL/TLS-Encrypted Session as part of a message formatted in accordance with PKCS#7.
2) Relying Parties may obtain CA Certificates from IdenTrust's secure web site. An e-mail or other communication may be sent to PKI Participants directing them to download the CA Certificate at an https:// website secured with a valid SSL Certificate that chains to one of IdenTrust's Root Certificates. Alternatively, Subscribers and Relying Parties may be directed to an http:// website that is not secured in which case, IdenTrust will provide the hash or fingerprint via authenticated out of band (OOB) sources (i.e., IdenTrust help desk phone support).

PKI Participants relying on CA Public Keys may deploy CA Certificates through enterprise-wide patch management, system maintenance utilities, Repository services, active directories and through SIA and AIA path discovery.

6.1.5 Key Sizes

Key sizes and algorithms shall be specified in the ACES CP and applicable certificate profile. All FIPS-approved signature algorithms shall be considered acceptable. Additional restrictions on key sizes are detailed below:

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this ACES CPS requires at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys.

IdenTrust generates certificates and CRLs that are covered under this policy by using 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 after 12/31/2030 shall be at least 3072 bits for RSA, or at least 156 bits for ECDSA.

IdenTrust generates certificates and CRLs under the ACES CP and uses SHA-256, or SHA-384 hash algorithm when generating digital signatures. RSA signatures on certificates and CRLs are 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.

As an issuer of certificates under this CP, IdenTrust ensures that end-entity certificates contain public keys that are at least 2048 bit for RSA, DSA, or Diffie-Hellman, or 244 bits for elliptic curve algorithms.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of the ACES CP shall require AES for the symmetric key, and at least 2048 bit RSA or 224 bit elliptic curve keys.

IdenTrust distributes the ACES / Federal Common Policy CA root chain when ACES certificates are retrieved and installed. Notwithstanding any other provision set forth above in this Section 6.1.5 relating to key sizes, key sizes of the certificates in the ACES / Federal Common Policy CA root chain not subject to such provisions.

6.1.6 Public Key Parameters Generation Quality Checking

The public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS186-2. IdenTrust currently supports RSA keys using PKCS-1 v.2, but has capabilities to support:

a) DSA, in accordance with FIPS PUB 186-2, Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), December 1998.

b) ECDSA, in accordance with ANSI X9.62, American National Standard for Financial Services – Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm (ECDSA), draft, ASC X9 Secretariat - American Bankers Association, 1997; and

c) Alternate Government-approved key generation algorithms;

where contractually obligated.

IdenTrust checks Parameter Quality during the Client key submission processes in accordance with FIPS 186-2 or a more stringent test if specified by the GSA.

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

IdenTrust's CA system records whenever IdenTrust generates a key and all changes to the trusted public keys, including additions and deletions.

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.

IdenTrust does not use Private Keys corresponding to Root Certificates to sign certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g., administrative role certificates, internal CA operational device certificates; and
4. Certificates for OCSP Response verification

CA Certificates

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

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.

IdenTrust may opt to add additional extensions for SSL Certificates. When this adoption occurs, the changes will be reflected in the profiles. Additionally, any verification practice will be included in this ACES CPS.

IdenTrust ACES CAs set the key usage bits in all IdenTrust ACES Infrastructure Certificates in accordance the FPKI certificate profile document (Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile available at https://www.idmanagement.gov) and Section 7 of the ACES CP.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

IdenTrust's CAs, Authorized RAs, and CMAs shall each protect their private key(s) in accordance with the provisions of IdenTrust's ACES MOA, the ACES CP and Section 6.1 of this ACES CPS.

6.2.1 Cryptographic Module Standards and Controls

The cryptographic module must meet or exceed FIPS 140-1 or FIPS 140-2, Security Level 2 overall. IdenTrust uses FIPS PUB 140-1 or 140-2, validated cryptographic modules that adhere, as a minimum, to the following requirements referencing FIPS PUB 140-1 or 140-2:

a) Level 3 - 4 (identity-based operator authentication) for "Roles and Services" and

b) Level 3 (tamper protection and response envelope for covers and doors) for 'Physical Security' for CA private key storage in hardware.

Upon request and in accordance with applicable pricing arrangements, IdenTrust will provide at least Level 2 FIPS PUB 140-1 or 140-2 validated cryptographic modules for key pair generation and storage of private keys to application servers.

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [latest version of FIPS 140 series]. Cryptographic modules shall be validated to the latest version of the FIPS 140 series level; or validated, certified, or verified to requirements published by the GSA, as follows (or better):

- Level 2 Hardware for RAs
- Level 1 Hardware or Software for Subscribers

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 IdenTrust CA private signing key. The IdenTrust CA signature keys may be backed up only under two-person control. Access to IdenTrust 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 are 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

Not applicable.

6.2.3.3 Escrow of Subscriber Private Signature Keys

Subscriber private signatures keys shall not be escrowed.

Subscriber private signature keys may be backed up or copied, but must be held in the Subscriber's control.

6.2.3.4 Escrow of Subscriber Private Encryption Keys

Private encryption keys are escrowed to enable key recovery in accordance with Section 4.12.1. (Private signature keys are never escrowed or archived.) As part of the certificate issuance/key escrow process, Subscribers are notified that the private keys associated with their encryption certificates will be escrowed. During the key generation event, the private key is stored in an encrypted file (a PKCS#12), and the information needed to decrypt the encrypted private key consists of a system-generated code (a strong passphrase) that is itself encrypted. The key escrow and passphrase files are stored in the Key Escrow Database, or "KED," as a collection of encrypted keys and encrypted passwords protected by a passphrase. The KED is housed and operates in IdenTrust's facilities, computer systems and networks as described in Sections 6.5, 6.6 and 6.7 of this ACES CPS.

6.2.4 Private Key Backup

6.2.4.1 Backup of Authorized ACES CA Private Signature Keys

Hardware tokens containing CA private signature keys may be backed-up in accordance with security audit requirements defined in Section 6.2.4.1.

IdenTrust's CA private signature keys are backed up and stored under the same security precautions and multi-person control as the original signature key. No other party is allowed to backup and archive the private signature keys of the CA Certificate or subordinate CA Certificate. All access to certificate subject private keys retained within IdenTrust for key recovery purposes (see Section 6.2.3) must be documented.

6.2.4.2 Backup of Subscriber Private Signature Key

Private keys of signing certificates delivered to hardware cryptomodules are not backed up. Private keys installed on hardware tokens are not exportable, and cannot be backed up. For more information on hardware tokens see Section 3.2.1.1.

Private keys of certificates delivered to software cryptomodules may be backed up or copied as long as they remain under the control of the Subscriber, the private signature keys never appear outside the cryptomodule in plain text and the cryptomodule in which they are stored is evaluated to FIPS PUB 140-2 Level 1 or higher. Subscribers are obligated to protect backed up or copied Private Keys.

6.2.4.3 Backup of Subscriber Key Management Private Keys

Medium assurance Subscribers may make backup copies (encrypted, protected by password) of their own confidentiality (but not Signature) private keys. Subscribers are permitted to make operational copies of private keys residing in software Cryptographic Modules for each of the Subscriber's applications or locations that require the key in a different location or format. Subscribers are notified of their obligation to make the backup copies on cryptographic modules validated at FIPS 140 level 1 that are kept under their control. PKI Sponsors are authorized to make a single backup copy of the component private keys to support backup in cases where component malfunction results in key corruption.

All key transfers will be done from an approved cryptographic module, and the key must be encrypted during the transfer. The Subscriber and the PKI Sponsor are responsible for ensuring that all copies of private keys are protected, including protecting any workstation on which any of its private keys reside.

Under two-person control, IdenTrust backs up its CA private key and CSA private key on separate cryptographic modules in order to obviate the need to Re-key in the case of cryptographic module failure. The backup modules are FIPS 140-2 Level 3 validated and are securely stored under dual-controlled lock and key at all times. IdenTrust stores all IdenTrust CA and CSA production private keys and corresponding backup copies in a secure and trustworthy environment. The second backup copies, for CA and CSA, are held in the offsite facility under the controls explained in Sections 5.1.6 and 5.1.8. When the CA and CSA keys are no longer needed and after three-years of the last Re-key, the cryptographic module containing them will be zeroized and/or destroyed.

6.2.4.4 Backup of CSS Private Key

CSS Private Signature Keys are backed up and stored under the same security precautions and multi-person control as the original CSS Signature Private Key on cloned HSMs to obviate the need to Re-Key in the case of hardware failure or disaster. No entity other than IdenTrust is allowed to backup or archive CSS Private Signature Keys. Two copies of all CSSs are created in a shared HSM. All backup Cryptomodules are evaluated to FIPS PUB 140-2 Level 3 or higher.

The backup of all other CSS Keys is performed during a ceremony that is scripted, videotaped and witnessed under the same controls used for the original Key Generation. The backup is performed using the PED keys specified for such purpose. PED keys are kept under Separation-of-Duties/Multi-party Control as explained in Section 5.1.2.1.

IdenTrust stores CSS Private Keys and one of the backup copies in the secure room. The second backup of CSS Private Keys is kept in a secure offsite facility.

When the CSA Keys are no longer needed, the HSM containing them is zeroized in accordance with Section 6.2.10.

6.2.5 Private Key Archival

The Private Keys of Signing Certificates that are issued to Subscribers are not archived or escrowed by IdenTrust.

Parties other than the Subordinate CA are not allowed to archive the Subordinate CA Private Keys without authorization by the Subordinate CA.

6.2.6 Private Key Transfer into or from a Cryptographic Module

IdenTrust 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 does IdenTrust's private key exist in plaintext outside the cryptographic module.

All other keys are 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 is 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 are protected from disclosure.

6.2.7 Private Key Storage on a Cryptographic Module

IdenTrust's CA private keys are generated and remain in FIPS 140-2 level 3 Modules, which do not allow exportation to other unsecured media. The CA private keys may be backed up in accordance with Section 6.2.2.

If IdenTrust generates the Private Key on behalf of a Subordinate CA, then IdenTrust will encrypt the Private Key for transport to the Subordinate CA. If IdenTrust becomes aware that a Subordinate CA's Private Key has been communicated to any unintended person or an organization not affiliated with the Subordinate CA, then IdenTrust will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.8 Method of Activating Private Keys

IdenTrust's signing key activation requires multi-person control as specified in Section 5.2.2, Number of Persons Required per Task.

IdenTrust utilizes industry best practices when enabling any of the private keys used within the IdenTrust CA, RA or CMA systems and encourages these same practices with Subscribers when managing and activating their private keys. Some practices include requiring authentication to the cryptographic module before the activation of any private key(s) using passphrases, PINs, or biometrics. Entry of activation data should be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Method of Deactivating Private Keys

IdenTrust's cryptographic modules storing CA private signing keys that have been activated are not left unattended or otherwise available to unauthorized access. After use, the cryptographic modules are

deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity. Hardware cryptographic or modules are removed and stored in a secure container when not in use.

6.2.10 Method of Destroying Subscriber Private Signature Keys

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 is not required.

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

Public keys are archived as part of the certificate archival.

6.3.2 Certificate Operational Periods and Key Usage Periods

IdenTrust distributes the ACES / Federal Common Policy CA root chain when ACES certificates are retrieved and installed; therefore key usage periods are not assigned by IdenTrust.

IdenTrust will 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 will 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 IdenTrust 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 IdenTrust'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 IdenTrust. 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 CA.

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

Under no circumstances shall IdenTrust 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

A pass-phrase, PIN or other Activation Data is used to protect access to Private Keys.

IdenTrust uses manually-held PED and PED keys to activate its Private Keys for CAs, CSAs, RAs and CMSs. The Activation Data used meets the requirements of FIPS PUB 140-2 Level 3. The PED and PED keys are held in the secure room under the multi-person controls explained in Section 5.1.2.1.

Participant CAs and External RAs may use a remote PED and PED keys for administration of RA and CMS system HSMs, provided controls surrounding use of such remote PED devices are described in their RPS and acceptable to IdenTrust.

All Subscribers are instructed to use strong passwords in accordance with FIPS PUB 140-2 Level 2 and to protect their passwords. When Activation Data is transmitted, it is sent through a secure OOB channel as explained in Sections 4.3.1 of this ACES CPS.

Subscribers of Certificates delivered to software Cryptomodules are instructed to use Strong Passwords.

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

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

6.4.3 Other Aspects of Activation Data

Not applicable.

6.5 COMPUTER SECURITY CONTROLS

IdenTrust operates a variety of commercial software and hardware systems to provide CA, RA, and repository services in accordance with Federal laws, regulations, and guidelines. IdenTrust operates these software systems on Sun Solaris, UNIX, and Windows 2000+ platforms. These systems are regularly scanned for potential security compromises and software is run locally to prevent such compromises. Machines running on the Windows 2000+ platform are for client interface purposes only.

6.5.1 Specific Computer Security Technical Requirements

IdenTrust supports the following computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the CA systems 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

IdenTrust operates systems that have received security evaluations from Common Criteria, FIPS NIAP or other comparable information-assurance evaluation programs. Such IdenTrust systems are deployed in accordance with the configuration guidelines established by such information-assurance evaluation(s). All CA and RA Systems are configured with user and system accounts assigned on a limited basis, by applying "needs only" criteria and subject to CIO approval, and have all unused network services and network ports and protocols disabled.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The entire system development life cycle for IdenTrust's ACES system is controlled to ensure its integrity at all levels, including the use of best commercial practices. IdenTrust uses software that has been designed and developed under a formal, documented development methodology.

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 IdenTrust can 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, IdenTrust can demonstrate that security requirements were achieved through software verification and validation and structured development/life-cycle management.
- Hardware and software procured to operate IdenTrust CA is 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).
- IdenTrust ensures that hardware and software is 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 IdenTrust's CA operation supports multiple CAs, the hardware platform may support multiple CAs.

- IdenTrust has implemented safeguards to ensure proper care is taken to prevent malicious software from being loaded onto the IdenTrust CA equipment. All applications required to perform the operation of IdenTrust's CA is 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 security features on IdenTrust's ACES systems are configured and enabled. The configuration of IdenTrust's ACES system (including hardware, software, and operating system) as well as any modifications and upgrades are documented and controlled. Mechanisms exist on IdenTrust's ACES system for detecting unauthorized modification to the ACES software or configuration.

IdenTrust conducts design reviews and system tests prior to placing its systems into operation to assure that they meet security specifications. In addition, if new controls are added to the application or the support system, additional acceptance tests of those new controls must be performed to ensure that the new controls meet security specifications and do not conflict with or invalidate existing controls. The results of the design reviews and system tests shall be fully documented, updated, as new reviews or tests are performed, and maintained in the official organization records.

IdenTrust follows a formal configuration management methodology in the installation and ongoing maintenance of its ACES system. IdenTrust's CA software, when first loaded, is verified as being that supplied from the vendor, with no modifications, and the version intended for use.

IdenTrust's CA equipment is dedicated to administering a key management infrastructure. It does not have installed applications or component software, which are not part of the CA configuration. Equipment (hardware and software) procured to operate IdenTrust's ACES system is purchased in a fashion to reduce the likelihood that any particular component was tampered with. IdenTrust's CA Equipment is developed in a controlled environment, which is defined and documented.

IdenTrust ensures that all hardware and software is shipped or delivered via controlled methods that provide a continuous chain of accountability, from the location where it has been identified as supporting a CMA function to the using facility.

For IdenTrust and governmental agencies responsible for local registration, reasonable care shall be taken to prevent malicious software from being loaded on RA equipment. Only applications required to perform the organization's mission shall be loaded on the RA computer, and all such software shall be obtained from sources authorized by local policy. Data on RA equipment shall be scanned for malicious code on first use and periodically afterward.

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.

6.6.3 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 law, regulations, and guidelines. The SSP specifies 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. IdenTrust's ACES system ensures 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

Not applicable.

6.7 NETWORK SECURITY CONTROLS

Firewalls are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. All unused network ports and services will be turned off. Any network software present on IdenTrust equipment will be necessary to the functioning of the CA, CSA and RA

6.7.1 Interconnections

Where IdenTrust 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.

Connectivity with Internet and Other WANs

IdenTrust will request written authorization from GSA prior to connecting with other systems and 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 (do not repeat the system rules)
- 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

The SSP provides 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.

6.7.2 Inventory

IdenTrust maintains a comprehensive inventory of its ACES 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.

Hardware/Software Maintenance Controls

Areas of control shall include system software controls in accordance with Federal laws, regulations, and guidelines and GSA security policy and supporting security guidelines.

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

6.8 TIME STAMPINGS

IdenTrust's ACES date/time stamps conform to the ITU-T Recommendation X.690 and the X.690 v2, Information Technology – ASN.1 Encoding Rules, 1994.

IdenTrust's system clock time is derived from multiple trusted third party time sources in accordance with applicable requirements and is used to establish timestamps for the following:

- Initial Validity time of a Certificate;
- Revocation of a Certificate;
- Posting of CRLs and CRL updates;
- OCSP Responses; and
- System audit journal entries.

System time for servers providing CA, OCSP and CMS services is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every 60 minutes. External time sources operated by government agencies and other trusted sources are used to maintain an average accuracy of one second or better.

SECTION 7: CERTIFICATE, CARL /CRL, AND OCSP PROFILES FORMAT

7.1 CERTIFICATE PROFILE

ACES Certificates shall contain public keys used for authenticating the sender and receiver of an electronic message, encrypting messages, and verifying the integrity of such messages, i.e., public keys used for digital signature verification. IdenTrust ACES certificate profiles are documented in the FPKI X.509 certificate and crl extension profile. *Federal PKI X.509 Certificate and CRL Extensions Profile* (FPKI-Prof).

For all Certificates, IdenTrust generates a non-sequential serial number that exhibits at least 64 bits of entropy. IdenTrust does not use DSA algorithms.

IdenTrust creates and maintains ACES Certificates that conform to RFC 5280 and ITU-T Recommendation X.509, The Directory: Authentication Framework, June 1997. IdenTrust ACES certificates all include appropriate ACES OIDs in the Certificate Policies extension and contain the required certificate fields as specified in accordance with the ACES CP, this ACES CPS and IdenTrust's ACES Profiles, available through the Contact Person listed in Section 1.5.2.2.

Certificates issued by IdenTrust comply with the *Federal PKI X.509 Certificate and CRL Extensions Profile* (FPKI-Prof).

7.1.1 Version Numbers

IdenTrust issues X.509 v3 certificates (the certificate version field is populated with integer 2).

7.1.2 Certificate Extensions

CA certificates issued by IdenTrust do not include critical private extensions.

All private extensions may be used in subscriber certificates, will be identified in this ACES CPS.

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

After August 22, 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 64 bits of entropy in the serial number.

7.1.3 Algorithm Object Identifiers

Certificates issued under the ACES CP and this ACES CPS use the following OIDs for signatures:

Ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1 }
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-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 }

Certificates under the ACES CP and this ACES CPS use the following OIDs for identifying the algorithm for which the subject key was generated:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
Id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

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 }

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 above, 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.

7.1.4.1 Subject

The content of the Certificate Issuer Distinguished Name field MUST match the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

Human Subscribers- Individual Unaffiliated:

Subscriber's Distinguished Name, which may contain a unique identifier to ensure name uniqueness:

cn = <subject name> (firstname MI lastname)

o = <Certificate Type>

c = <country of Subscriber>

Human Subscribers- Business Affiliated:

Subscriber's Distinguished Name, which may contain a unique identifier to ensure name uniqueness:

cn = <subject name> (firstname MI lastname)

ou = < Sponsoring Organization name>

o = <Certificate Type>

c = <country of Subscriber>

SSL Certificates:

Subscriber's Distinguished Name, which may contain a unique identifier to ensure name uniqueness:

C n = <subject Domain name>

ou = < Sponsoring Organization name>

o = <Sponsoring Organization name >

LocalityName = <verified city of the Sponsoring Organization>

StateOrProvinceName = <verified state>

c = <country of Sponsoring Organization>

7.1.4.3 Name Forms

Where required as set forth above, 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.

For ACES SSL Certificates the following attributes will be included:

- The subject:CommonName will be alphanumeric text and include the public IP address or Fully Qualified Domain Name of the component or device being certified. If the component is a web Server, the URI is always listed in subjectAltName. For OCSP the uniform resource identifier for the OCSP responder.
- The subject:serialNumber will be a hexadecimal string of characters for a universally unique identifier that will create a non-sequential number that exhibits at least 64 bits of entropy.
- The subject:AltName: required for the Device Certificate. This can be:
  - rfc822name and the extension for an e-mail;
  - the dNSName containing the FQDN;
  - No IP Address entries are included.
- Multiple FQDNs (up to 50) can be supported in the SAN.
- The subject:localityName, stateorProvinceName will be included when the organization name (O) is included.
- The CA/B Forum OID may or may not be included at IdenTrust's discretion; however, when asserted the certificate must meet all requirements for the CA/B Forum.

7.1.5 Name Constraints

IdenTrust does not utilize name constraints except in the instance of Cross-Certificates as necessary to permit or exclude trust sub-trees.

When issuing a Subordinate CA Certificate, IdenTrust conducts a scripted ceremony which encompasses all procedures set forth in the ACES CP and this CPS. The script is compiled by using the Subordinate CA Certificate profile to define all attributes, including Subject Information, to be included in the Subordinate CA Certificate. Verification of Subject Information for accuracy is completed prior to the Subordinate CA certificate issuance.

7.1.6 Certificate Policy Object Identifiers

Certificates issued under the ACES CP and this ACES CPS shall assert the OID appropriate to the type of certificate and level of assurance with which it was issued. See Section 1.2.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

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 version two (2) and RFC 5280.

7.2.1 Version Numbers

IdenTrust issues X.509 Version two (2) CRLs.

7.2.2 CRL Entry Extensions

Processing semantics for the critical certificate policy extension used by IdenTrust shall conform to [FPKI-Prof].

7.3 OCSP PROFILE

Certificate status servers (CSSs) operated under the ACES CP shall sign responses using algorithms designated for CRL signing as defined in Section 6.1.5 Key Sizes.

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 RFC 6960.

SECTION 8: COMPLIANCE AUDITS AND OTHER ASSESSMENTS

IdenTrust is subject to inspections and reviews in accordance with Federal regulations and security guidelines as defined in the ACES CP and this ACES CPS. IdenTrust's system security test and evaluation plan describes how the security features and controls of its systems are to be tested and reviewed when significant modifications are made. IdenTrust is audited annually with no gap between audit periods pursuant to the American Institute of Certified Public Accountants' (AICPA's) / Canadian Institute of Chartered Accountants' (CICA's) Web Trust Program for Certification Authorities. (CA Web Trust).

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

IdenTrust has demonstrated compliance with the ACES CP, this ACES CPS, and its MOA. The GSA and other authorized Federal entities may perform periodic and aperiodic compliance audits or inspections of IdenTrust, 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 CPSs, Registration Practices Statements (RPSs), SSPs and PPPs.

IdenTrust Operations related to its own CA, CSA and RA are audited annually against the criteria of WebTrust Program for Certification Authorities. (WebTrust for CA), developed by the American Institute for Certified Public Accounts and CPA Canada (formerly the Canadian Institute of Chartered Accountants). These audits provide an unbroken sequence of audit periods that shall not exceed one year in duration.

Certificates that are capable of being used to issue new certificates are either (a) technically constrained in line with Section 7.1.5 and audited in line with Section 8 only in regards to self-audits, or (b) unconstrained and fully audited in line with all remaining requirements from the CA/B Forum Baseline Requirements. A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509 v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

IdenTrust's compliance auditors demonstrate competence in the field of compliance audits, and are thoroughly familiar with the requirements that IdenTrust imposes on the issuance and management of its certificates. The auditor performs such compliance audits as its primary responsibility.

To perform the compliance audit, IdenTrust engages the services of a professional auditing firm having the following qualifications:

(1) **Focus and experience**. Auditing must be one of the firm's principal business activities. Moreover, the firm must have experience in auditing secure information systems and Public Key Infrastructures (PKI).

(2) **Expertise**: The firm must have a staff of auditors trained and skilled in the auditing of secure information systems. The staff must be familiar with PKI, certification systems, and the like, as well as internet security issues (such as management of a security perimeter), operations of secure Datacenters, personnel controls, and operational risk management. The staff must be large enough to have the necessary depth and range of expertise required to audit IdenTrust's operations, or the Sponsoring Organizations with Enterprise RAs registration functions, in a competent manner.

(3) **Reputation**: The firm must have a reputation for conducting its auditing business competently and correctly.

(4) **Disinterest**: The firm has no financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against IdenTrust (or the RA being audited). In the case of a Sponsoring Organizations with Enterprise RAs internal auditing group, the auditing group must be independent of the group being audited.

(5) **Rules and standards**: The firm must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body, and must require its audit professionals to do the same.

Moreover, in auditing secure information systems, the independent firm should be guided by generally accepted standards for evaluating secure information systems such as ISO 27001, Annex B of ANSI X9.79, the Common Criteria, or ISO 21188. The engagement of the auditing firm takes the form of a contract obligating the firm to assign members of its professional auditing staff to perform the audit when required. The contracted independent firm must also carry an omissions insurance with policy limits of at least one million US dollars in coverage. While the audit is being performed, those staff must, by agreement, perform the audit as their primary responsibility.
In addition, the members of the firm's staff performing the audit are contractually subject to the following requirements:

(1) **Professional qualifications**: Each external auditing professional performing the audit must be a member of the AICPA, CICA, ICAEW, ISSA, (ISC)2, IIA, or ISACA. In addition, at least one staff member must be qualified as a Certified Information Systems Auditor, AICPA Certified Information Technology Professional (CPA.CITP), or have another recognized information security auditing credential.

(2) **Primary responsibility**: The external auditing professional assigned by the auditing firm to take the lead in the audit must have the audit as his or her primary responsibility until the audit is completed. That staff member and IdenTrust will agree on a project plan before beginning the audit to ensure that adequate staff, other resources, and time are provided.

(3) **Conformity to professional rules**: Each external professional active in auditing IdenTrust must conform to the ethical and other professional rules of the AICPA, CICA, ICAEW, ISSA, (ISC)2, IIA, or ISACA or those of the applicable other qualified auditing standards body.

(4) **Professional background**: The external professionals assigned to perform the audit must be trained to a standard generally accepted in the auditing field. They should also be familiar with PKI and other information security technologies and their secure operation. IdenTrust's operations are audited to ensure that IdenTrust conforms to its ACES CP and CPS and familiarity with those documents is necessary for performing the audit for either IdenTrust or for an RA. The auditor that IdenTrust has selected for past audits has in every case been one of the large, well-known auditing firms. IdenTrust expects to continue this practice while changing from time to time the specific firm selected, and expects that its RAs will do the same.

8.3 AUDITOR'S RELATIONSHIP TO ASSESSED ENTITY

IdenTrust's Internal Auditors

With respect to each internal Audit at IdenTrust called for under this ACES CPS, IdenTrust will select a Security Officer or other Individual authorized by IdenTrust to perform such audit; provided, however the Individual who is such auditor be neither (a) an Individual responsible for daily operation of IdenTrust's PKI environment or involved in RA functions during the audit nor (b) an Individual who was responsible for daily operation of IdenTrust's PKI environment or involved in RA functions during the period being audited.

IdenTrust's External Auditors

With respect to each audit called for under this ACES CPS which requires use of an external auditor, IdenTrust shall have a contractual relationship with the auditing firm performing such audit, but save for the relationship formed via such contract: (i) IdenTrust and the audit firm shall be entities that are independent of, unrelated to, and with no financial interest each other; and (ii) the Individuals performing the audit for the audit firm shall have no other relationships with IdenTrust or its officers and directors, including financial, legal, social, or other relationships, where such relationships would constitute a conflict of interest.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a quality assurance inspection and review of IdenTrust is to verify that it is operating in compliance with the requirements of the ACES CP, its MOA, and this ACES CPS. Quality assurance inspections **of IdenTrust are conducted pursuant to the AICPA/CICA's Web Trust Program for Certification A**uthorities (CA Web Trust) and in accordance with the ACES CP retains a WebTrust licensed auditor to perform the audit.

The purpose of a quality assurance inspection and review of IdenTrust is to verify that it is operating in compliance with the requirements of the ACES CP, its MOA, and this ACES CPS. Quality assurance inspections of IdenTrust are conducted pursuant to the AICPA/CICA's Web Trust Program for Certification Authorities (CA Web Trust) and in accordance with the ACES CP retains a WebTrust licensed auditor to perform the audit.

The scope of the annual audit must include all CAs that validate or with a path to IdenTrust. The audit must document the full PKI hierarchy and contain audit information of all PKI components either controlled or contracted by IdenTrust, such as artifacts validating external Registration Authority audit results. 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.

IdenTrust is not reliant on, nor does it have an MOA with any other PKI, for the implementation and compliance with the ACES CP and CPS; therefore beyond the inclusion of the results of audits performed by IdenTrust-authorized external Registration Authorities, no other external audit materials are required.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

IdenTrust shall correct any deficiencies noted during compliance reviews, as specified by GSA. The results of compliance audits will not be made public except as described in Section 8.6.

If an auditor finds discrepancies between how IdenTrust is designed or is being operated or maintained, the requirements of the ACES CP, any applicable MOAs, and/or the ACES 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.

- IdenTrust shall determine what further notifications or actions are necessary to meet the requirements of the ACES CP, this ACES CPS, and any relevant ACES MOA provisions.
- GSA will address any identified deficiencies with the IdenTrust and IdenTrust 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 IdenTrust ACES CA to perform a new audit at the expense of IdenTrust.

8.6 COMMUNICATION OF RESULTS

IdenTrust posts its auditor's CA Web Trust certification on its web site in accordance with applicable AICPA audit-reporting standards. IdenTrust complies with and provides all audit information to the ACES PMO as detailed in the Federal Public Key Infrastructure (FPKI) Annual Review Requirements Version 1.0.

Audit information is not made publicly available when that information might pose an immediate threat of harm to Program Participants or that could potentially compromise the future security of IdenTrust's operations.

The results of IdenTrust's compliance audit are fully documented, and reports resulting from Quality Assurance Inspections are submitted to GSA within 30 calendar days of the date of their completion.

The CP/CPS compliance report shall identify the versions of the ACES CP and the ACES CPS used in the assessment.

8.7 INTERNAL AUDITS

8.7.1 Internal Audits

IdenTrust conducts a separate internal Audit to ensure the SSL Certificates issuance quality to the standards outlined in this ACES CPS. These audits are conducted quarterly on one or 3% of randomly selected SSL Certificates issued in the prior quarter (whichever is larger in volume). The Certificates selected are chosen from the period immediately after the prior Audit. Results from these quarterly Audits are saved and provided upon request to third-party Auditors.

8.7.2 Actions Taken as a Result of Internal Audit Deficiency

If an internal Audit conducted quarterly determines the Certificate issuance quality of SSL Certificates has deficiencies between how IdenTrust is designed or is being operated or maintained as a CA and the requirements of the ACES CP and this ACES CPS, the following actions will be performed:

- The security officer will note the discrepancy;
- The security officer will notify IdenTrust about the discrepancy;
- IdenTrust will address any identified discrepancies; and
- IdenTrust will correct any deficiencies noted during compliance reviews, as specified by the management including proposing a remedy and expected time for completion.

The results of IdenTrust's internal certificate issuance quality Audit for SSL Certificates are fully documented, and reports resulting from it are submitted to the Chief Information Officer within 30 calendar days of the date of their completion by the security officer. Such reports will identify the ACES CP and the ACES CPS used in the assessment including their dates and version numbers.

8.7.3 Technical Access Controls

IdenTrust shall provide technical access controls designed to provide least privilege and protections against unauthorized access to IdenTrust's ACES system resources. Technical controls shall be developed and implemented in accordance with FIPS Publication 83, Federal law, regulations and guidelines in addition to GSA security policy and supporting security guidelines. IdenTrust describes its technical security controls in the SSP.

The system shall support a lock-out threshold if excessive invalid access attempts are input, and shall record when an administrator unlocks an account that has been locked as a result or unsuccessful authentication attempts. User IDs must be revoked if a password attempt threshold of three failed login attempts is exceeded.

8.7.4 Identification and Authentication

All ACES systems shall incorporate proper user authentication and identification methodology. This methodology shall include the use of user ID/password, token-based, and/or biometrics authentication schemes. The use and enforcement of password security shall be in accordance with GSA security policy and supporting security guidelines.

Users shall be required to identify themselves uniquely before being allowed to perform any actions on the system. IdenTrust's ACES system internally maintains the identity of all users throughout their active sessions on the system and is able to link actions to specific users. Identification data must be kept current by adding new users and deleting former ones. User IDs that are inactive on the system for a specific period of time (e.g., three months) shall be disabled. IdenTrust authenticates all data requests from the application.

The SSP describes the self-protection techniques for user authentication, any policies that provide for bypassing user authentication requirements, single-sign-on technologies (host-to-host authentication servers, user-to-host identifier, and group user identifiers), and any compensating controls.

8.7.5 Trusted Paths

ACES accountability shall cover a trusted path between the user and the system. A trusted path is a secure means of communication between the user and the system. For example, when a user types in their account name and password, the user wants to be sure that it is the system that the user is talking to, not a malicious program that someone else has left running on the terminal.

SECTION 9: OTHER BUSINESS AND LEGAL MATTERS

As an authorized Certification Authority for the ACES program, IdenTrust follows the privacy policies and procedures described in this Section 9. These privacy policies and procedures (PPPs) are in addition to those described elsewhere in this ACES CPS, and apply to all ACES certificates issued by IdenTrust. In addition, it is IdenTrust's policy that all officers and employees working with ACES information read and understand the IdenTrust CPS and its privacy policies and procedures. After reading this ACES CPS, officers and employees must sign a letter indicating that they have read and understood the ACES CPS and its privacy policies and procedures.

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

Fees may be assessed for certificate issuance and for certificate renewal (Re-key). Fees will not be assessed for certificate suspension and revocation.

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees (Certificate Validation Services)

Fees may be assessed for certificate validation services based upon Relying Party agreements negotiated between IdenTrust and the validating party.

9.1.4 Fees for Other Services such as Policy Information

IdenTrust may charge for recovery of escrowed decryption keys, but shall not impose fees for access to policy information.

9.1.5 Refund Policy

Refunds are not provided unless other arrangements are specifically made through customer agreements

9.2 FINANCIAL RESPONSIBILITY

Not applicable.

9.2.1 Insurance Coverage

Not applicable

9.2.2 Other Assets

CAs and RAs shall maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to entities described in Section 1.3 of this ACES CPS.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Information provided to IdenTrust that is within the scope of information described in Section 9.3.1 shall be protected by IdenTrust in accordance with Section 9.3.3 except to the extent such information consists of information within the scope of any of the exclusions or exceptions provided for in under Section 9.3.3 or Section 9.4.3 or Section 9.4.5 or Section 9.4.6 or Section 9.4.7.

9.3.1 Scope of Confidential Information

Any information provided by any LRA or TA where such information is within the scope of information described in Section 9.4.2. Any information provided to IdenTrust by the GSA or other U.S. government agency in connection with the ACES program.

9.3.2 Information Not Within the Scope of Confidential Information

See Section 9.4.3.

9.3.3 Responsibility to Protect Confidential Information

IdenTrust shall take commercially reasonable steps to protect the confidentiality of any GSA or other U.S. government information provided to IdenTrust. Such information shall be used only for the purpose of providing CA Services and as provided for under any of the ACES CP, this ACES CPS, or the ACES MOA, and shall not be disclosed in any manner to any person except as provided for under any of the ACES CP, this ACES CPS, or the ACES MOA.

9.4 PRIVACY OF PERSONAL INFORMATION

IdenTrust implements appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained, in accordance with the requirements of the ACES CP and the ACES MOA.

9.4.1 Privacy Plan

IdenTrust's written Privacy Policies and Procedures (PPP), designed to comply with the requirements of the ACES CP and the ACES MOA, may be found in Section 9.4 and its subparts. In addition, Section 9.4 and its subparts, as well as the PPP, describe the practices and procedures of IdenTrust relative to the requirements of Appendix J of NIST 800-53.

9.4.2 Information Treated as Private

Certificates issued by IdenTrust only contain information that is necessary for their effective use. Non-Certificate information, however, is requested from applicants and is required to identify Subscribers, issue Certificates and manage information on behalf of Subscribers. Such information includes numeric identifiers of driver's licenses, credit card accounts, passports, social security numbers and other identifiers, as well as business or home addresses and telephone numbers (See Section 3). Such personal information collected by IdenTrust is treated as private and is not disclosed unless otherwise required by law or for auditing purposes. All non-Certificate, non-repository information in IdenTrust records will be handled as sensitive, and access will be restricted to those with business, operational or official needs. Certificate-restricted access will require presentation of a user's Certificate, and only the appropriate access permissions will be granted to the user.

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 CA Services and carrying out the provisions of the ACES CP and IdenTrust's ACES MOA. However, a compilation of such

information about the Subscriber or Sponsoring Organization named in any given certificate issued pursuant to this ACES CPS shall be treated as confidential.

9.4.4 Responsibility to Protect Private Information

Each officer or employee of IdenTrust to whom information may be made available or disclosed shall be notified in writing by IdenTrust that information disclosed to such officer or employee can be used only for a purpose and to the extent authorized in this ACES CPS. Any GSA or Government information collected by IdenTrust will not be used, and will not be divulged or made known in any manner to any person, except as may be necessary for IdenTrust to fulfil its duties and obligations or enjoy its rights and privileges as provided for under this ACES CPS, the ACES CP, or IdenTrust's ACES MOA. IdenTrust assumes responsibility for protecting the confidentiality of its records and for ensuring that all work is performed under the supervision of IdenTrust or IdenTrust's responsible employees. IdenTrust promulgates and maintains written Privacy Policies and Procedures to comply with the requirements of the ACES MOA. These policies and procedures have been incorporated into this ACES CPS and contain the rules of conduct that are used to instruct IdenTrust's officers and employees in compliance requirements and penalties for noncompliance. The PPP can be accessed on the IdenTrust website at https://www.identrust.com/privacy.html.

9.4.5 Notice and Consent to Use Private Information

IdenTrust protects 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 the requirements stated in the ACES CP. Such information is used only for the purpose of providing CA Services and carrying out the provisions of the ACES CP and the ACES MOA, and is not 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 CA Services in accordance with ACES MOA.

For purposes of notification of the existence of and granting access to records, IdenTrust 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.

Under no circumstances shall IdenTrust (or any Authorized RA, CMA, or Repository) have access to the private signature keys of any Subscriber to whom it issues an ACES Certificate.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

IdenTrust may release sensitive information to law enforcement officials as required by law, government rule or regulation, or order of a court of competent jurisdiction. Disclosure is permitted to any agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity. IdenTrust will make reasonable efforts to provide notice of any such disclosures except when it is prohibited by law (e.g., ongoing criminal investigations, national security, etc.).

9.4.7 Other Information Disclosure Circumstances

Personal information submitted by Subscribers:

a) Shall be made available by IdenTrust to the Subscriber involved following an appropriate request by such Subscriber;

b) Shall be subject to correction and/or revision by such Subscriber;

c) Shall be protected by IdenTrust in a manner designed to ensure the data's integrity; and

d) Is not be used or disclosed by IdenTrust 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. Access Certificates for Electronic Services, ACES, and the ACES OIDs are the property of GSA, which may be used only by IdenTrust in accordance with the provisions of the ACES CP, this ACES CPS and IdenTrust's ACES MOA. Any other use of the above without the express written permission of GSA is expressly prohibited.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

IdenTrust is responsible for all aspects of the issuance and management of ACES Certificates, including the application/enrollment process; the identification verification and authentication process; the verification of authorization by Domain Name Registrant as described in Section 3.2.3.2.1; the certificate manufacturing process; dissemination and activation of the certificate; publication of the certificate (if required); renewal, suspension, Revocation, and replacement of the certificate; verification of certificate status upon request; maintenance of an online 24x7 publicly accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates as described in Section 2.2.1, and ensuring that all aspects of IdenTrust's services, operations and infrastructure related to ACES Certificates are performed in accordance with the requirements, representations, and warranties of the ACES CP (except in circumstances where government agencies or Relying Parties agree to provide defined RA roles and functions).

IdenTrust assumes responsibility for ensuring that all work is performed under the supervision of IdenTrust and responsible IdenTrust employees. IdenTrust provides assurance of the trustworthiness and competence of its employees and their satisfactory performance of duties relating to the provision of ACES services as described in this ACES CPS and other relevant documents. Each IdenTrust employee to whom information is made available or disclosed is notified in writing by IdenTrust that information disclosed to such employee can be used only for the purpose and to the extent authorized in the ACES CP and other relevant documents.

IdenTrust complies with all applicable Federal and GSA requirements set forth in its ACES MOA and regulations governing the prevention and reporting of waste, fraud and abuse, as supported by the documentation that it submits to GSA and/or other Federal agencies. IdenTrust has standard forms for contracts, which contain IdenTrust's obligations among different classes of subscribers and relying parties. IdenTrust's system architectures support varying levels of workload, as set forth in the ACES MOA.

9.6.2 RA Representations and Warranties

A Registration Authority (RA) is a person or entity responsible for the applicant registration, certificate application, and authentication of identity functions for Unaffiliated Individuals, Business Representatives, State and Local Government Representatives, Servers, and Relying Parties. An Authorized RA may also be responsible for handling suspension and Revocation requests, and for aspects of Subscriber education.

Authorized RAs retained under contract to perform RA services on behalf of IdenTrust are required to comply with the provisions of this ACES CPS and the ACES CP.

Trusted Agents are responsible for reviewing and collecting registration data and completed in-person registration forms for submission to IdenTrust or its Authorized RA as part of a bulk-loading registration process for applicants who are authorized by the Trusted Agents' organization to hold an ACES Certificate. IdenTrust enters into contractual agreements with some Trusted Agents and Authorized RAs requiring them to retain and protect collected information in accordance with applicable requirements of the ACES CP. IdenTrust and its Authorized RAs and Trusted Agents shall accurately verify subscriber identity and process requests and responses timely and securely. IdenTrust's Authorized RAs and Trusted Agents shall comply with this ACES CPS and the ACES CP. IdenTrust will monitor the compliance of its Authorized RAs and Trusted Agents with this ACES CPS and the ACES CP. Failure to comply with the provisions of this ACES CPS and the correlated CP may subject IdenTrust, and any Authorized RA or Trusted Agent, to sanctions, including possible civil and criminal sanctions, as well as termination by IdenTrust of the entities Authorized RA or Trusted Agent status and relationship with IdenTrust.

9.6.3 Subscriber Representations and Warranties

Each Subscriber 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. With respect to device certificates, the human sponsor of such certificate shall sign on behalf of the device.

Without forming any limitation on the duties and obligations that IdenTrust may require the Subscriber to agree on, Subscribers shall be required to agree to the following:

- provide complete and accurate responses to all requests for information made by IdenTrust (or a Trusted Agent or 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;
- promise to protect a private keys at all times, in accordance with the applicable Subscriber Agreement, this ACES CPS, the ACES CP and any other obligations that the Subscriber may otherwise have;
- use the ACES Certificate and the corresponding private key exclusively for purposes authorized by the ACES CP and only in a manner consistent with the ACES CP;
- instruct IdenTrust (or an Authorized RA or employer) 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 ACES Certificates, whenever the Subscriber is no longer affiliated with the Sponsoring Organization; and
- respond as required to notices issued by IdenTrust or its authorized agents.

Subscribers who receive certificates from IdenTrust shall comply with the aforementioned duties and obligations of Subscribers as well as those set forth for Subscribers the ACES CP. Additional information concerning the duties and obligations of Subscribers may be found in Sections 1.3, 3.1 and 4.1 of this ACES CPS.

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 the ACES CP or this ACES CPS.

Parties who rely upon the certificates issued under this ACES CPS must 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.

Relying Parties represent and warrant at each moment of reliance on an ACES Certificate issued hereunder that the Relying Party has noticed IdenTrust via email delivered (confirmation of receipt from IdenTrust required in order for the notice to be effective) to product@identrust.com and has via such method of contact provided IdenTrust with the Relying Party's then-current legal identity and contact information.

Each Relying Party covenants that the Relying Party will notice IdenTrust via email delivered (confirmation of receipt from IdenTrust required in order for the notice to be effective) to product@IdenTrust.com in the event that the Relying Party no longer needs to rely on any ACES Certificates.

In addition to the requirements set forth above in this section, Relying Parties must comply with the requirements applicable to Relying Parties as set forth in other sections of this ACES CPS, including but not limited to Section 4.5.2 of this ACES CPS.

9.6.5 Representations and Warranties of Other Participants

Not applicable.

9.7 DISCLAIMERS OF WARRANTIES

To the greatest extent permitted by applicable law and except as otherwise expressly provided in written contracts to which IdenTrust is a party, including IdenTrust's ACES MOA, IdenTrust disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.

Without forming limitation on the foregoing, issuance of certificates by IdenTrust or its representatives or agents in accordance with this ACES CPS does not make IdenTrust or its representative or agents, a fiduciary, trustee, or representative of any other Program Participant.

9.8 LIMITATIONS OF LIABILITY

Nothing in the ACES CP or this ACES CPS 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.

IDENTRUST SHALL HAVE NO LIABILITY FOR LOSS DUE TO USE OF AN IDENTRUST-ISSUED ACES CERTIFICATE, UNLESS THE LOSS IS PROVEN TO BE A PROXIMATE RESULT OF THE GROSS NEGLIGENCE OF, WILLFUL MISCONDUCT OF, OR FRAUD BY IDENTRUST.

IN NO EVENT SHALL IDENTRUST BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, REMOTE, EXEMPLARY, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR BUSINESS INTERRUPTION, LOSS OF PROFITS, REVENUES SAVINGS, REGARDLESS OF THE FORM OF ACTION AND REGARDLESS OF WHETHER IDENTRUST WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IDENTRUST SHALL INCUR NO LIABILITY IF IDENTRUST IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER, THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER

SYSTEM OPERATED BY ANY PARTY OTHER THAN IDENTRUST OR ANY ACT OF GOD, EMERGENCY CONDITION OR WAR OR OTHER CIRCUMSTANCE BEYOND THE CONTROL OF IDENTRUST.

Any applicable limitation of IdenTrust's liability contained in any IdenTrust agreement with a Program Participant Subscriber Agreement IdenTrust shall apply to any claim against IdenTrust by such Subscriber.

Without derogation of any other limitation of IdenTrust's liability, in no event shall the amount of IdenTrust's liability in connection with any dispute related to or arising from an ACES Certificate issued under this ACES CPS exceed the actual amount IdenTrust was paid for such Certificate.

Use of any ACES Certificate issued under this ACES CPS other than pursuant to the terms and conditions of IdenTrust applicable to such ACES Certificate is prohibited and is at the user's own risk.

9.8.1 RA, CMA, and Repository Liability

See Section 9.8.

9.9 INDEMNITIES

Neither IdenTrust nor its agents assume financial responsibility for improperly used Certificates.

Without forming any limitation on any other provision of this CPS, the ACES CP or any agreement between IdenTrust and an End Entity: (i) a Relying Party under an IdenTrust ACES Relying Party Agreement shall indemnify IdenTrust under the applicable terms and conditions of any indemnification provision therein; and (ii)a Certificate Holder under an IdenTrust ACES Certificate Agreement shall indemnify IdenTrust under the applicable terms and conditions of any indemnification provision therein.

Notwithstanding any limitations on its liability to Certificate Holders and Authorized Relying Parties, IdenTrust understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with IdenTrust do not assume any obligation or potential liability of IdenTrust under the CA/B Forum Baseline Requirements or that otherwise might exist because of the issuance or maintenance of ACES Certificates or reliance thereon by Authorized Relying Parties or others. IdenTrust will defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to an ACES Certificate issued by IdenTrust, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to an ACES Certificate issued by IdenTrust where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy an ACES Certificate that is still valid, or displaying as trustworthy: (1) an ACES Certificate that has expired, or (2) an ACES Certificate that has been revoked (but only in cases where the revocation status is currently available from IdenTrust online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.1 INDEMNIFICATION BY RELYING PARTIES

A Relying Party under an IdenTrust ACES Relying Party Agreement shall indemnify IdenTrust under the applicable terms and conditions of any indemnification provision therein.

9.9.2 Indemnification of Application Software Suppliers

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, IdenTrust understands and acknowledges that the application software suppliers who have a root Certificate distribution agreement in place with the IdenTrust do not assume any obligation or potential liability of IdenTrust under the Baseline Requirements of the CAB Forum or that otherwise might exist because of the issuance or maintenance of ACES Certificates or reliance thereon by Relying Parties or others. IdenTrust will defend, indemnify, and hold harmless each application software supplier for any and all claims, damages, and losses suffered by such application software supplier related to an ACES Certificate issued by IdenTrust, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such application software supplier related to an ACES Certificate issued by IdenTrust where such claim, damage, or loss was directly caused by such application software supplier's software displaying as not trustworthy an ACES Certificate that is still valid, or displaying as trustworthy: (1) an ACES Certificate that has expired, or (2) an ACES Certificate that has been revoked (but only in cases where the Revocation status is currently available from IdenTrust online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.3 Indemnification by Subscriber

A Subscriber under an IdenTrust ACES Subscriber Agreement shall indemnify IdenTrust under the applicable terms and conditions of any indemnification provision therein.

9.10 TERM AND TERMINATION

9.10.1 Term

This ACES CPS shall be coterminous with the ACES CP.

9.10.2 Termination

Termination of the ACES CP is at the discretion of the GSA ACES PMO.

9.10.3 Effect of Termination and Survival

The provisions of this ACES CPS necessary for IdenTrust to fulfil its obligations, if any, under Section 9.10.3 of the ACES CP shall survive termination of this ACES CPS for as long as such necessity exists.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The provisions below in Section 9.11 shall govern with respect to any notice provided in relation to this ACES CPS to or from IdenTrust; provided, however, this section shall not be construed to govern with respect to any communication, including notices, for which a different method is expressly provided for (a) in the ACES CP or this ACES CPS or (b) in an agreement between IdenTrust and the given Program Participant

9.11.1 Notices by Program Participants to IdenTrust

Notices by Program Participants to IdenTrust shall be made by at least one of the following methods, with the choice between methods to be made by the Program Participant:

i. by digitally signed communication sent from the Participant to IdenTrust via email to Registration@IdenTrust.com, which communication will be deemed effective when acknowledged via email by IdenTrust; or

ii. by written communication sent from the Program Participant to IdenTrust via internationally recognized overnight courier to IdenTrust Registration, 5225 Wiley Post Way, Suite 450, Salt Lake City, UT 84116, which such communication will be deemed effective when delivered as evidenced by written confirmation of receipt as recorded by the courier provided that such communication expressly sets forth information sufficient for IdenTrust to recognize by primary (i.e., information not requiring further reference or interpretation) the Program Participant.

9.11.2 Notices by IdenTrust to individual Program Participants

Notices by IdenTrust to individual Program Participants shall be made by at least one of the following methods, with the choice between methods to be made by IdenTrust:

i. by digitally signed communication sent from IdenTrust to the Program Participant via email to the email address of Program Participant provided for contact as requested by IdenTrust during the Program Participant's registration, contracting, or certificate lifecycle maintenance interactions with IdenTrust, which communication shall be deemed effective when sent by IdenTrust; or
ii. by written communication sent from IdenTrust to the Program Participant via U.S. Postal Service mail of the First Class to the mail address of Program Participant provided for contact as requested by IdenTrust during the Program Participant's registration, contracting, or certificate lifecycle maintenance interactions with IdenTrust.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

9.12.1.1 Amendments to the ACES CP

See Section 9.12.1.2.

9.12.1.2 Amendments to the IdenTrust ACES CP

IdenTrust makes this ACES CPS and a copy of the ACES CP available on its Website at the following Internet address:

http://www.identrust.com/certificates/aces_policies.html

IdenTrust makes copies of this ACES CPS and copies of the ACES CP available in hardcopy (i.e., printed on paper). IdenTrust reserves the right to subject its fulfilment of any request for a hardcopy to payment in advance to IdenTrust for time, materials, consumables, processing, and postage costs relative to requests for hardcopies. The foregoing shall not be construed as IdenTrust charging for the content for which the hardcopy is a carrier medium, but for the printing, tangible materials, consumables, time, and postage costs relative to the producing and sending the hardcopy.

9.12.2 Notification Mechanism and Period

Notice of all proposed changes to this ACES CPS that may materially affect users of IdenTrust's services under the ACES CP (i.e., changes other than editorial or typographical corrections, changes to contact details set forth herein, or other changes of a similar nature so far as effect on the rights, duties, obligation, and benefits of Program Participants) will be provided by IdenTrust (a) to the GSA directly by electronic mail and (b) to other Program Participants, including Relying Parties and Subscribers, by being posted on IdenTrust's Website at the following Internet address: http://www.identrust.com/certificates/aces_policies.html.

IdenTrust shall be deemed to have advised Subscribers of revisions made to the ACES CPS by (a) the posting as described above in this section of proposed revisions, and (b) where changes materially affect users of IdenTrust's services under the ACES CP (i.e., changes other than editorial or typographical corrections, changes to contact details set forth herein, or other changes of a similar nature so far as effect on the rights, duties, obligation, and benefits of Program Participants), emailing the Subscriber at the email address of the Subscriber contained in the Subscriber's Certificate so as to communicate that proposed revisions to the ACES CPS have been posed as described above in this section.

Any interested person may provide comments to IdenTrust concerning this ACES CPS.

IdenTrust shall review this ACES CPS at least once per calendar year.

Exclusive of revisions to this ACES CPS to effect editorial or typographical corrections, changes to contact details set forth herein, or other changes of a similar nature so far as effect on the rights, duties, obligation, and benefits of Program Participants, GSA must approve any revisions to this ACES CPS prior to such revisions becoming effective and, provided such approval is obtained, each approved, revised ACES CPS shall become effective and supersede the prior effective ACES CPS version when posted by IdenTrust to its Website at the following Internet address:

http://www.identrust.com/certificates/aces_policies.html.

9.12.3 Circumstances under Which OID Must Be Changed

OIDs will be changed if the ACES PMO determines that a change in the ACES 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 the ACES CP, ACES MOAs, or this ACES CPS, or agreements other than the ACES CP, the ACES MOA, or this ACES CPS but which are related to this ACES CPS, which such other agreements 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). The foregoing shall not limit recourse of any entity to take action in any court of competent jurisdiction should such negotiations not produce a resolution within 90 days of such notice becoming effective. Notwithstanding the foregoing, in no event shall the provisions of this section preclude IdenTrust, in its sole discretion, from suspending or revoking any certificate in accordance with the provisions hereof, the ACES MOA or any agreement referenced herein, including Subscriber Agreements or from taking, or not taking, any other action in order for IdenTrust to fulfil or enjoy, as applicable, a right, duty, obligation, or benefit that is IdenTrust's hereunder, under the ACES MOA, or any agreement referenced herein, including Subscriber Agreements.

9.14 GOVERNING LAW

9.14.1 Governing Law ACES CP

The laws of the United States and the State of Utah shall govern the enforceability, construction, interpretation, and validity of this ACES CPS.

9.14.2 Governing Law IdenTrust ACES CPS

The laws of the United States and the State of Utah shall govern the enforceability, construction, interpretation, and validity of this ACES CPS.

9.15 COMPLIANCE WITH APPLICABLE LAW

IdenTrust shall comply with those Federal laws of the United State of America applicable to IdenTrust's duties and obligations hereunder, and where not pre-empted by such Federal law, IdenTrust shall comply with those laws of the State of Utah applicable to IdenTrust's duties and obligations hereunder.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

Not applicable.

9.16.2 Assignment

IdenTrust may assign its rights, duties, benefits, and obligations under this ACES CPS as permitted by the GSA. No other entity with rights, duties, obligations, or benefits under this ACES CPS can assign any of its/their rights, duties, obligations, or benefits under this ACES CPS without the consent of IdenTrust made in writing and signed by an officer or director of IdenTrust.

9.16.3 Severability

9.16.3.1 Severability ACES CP

Should it be determined by a court of competent jurisdiction that any provision of this ACES CPS is incorrect, illegal, invalid, or unenforceable, the other provisions of this ACES CPS shall, to the extent greatest extent possible, remain in effect. Any revisions to address Sections determined to be incorrect or invalid will be made by amendment as provided for in Section 9.12.

In the event IdenTrust becomes aware of a conflict between this CPS and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which IdenTrust operates or issues ACES Certificates, IdenTrust will modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction.

This applies only to operations or certificate issuances that are subject to that Law. In such event, IdenTrust will immediately (and prior to issuing a ACES certificate under the modified requirement) include a detailed reference to the Law requiring a modification of this CPS under this section, and the specific modification to this CPS implemented by IdenTrust. IdenTrust will also (prior to issuing an ACES SSL certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to this CPS accordingly.

Any modification to IdenTrust practice enabled under this section will be discontinued if and when the Law no longer applies, or this CPS is modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CPS and a notice to the CA/Browser Forum, as outlined above, will be made within 90 days.

9.16.3.2 Severability IdenTrust ACES CPS

Should it be determined that one section of this ACES CPS is incorrect or invalid, the other sections of this ACES CPS shall remain in effect until the ACES CPS is updated.

9.16.4 Enforcement (Attorney Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

IDENTRUST SHALL NOT INCUR LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: (I) ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; (II) CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; (III) THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IDENTRUST HAS NO CONTROL; (IV) FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; (V) STRIKE; (VI) ACTS OF TERRORISM OR WAR; (VII) ACT OF GOD; OR (VIII) OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL.

9.17 OTHER PROVISIONS

9.17.1 Waivers

No waiver by IdenTrust of any default by another entity on an obligation or duty under this ACES CPS will operate as a waiver of any other default, or of a similar default on a future occasion. No waiver of any provision of this ACES CPS by IdenTrust will be effective unless such waiver makes express reference to a waiver of a particular section or sections of this ACES CPS and is made in writing and signed by an officer or director of IdenTrust.

To be legally valid, an ACES Certificate must be issued in accordance with the ACES CP, this CPS and any applicable law.

9.17.2 Acceptance

The act of Acceptance will be logged by IdenTrust and may consist of a record made when the End Entity downloads the Certificate. Such act will be recorded and maintained in an auditable trail kept by IdenTrust in a trustworthy manner that comports with industry standards and any applicable laws or provisions of the ACES CP, this CPS or related agreements.

9.17.3 Operational Period

A revoked or expired ACES Certificate may not be used for any purpose. No action taken by an Authorized Relying Party will be considered valid for purposes of this PKI unless the Digital Signature of the Authorized Relying Party verification request is able to confirm that the Digital Signature in question was created during the Operational Period of a valid ACES Certificate.

9.17.4 Rules of Repose Allowing Ultimate Termination of Certificate

Unless otherwise specified by the Parties, reliance on an ACES Certificate is no longer enforceable by an Authorized Relying Party against IdenTrust or RA four months after termination of the applicable Authorized

Relying Party Agreement or two years after the Authorized Relying Party's validation of the ACES Certificate with IdenTrust's Repository, whichever occurs first.

APPENDIX A: APPLICABLE STANDARDS AND GUIDELINES

SEE APPENDIX A OF THE ACES CP available online at:
https://secure.identrust.com/certificates/policy/aces/index.html

APPENDIX B: ACRONYMS AND ABBREVIATIONS

AIA	Authority Information Access
AIS	Automated Information System
CAA	Certification Authority Authorization
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
CSA	Certificate Status Authority
CSOR	Computer Security Object Registry
DBA	Doing Business As
DCID	Director of Central Intelligence Directive
DES	Data Encryption Standard
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DN	Distinguished Name
DOD	Department of Defense
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard

EO	Executive Order
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FedCIRC	Federal Computer Incident Response Capability
FED-STD	Federal Standard
FIPS	Federal Information Processing Standards
FIPS PUB	(US) Federal Information Processing Standard Publication
FISCAM	Federal Information System Controls Audit Manual
FPKI	Federal Public Key Infrastructure
FPKI Management Authority	Federal PKI Management Authority
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
FPKIPA	Federal PKI Policy Authority
GAO	(US) General Accounting Office
GPEA	Government Paperwork Elimination Act of 1998
HAG	High Assurance Guard
IATO	Interim Authority to Operate
IAW	In Accordance With
IETF	Internet Engineering Task Force
IS	Information System
ISO	International Organization for Standardization
ISSM	Information System Security Manager
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)
NAC	National Agency Check
NACIC	National Agency Check with Inquiries Credit
NIACAP	National Information Assurance Certification and Accreditation Process
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OID	Object Identifier
OMB	(US) Office of Management and Budget
OPM	(US) Office of Personnel Management
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PIN	Personal Identification Number
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
RPS	Registration Practices Statement
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SBU	Sensitive But Unclassified
SHA-1	Secure Hash Algorithm, Version 1
SHS	Secure Hash Standard
SIA	Subject Information Access
S/MIME	Secure Multipurpose Internet Mail Extension
SO	System Owner
SPM	Security Program Manager
SSL	Secure Sockets Layer
SSP	System Security Plan
TAISS	Telecommunications and Automated Information Systems Security
TSDM	Trusted Software Development Methodology
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WAN	Wide Area Network
WWW	World Wide Web

APPENDIX C: AUDITABLE EVENTS TABLE

(Used for Mapping with the ACES CP)

Auditable Event	Basic	Medium
SECURITY AUDIT		
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X
Any attempt to delete or modify the Audit logs	X	X
Obtaining a third-party time-stamp		
IDENTIFICATION AND AUTHENTICATION		
Successful and unsuccessful attempts to assume a role	X	X
Change in the value of maximum authentication attempts	X	X
Maximum number of unsuccessful authentication attempts during user login	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X
An Administrator changes the type of authenticator, e.g., from password to biometrics	X	X
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 IdenTrust generates a key. (not mandatory for single session or one-time use symmetric keys)	X	X
PRIVATE KEY LOAD AND STORAGE		
The loading of Component private keys	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
All changes to the trusted public keys, including additions and deletions	X	X

Auditable Event	Basic	Medium
SECRET KEY STORAGE		
The manual entry of secret keys used for authentication		
PRIVATE KEY AND SECRET KEY EXPORT		
The export of private and secret keys (keys used for a single session or message are excluded)	X	X
CERTIFICATE REGISTRATION		
All certificate requests, including: date and time of request, type of event, and request information automatically logged by the application. This includes initial application, issuance, Renewal, and Re-key requests as well as sender/requester DN, Certificate serial number, date and time of response and success or failure indication are automatically logged by the application; manual interactions with participants such as telephone or in person inquiries and results of verification calls will be logged manually in a logbook or in a computer-based recording/tracking system and include date/time, description of interaction and identity provided	X	X
CERTIFICATE REVOCATION		
All certificate Revocation requests including: Date and time of Revocation request, sender/requester DN, Certificate serial number, subject DN of Certificate to revoke, End Entity's common name, Revocation reason, date and time of response and success or failure indication are automatically logged by the application; manual interactions with requestors such as telephone or in person inquiries and requests for Revocation are logged manually in a logbook or in a computer-based recording/tracking system. The date/time, description of interaction and identity provided are also recorded.	X	X
CERTIFICATE STATUS CHANGE APPROVAL		
The approval or rejection of a certificate status change request	X	X
AUTHORIZED CA CONFIGURATION		
Any security-relevant changes to the configuration of the CA	X	X
ACCOUNT ADMINISTRATION		
Roles and users are added or deleted	X	X
The access control privileges of a user account or a role are modified	X	X
CERTIFICATE PROFILE MANAGEMENT		

Auditable Event	Basic	Medium
All changes to the certificate profile	X	X
REVOCATION PROFILE MANAGEMENT		
All changes to the revocation profile	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
All changes to the certificate Revocation list profile	X	X
MISCELLANEOUS		
Appointment of an individual to a trusted role		
Designation of personnel for multiparty control		
Installation of the Operating System	X	X
Installation of the CA	X	X
Installing hardware cryptographic modules		X
Removing hardware cryptographic modules		X
Destruction of cryptographic modules	X	X
System Startup	X	X
Logon Attempts to CA Apps	X	X
Receipt of Hardware / Software		X
Attempts to set passwords	X	X
Attempts to modify passwords	X	X
Backing up CA internal database	X	X
Restoring CA internal database	X	X
File manipulation (e.g., creation, renaming, moving)		X
Posting of any material to a repository		X
Access to CA internal database		X
All certificate compromise notification requests	X	X
Loading tokens with certificates		X
Shipment of Tokens		X
Zeroizing tokens	X	X
Re-key of CA	X	X
Configuration changes to the CA server involving:		
Hardware	X	X
Software	X	X
Operating System	X	X
Patches	X	X

Auditable Event	Basic	Medium
Security Profiles		X
PHYSICAL ACCESS / SITE SECURITY		
Personnel Access to room housing CA		X
Access to CA server		X
Known or suspected violations of physical security	X	X
ANOMALIES		
Software Error conditions	X	X
Software check integrity failures	X	X
Receipt of improper messages		X
Misrouted messages		X
Network attacks (suspected or confirmed)	X	X
Equipment failure	X	X
Electrical power outages		X
Uninterruptible Power Supply (UPS) failure		X
Obvious and significant network service or access failures		X
Violations of Certificate Policy	X	X
Violations of Certification Practice Statement	X	X
Resetting Operating System clock	X	X

APPENDIX D: CERTIFICATE PROFILES

IdenTrust ACES Certificate profiles are maintained in a separate document and can be made available by making a request through the IdenTrust Service Center. See Section 1.5.2.3 IdenTrust Service Center for procedures for contacting the Service Center.

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.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
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.
Attribute Authority	An entity recognized by the Federal PKI Policy Authority or comparable Agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
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.
Authority Information Access	An extension in a Certificate that indicates how to access information and services for the issuer of the certificate in which the extension

	appears. Information and services may include on-line validation services and CA policy data.
Authorized Registration Authority	A Registration Authority that is either an IdenTrust-employed registration agent, an RA under contract for managing ACES certificates, or an Agency under a contractual or other agreement to perform RA functions.
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.
CAA	A Certification Authority Authorization (CAA) record is used to specify which certificate authorities (CAs) are allowed to issue certificates for a domain.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and Revocation.
CA/B Forum or CA/Browser Forum	The Certificate Authority and Browsers Forum is a voluntary organization of leading certification authorities (CAs) and vendors of Internet browser software and other applications. Members of the CAB Forum provide guidelines known as the CA/Browser Forum Baseline Requirements for the Issuance and management of Publicly-Trusted Certificates and means of implementation for the extended validation SSL Certificate standard as a way of providing a heightened security for internet transactions and creating a more intuitive method of displaying secure sites to internet users.
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 a CP, the term “Certificate” refers to certificates that expressly reference the OID of the same CP in the “Certificate Policies” field of an X.509 v.3 certificate.
Certificate Management Authority (CMA)	An entity that is delegated or outsourced the task of actually manufacturing the certificate on behalf of an Authorized 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 that is maintained by a Certification Authority, of the certificates which it has issued and that have been revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
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 that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Component Private Key	Private key associated with a function of the certificate issuing equipment, as opposed to being associated with an operator or administrator.

Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
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.
Domain Name	The label assigned to a node in the Domain Name system.
Domain Registrant (also Domain Name Registrant)	Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
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 as defined above.
Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption	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.
Federal Bridge Certification Authority Membrane	The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.
FBCA Operational Authority	The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The 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.
Fully Qualified Domain Name (FQDN)	A Domain Name that includes the labels of all superior nodes in the internet Domain Name System.
GET Method	GET Method: An OCSP request using the GET Method is constructed as follows: GET {url}/{url-encoding of base-64 encoding of the DER encoding of the OCSPRequest} where {url} may be derived from the value of the authority information access extension in the certificate being checked for revocation, or other local configuration of the OCSP client.
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.
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
High Risk FQDN List	A list of fully qualified domain names that have been identified through research during the verification and validation of the SSL application as being high risk. This list is compiled and maintained by IdenTrust.
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.
Inside Threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Integrity	Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
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.
Least Privilege	The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks in order to limit the damage that can be caused by accident, error, or unauthorized use**.**
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.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
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 (OOB)	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	A natural person or PKI Sponsor who is employed by the Sponsoring Organization or an authorized agent who has express authority to represent the organization but is not the Subscriber for non-human

	system Devices that are named as Public Key Certificate subjects. The PKI Sponsor is responsible for meeting the obligations of Subscribers as defined throughout this CP. The Sponsoring Organization verifies the PKI Sponsor is an individual that: (i) signs and submits, or approves a Device Certificate request on behalf of the organization, and/or (ii) signs and submits a Subscriber Agreement on behalf of the organization, and/or (iii) acknowledges and agrees to the Certificate Terms of Use on behalf of the organization when the organization is an affiliate of the CA. This term is referred to as Applicant representative in the Baseline Requirements for the CAB Forum.
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 to which requirements of confidentiality apply under Section 9.4 hereof, which statement for every computer system of IdenTrust used to maintaining a system of records containing such information**.**
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or 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 (Revocation)	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 Officer	Described in Section 5.2.1.4.
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.
Subject Information Access	An extension in a Certificate that indicates how to access information and services for the subject of the certificate in which the extension appears. When the subject is a CA, information and services may include certificate validation services and CA policy data. When the subject is an end entity, the information describes the type of services offered and how to access them.
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 High	The highest security level supported by an information system.
System Security Plan (SSP)	Documentation of the management, technical, and operational security controls of an automated information system.
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.
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with 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 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 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.