IdenTrust
Certification Practice Statement
for the
US Department of Defense
External Certification Authority (ECA) Program
Version 2.1

March 30, 2018

IdenTrust Services, LLC

TABLE OF CONTENTS

Revision History

Revision	Date	Summary of Changes/Comments
1.0	November 8, 2006	Original
1.1	August 27, 2008	Updated to reflect select portions of ECA Certificate Policy (v. 4.0) that deal with Medium Token Assurance Certificates and 2048-bit public keys. Clarified form submission and review processes stated in 4.1.1.4 and 4.1.1.5. Also made other conforming changes for purposes of cross-referencing relocated sections of v.4 of the Certificate Policy.
1.2	November 26, 2008	Converted to RFC 3647 Format for compliance with v.4.0 of ECA CP. Clarified (1) requirements for organizational affiliation, (2) procedures for enrollment by Trusted Correspondents, (3) delivery mechanisms for registration materials, (4) revocation procedures, (5) descriptions of security at RA and off-site storage sites, and (6) use of 2048-bit RSA. Addressed obsolescence of FIPS 112 and revised legal forms.
2.0	April 8, 2016	Updated to include changes to conform to the ECA Certificate Policy documents (versions 4.1, 4.2, 4.3 and 4.4). Integrated all changes included in the "Errata to IdenTrust Certification Practices Statement for the U.S. DOD ECA Program, Version 1.1, dated 8/27/2008.
2.1	March 30, 2018	Updated to new branding standards and clarify language regarding Trusted Roles in sections 5.1 Physical Controls and 9.4.2 Information Treated as Private.

1. Introduction

This Certification Practice Statement ("CPS") is a statement of the policies, practices and procedures used by IdenTrust Services, LLC ("IdenTrust") while acting as an External Certification Authority ("ECA"). Certain operational details have been left out of the published version of this CPS in the interest of system security. The published version is referred to as the public version of the CPS.

This CPS governs the issuance, management and use of Medium Assurance X.509 public-key Certificates, including Medium Assurance Certificates, Medium Token Assurance Certificates, and Medium Hardware Assurance Certificates, as defined in the Certificate Policy for External Certification Authorities Version 4.4 (October 1, 2015), as published by the US Department of Defense ("DOD") and downloadable from http://iase.disa.mil/pki/eca/Pages/documents.aspx (the "ECA CP").

The outline and content of this CPS are in accordance with [IETF RFC 3647], which is entitled "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". Unless otherwise noted, capitalized words or phrases have the meaning given to them in the Section 14, Glossary of Terms, which is near the end of this document. Also, forms of the verb "confirm" and the noun "confirmation" have the meanings given to the word "confirm" in Section 14, even when not capitalized.

1.1 Overview

This CPS has the following purposes:

Compliance checking: It documents how IdenTrust satisfies the requirements of the ECA CP and sets the standard for IdenTrust's internal procedures and their documentation.

System specifications for contractual purposes: The public version of the CPS specifies for IdenTrust customers (Subscribers under contract with IdenTrust and ECA Relying Parties) how IdenTrust performs its public key Certificate issuance and revocation services.

System documentation for external review: Prospective IdenTrust customers can review IdenTrust's services in detail using the public version of this CPS, which is published for this reason. It enables prospective customers to evaluate IdenTrust's services and the services' suitability for the prospective customer's purposes.

Documentation of rights and obligations. Subscriber Agreements and Subscribing Organization Agreements (where applicable) and the public version of this CPS together specify the rights and obligations binding on users of IdenTrust's public key Certificate issuance and revocation services. This CPS sets out the principal rights and obligations of Subscribers and Relying Parties. While price, contractual effective date, and other customer-specific items may appear in the Subscriber Agreements and Subscribing Organization Agreements, this CPS governs in the event of conflict of its terms with the terms of such other documents as the Subscriber Agreements and Subscribing

Organization Agreements. Further, terms of this CPS cannot be changed by such other documents as the Subscriber Agreements and Subscribing Organization Agreements. In this CPS, IdenTrust specifies how it will provide its public key Certificate issuance and revocation services to its customers (Subscribers and Relying Parties). Those services consist of the following basic components:

(1) **Registration** is the process of enrolling a new customer for IdenTrust's public key Certificate issuance and revocation services. Besides contracting for IdenTrust's services, registration includes identity proofing in the case of a Subscriber, as well as documentation and archival. The identity-proofing process covers both incorporation (i.e. proper legal formation) of the Subscribing Organization and legal authorization of its signatories, and identity proofing of the Individual Subscriber.

(2) **Issuance of a Certificate** is the process of creating a Certificate and sending it to the Individual Subscriber for acceptance and installation into the Subscriber's system.

(3) **Publication of a Certificate** is the process of placing it online so as to be available to users via a Repository that can be accessed through a standard communications protocol (e.g., Lightweight Directory Attribute Protocol ("LDAP"), Hypertext Transfer Protocol ("HTTP")).

(4) **Revocation of a Certificate** is the process of invalidating it when it has become unreliable or questionable.

These functions are detailed in the remainder of this document.

In all cases, IdenTrust performs the issuance of Certificates and their publication. IdenTrust also performs revocation of a Certificate and makes the latest revocation information available through publication of CRL and through an OCSP Responder

1.2 Identification

Certificates issued pursuant to this CPS contain at least one of the following Certificate Policy OIDs. All policy OIDs from the ECA CP section 1.2 are included in this list. Those OIDs indicate that this CPS and the ECA CP apply in relation to the Certificate (see section 1.4.3). They also indicate whether the Certificate is a Medium Assurance, Medium Token Assurance, or a Medium Hardware Assurance Certificate.

Certificates issued by IdenTrust as an ECA will conform to the ECA CP Medium Assurance Certificate, Medium Token Assurance, or Medium Hardware Assurance Certificate profile with Certificate Policy Object Identifiers ("OIDs") of:

id-eca-medium ID::= {id-eca-policies 1}

id-eca-medium-hardware ID::= {id-eca-policies 2}

id-eca-medium-token ID::= {id-eca-policies 3}

id-eca-medium-hardware-sha256 ID::= {id-eca-policies 10}

The sha256 OIDs include the following:

id-eca-medium-sha256::= {id-eca-policies 4}

id-eca-medium-token-sha256::= {id-eca-policies 5}

id-eca-medium-device sha256::= {id-eca-policies 9}

where id-eca-policies represents the prefix:

{joint-iso-ccitt(2)country(16) us(840) organization(1) gov(101) csor(3) pki(2) cert-policy(1) eca-policies(12)}.

1.3 PKI Participants

1.3.1 PKI Authorities

1.3.1.1 ECA Policy Management Authority

Among other things, the ECA Policy Management Authority ("EPMA") reviews this CPS for conformity with the ECA CP. Audit reports of IdenTrust's performance according to this CPS are also reviewed by the EPMA. In operating the ECA Root CA, the EPMA determines the continuation of IdenTrust's role as an ECA within the overall ECA PKI. The EPMA is the DoD Chief Information Officer.

1.3.1.2 Certification Authority

A Certification Authority is defined in the Glossary of the ECA CP as "An authority trusted by one or more users to create and assign Certificates."[1] The ECA CP explains a Certification Authority further as:

> an entity authorized by the EPMA to create, sign, and issue public key Certificates. A CA [Certification Authority] is responsible for all aspects of the issuance and management of a Certificate, including control over the registration process, the identification and authentication process, the Certificate manufacturing process, publication of Certificates, revocation of Certificates, and re-key; and for ensuring that all aspects of the CA services and CA operations and infrastructure related to Certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy. CA is an inclusive term, and includes all types of CAs.[2]

As an ECA, IdenTrust performs its services in accordance with those requirements see section 9.6.1.

As an ECA, IdenTrust issues Certificates only to Subscribers who are end entities as described in section 1.3.3. This CPS does not apply to any Certification Authority other than IdenTrust. For that reason, all Certificates issued by IdenTrust do not contain the basicConstraint extension or set cA Boolean to false when the basicConstraints extension is included. This is intended to prevent a Subscriber from also acting as a Certification Authority. For more information about this, see the basicConstraints extension in the Certificate profiles (see section 10). The keyCertSign and cRLSign bits are never set in

[1] ECA CP section 14 (Glossary).

[2] ECA CP section 1.3.2.

order to prevent a Subscriber from signing Certificate Revocation Lists ("CRLs") or Certificates.

The IdenTrust ECA publishes CRLs, and IdenTrust's OCSP Responder provides responses to OCSP requests in order to inform prospective relying parties about the current revocation status that the IdenTrust ECA has issued. Details, including information on the timeliness of the published information, are set out in section 4.9.

All Certificates issued by IdenTrust as an ECA are verifiable by reference to a Certificate issued by the ECA Root Certification Authority. In other words, using PKI terminology, IdenTrust is subordinate to the ECA root Certification Authority in the ECA hierarchy, as provided in the ECA Root CA CPS and other documents.

1.3.1.3 Registration Authority

The ECA CP defines a Registration Authority as an:

> Entity responsible for identification and authentication of Certificate subjects [Subscribers] that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke Certificates.[3]

IdenTrust serves as a Registration Authority, utilizing its own staff to fulfill the responsibilities of the role. IdenTrust does not leverage the capabilities of a third-party Registration Authority.

The RA responsibilities are carried out by a trusted IdenTrust employee in the role of Registration Authority Operator ("RA Operator") using an RA workstation. (The RA is an entity, whereas the RA Operator is an individual.) The RA Operator receives and collects process documentation from prospective Subscribers (e.g. the notarized In-Person ID Form, which is included in section 15.4 below) and from Trusted Correspondents, (see further discussion below in sections 1.3.2.1 and 4.1.3 and form found in section 15.3) and confirms each Individual Subscriber's identity information for inclusion in the Subscriber's Certificate. The RA Operator is a Trusted Role held by an Individual who is subject to the requirements of section 5.2.1.2. Technical controls may be put in place by Operations Management so the RA may limit the RA Operator to service specific groups in the scope of their trusted responsibilities.

1.3.1.4 Certificate Management Authority

The ECA CP defines both Certification Authorities and Registration Authorities to be "Certificate Management Authorities".

The ECA CP also provides that server-based Certificate Status Authorities ("CSAs") such as OCSP Responders are also considered Certificate Management Authorities. IdenTrust itself is a Certificate Status Authority—IdenTrust does not use the services of any third party Certificate Status Authority.

Because IdenTrust operates as ECA, CSA, and RA, IdenTrust is a Certificate Management Authority as defined in the ECA CP. IdenTrust conform to the ECA CP requirements applicable to Certificate Management Authorities.

[3] ECA CP section 14 (Glossary).

CMA tasks performed by IdenTrust employees are performed by personnel in Trusted Roles as outlined in Section 5.2.1 of this CPS.

1.3.1.5 Additional Authorities

In operation as an ECA, CSA, and RA, IdenTrust also recognizes the following Authorities:

IdenTrust Policy Management Authority -

IdenTrust's Policy Management Authority oversees the administration and application of this CPS with IdenTrust. The Policy Management Authority also has charge of the future development and amendment of this CPS, as provided in sections 1.5 and 9.12.

IdenTrust ECA Appeal Officer -

For non-government Claimants desiring to contest IdenTrust's initial determination of a claim, the IdenTrust ECA Appeal Officer handles claims under the Dispute Resolution Procedures outlined in section 9.13. The IdenTrust ECA Appeal Officer reviews the decision in the exercise of its oversight of IdenTrust's policies and their implementation in practice.

Security Officer -

The Security Officer is the individual within IdenTrust, reporting directly to the Vice President of Operations or Chief Information Officer ("CIO"), who does not participate in RA, CA, or CSA functions. This position is responsible for monitoring and auditing activities, functions and work performed in relation to CA/CSA and RA functions.

Operations Management -

IdenTrust's Operations Management includes the Chief Operating Officer ("COO"), CIO, the Vice-president of Operation, and any designees they formally appoint. Operation Managers are the individuals within IdenTrust who, at the highest level, oversee and administer the operations of the ECA PKI. Their responsibilities are explained throughout this CPS.

Vice President of Operations -

The Vice President of Operations is the individual within IdenTrust ultimately responsible for overseeing the daily operation of IdenTrust's CA, CSA, and RA. If the VP of Operations is unavailable or the role is not filled, these responsibilities will be fulfilled by the CIO.

1.3.2 Registrars

IdenTrust uses the term "Registrar" to mean the person performing the in-person confirmation of the Subscriber's identification. Registrars include: Trusted Agents, Notaries, Embassy/Consular officers, Authorized DoD Employees, and Judge Advocate General (JAG) Officers may play a part in Subscriber registration. An RA Operator may also be considered a Registrar when performing the specific actions related to confirmation of the identity using approved identification.

1.3.2.1 Trusted Agents

The ECA CP defines a "Trusted Agent" as an:

> Entity authorized to act as a representative of a Certificate Management Authority in providing Subscriber identification during the registration process.[4]

IdenTrust may provide software such as web pages, forms, instructions, and other resources to facilitate the work of Trusted Agents, but it does not provide them with any interface into the systems used to issue and revoke Certificates. Trusted Agents, which are referred to hereinafter as "Trusted Correspondents," do not have privileged access to or any control over the operation of those systems.

By agreement with IdenTrust, Trusted Correspondents are subject to the responsibilities imposed by the DOD ECA CP and this CPS.

As specified in Section 1.3.6.1 of the ECA CP, IdenTrust's Trusted Correspondents are considered to be agents of the CMA.

A Trusted Correspondent is an individual who assists RA Operators by confirming and documenting the identification of an Individual Subscriber (see sections 3.2.3 and 4.2.1). A Trusted Correspondent may be one of two types. A Trusted Internal Correspondent is an employee of the same Subscribing Organization as the Individual Subscribers to be identified. A Trusted Internal Correspondent is ordinarily appointed by the Subscribing Organization subject to IdenTrust's approval. The other type of Trusted Correspondent is a Trusted External Correspondent, which is an independent third party under contract directly with IdenTrust and acceptable to the Subscribing Organization. By stating Trusted Correspondents in this CPS, it is meant to include both Trusted Internal Correspondents and Trusted External Correspondents. However if the responsibilities described are applicable to either External and Internal Trusted Correspondents, but not both, then the text will differentiate the roles by stating the full title.

When IdenTrust enters into a contract to provide public key Certificate issuance and revocation services to a Subscribing Organization, that contract obligates the Subscribing Organization to nominate a Trusted Internal Correspondent and cite the nominee's role in the Subscribing Organization and qualifications as a Trusted Internal Correspondent. The Subscribing Organization, in choosing Trusted Internal Correspondent candidates, shall ensure that there would be no conflict between the duties of that candidate as an employee of the Subscribing Organization and his or her duties as a Trusted Internal Correspondent. The nominee is appointed when IdenTrust accepts the nomination within a time limit specified in the contract. In the event that the nomination is rejected, another one is required. Appointment as Trusted Internal Correspondent includes authorization by the Subscribing Organization to fulfill all responsibilities of a Trusted Internal Correspondent on behalf of the Subscribing Organization as prescribed in the ECA CP and this CPS. The Trusted Internal Correspondent accepts the appointment and becomes personally obligated accordingly. The Subscribing Organization is similarly obligated and can bring to bear the Organization's employee discipline powers on the Trusted Internal Correspondent, should that be necessary.

[4] *Id*.

Trusted External Correspondents differ from their internal counterparts in that they are not employees of the Subscribing Organization and are not nominated by it. Instead, Trusted External Correspondents are third parties under contract directly with IdenTrust separately from any Subscribing Organization, although their service availability, location, and convenience factors must be acceptable to the Subscribing Organization and Subscriber for them to provide their services in a given instance. Like Trusted Internal Correspondents, Trusted External Correspondents are obligated by their contracts with IdenTrust to conform to the ECA CP and this CPS.

In both cases, a Trusted Correspondent's qualifications and terms of service are contractually agreed to ensure trustworthiness. IdenTrust has the contractual right to supervise a Trusted Correspondent and remove him/her from his/her role in the event he/she fails to perform his/her role as required. In the case of a Trusted Internal Correspondent, supervision by IdenTrust occurs in consultation with the Subscribing Organization, and removal only after notice to the Subscribing Organization, which then becomes obligated to nominate a successor. Before removing a Trusted Internal Correspondent, IdenTrust attempts to resolve problems by communicating with the Trusted Internal Correspondent and the Subscribing Organization to avoid disrupting service and trust relationships.

IdenTrust provides information and instructions to Trusted Correspondents, whether Internal or External, on how to perform their roles. Trusted Correspondents also have copies of the ECA CP and this CPS and are advised to study them and refer to them as necessary. In confirming and documenting identity, a Trusted Correspondent acts pursuant to contractual obligations requiring him or her, among other things, to:

Conform to the ECA CP and this CPS in providing confirmation and documentation services.

Follow IdenTrust's instructions relative to the services performed for IdenTrust.

Keep informed of responsibilities as a Trusted Correspondent by reading written instructions and any training materials provided by IdenTrust.

Demonstrate trustworthiness and competence during training and in performing verification services.

A Trusted Correspondent may also provide local support, training, and other assistance, if agreed. In some Subscribing Organizations, the Trusted Correspondent may be the Organization's PKI administrator. In others, the Trusted Correspondent may work in a Personnel or Human Resources Department. In small organizations without such departments, the Trusted Correspondent may be a person responsible for payroll functions. The contract with the Subscribing Organization ordinarily permits the Organization to appoint as many Trusted Correspondents as needed.

1.3.2.2 Notaries

IdenTrust uses the services of notaries public to assist in performing identification of applicants for Medium Assurance and Medium Token Assurance Level Certificates. Like a Trusted Correspondent, a notary assists IdenTrust by confirming and documenting the identification of an Individual Subscriber. Although IdenTrust provides forms and instructions for notaries, they are not contractually appointed but rather are commissioned

by law to Confirm personal identity, usually in conjunction with notarial acknowledgment of the authenticity of a document and/or administration of an oath. In the United States, a notary is commissioned by a state authority in the state where the notary resides. Statute and the commissioning authority prescribe how the notary is to perform its identity-confirmation function. The authority may terminate the notary's commission on grounds provided in the governing statute of the state concerned. Notaries are also generally bonded to ensure correct performance of their responsibilities.

IdenTrust uses U.S. notaries to assist in identifying the Individual Subscriber preparatory to issuance of a Medium Assurance (Software) and Medium Token Assurance (Token) Certificates. However, for a Medium Hardware Assurance Certificate, IdenTrust does not Confirm the accuracy of the Subscriber's identity based on notarial representations. Instead, identity is established through a Trusted Correspondent.

Section 4.1.2.3 on in-person registration of a Subscriber specifies how the notary is to perform his or her role.

1.3.2.3 Embassy or Consular Officers and Judge Advocate General (JAG) Officers

U.S. citizens located outside the U.S can use the notarial services provided by a United States embassy or consulate, or JAG office[5] for identity proofing of applicants for Medium Assurance and Medium Token Assurance Certificates. In doing so, they function much the same as notaries. If the embassy or consulate, or JAG office is located in Australia, Canada, New Zealand, or the United Kingdom, then its officers may provide in-person registration services for an applicant who is a citizen of one of those countries. Non-U.S. citizens who are not citizens of Australia, Canada, New Zealand, or the United Kingdom must be located in the U.S. and have their identity confirmed in accordance with Section 3.2.3, or have their identity confirmed by a Trusted Correspondent or an authorized DOD employee in accordance with Section 11 of the ECA CP.

1.3.2.4 Authorized DoD Employees

Department of Defense Employees authorized pursuant to procedures listed in Section 11.2 of the ECA CP may provide identify proofing services to foreign nationals under procedures described in Section 11.2 of the ECA CP. IdenTrust disclaims any and all liability related to the identity proofing of foreign nationals or other registration services performed by DOD employees pursuant to Section 11.2 of the CP.

1.3.3 Subscribers

Section 1.3.4 of the ECA CP defines 'Subscriber', and limits who may be a Subscriber, as follows:

[5] Judge Advocate General officers' mission is focused on providing services to Active Duty members of U.S. forces, their dependents and retirees, as their resources allow.

A Subscriber is the entity whose name appears as the subject in a Certificate, and who asserts that it uses its key and Certificate in accordance with this policy. ECA Subscribers are limited to the following categories of entities:

- Employees of businesses acting in the capacity of an employee and conducting business with a US government agency at local, state or Federal level;
- Employees of state and local governments conducting business with a US government agency at local, state or Federal level;
- Employees of foreign governments or organizations conducting business with a US Government agency at a local, state, or Federal level.
- Individuals communicating securely with a US government agency at local, state or Federal level; and
- Workstations, guards and firewalls, routers, trusted servers (e.g., database, FTP, and WWW), and other infrastructure components communicating securely with or for a US government agency at local, state or Federal level. These components must be under the cognizance of humans, who accept the Certificate and are responsible for the correct protection and use of the associated private key.

IdenTrust issues ECA Certificates to Subscribers who attest that they meet one of the definitions above and agree to the ECA CP-prescribed limitations.

In this CPS, a distinction is drawn between a Subscriber, also sometimes termed an 'Individual Subscriber', and a Subscribing Organization. A Subscribing Organization is a company, business, or other entity that is listed in an organizationalUnitName ("OU") attribute in the subject field of the Certificate, as specified in the Certificate profiles (Section 10) of this CPS. The Individual Subscriber and Subscribing Organization are distinct entities, and the relationship between the two is described in section 3.2.2.2.

IdenTrust provides its services to Individual Subscribers pursuant to a contract with the Subscribing Organization. IdenTrust does not issue Certificates to Subscribers acting in an individual capacity. It may, however, issue Certificates to Subscribers acting in a business capacity as professional consultants or DBAs.[6]. In other words, a Subscriber not affiliated with a separate organization, such as a sole proprietor, professional consultant or fictitious entity (e.g., a "doing-business-as" or "dba") must establish to IdenTrust's satisfaction that he or she is acting in a professional capacity and not solely as an individual.

1.3.4 Relying Parties

The ECA CP defines a Relying Party as follows:

[6] A DBA ("doing business as") is a fictitious business name under which a sole proprietor may conduct business as a going concern in lieu of organizing as a separate entity with limited liability (e.g. a corporation or limited liability company).

> A Relying Party is the entity who, by using another's Certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the Certificate, relies on the validity of the binding of the Subscriber's name to a public key. A Relying Party may use information in the Certificate (such as Certificate policy identifiers) to determine the suitability of the Certificate for a particular use and does so at their own risk.

Relying parties in the ECA program include the DOD. Relying parties are also often Subscribers, although possibly not Subscribers of IdenTrust-issued Certificates. IdenTrust's agreement with its Subscribers includes terms that govern reliance on IdenTrust-issued Certificates. Those terms are consistent with this CPS including section 9.6.4 (Relying Party Representations and Warranties).

Reliance on a Certificate involves drawing inferences from its content so that the content has meaning and value for a particular communication and transaction. The Certificate profiles (Section 10) of this CPS specify in detail the content of Certificates issued by the IdenTrust ECA and the inferences to be drawn from them in the reliance process.

Reliance on an ECA Certificate issued by the IdenTrust ECA is subject to the terms and conditions set out in the public version of this CPS published by IdenTrust. Publication of the public version of this CPS by IdenTrust as part of the ECA program constitutes an offer by IdenTrust, which a prospective Relying Party may accept by its act of reliance. In other words, by relying on an ECA Certificate issued by IdenTrust, the Relying Party assents to be legally bound by the applicable terms and conditions of the public version of the CPS, including the obligations of Section 9 (Other Business and Legal Matters) below.[7] Therefore, each act of reliance constitutes acceptance by the Relying Party of IdenTrust's then-current offer as reflected in the public CPS as then published.

Any attempt at reliance on an ECA Certificate except in accordance with the applicable terms of the ECA CP and the applicable provisions of the public version of this CPS (*see* footnote 7) is at the Relying Party's risk, and IdenTrust has no liability for claims arising out of such use even if a party relies to its detriment and incurs a loss; provided that the IdenTrust ECA issued the Certificate in accordance with the ECA CP and this CPS. *See* Sections 9.6.4, 9.7 and 9.8 of the ECA CP.

Nothing in this section limits IdenTrust's obligations or liability to the DOD when the DOD acts in the role of a Relying Party.

1.3.5 Other Participants

1.3.5.1 PKI Sponsor

A PKI Sponsor fulfills the role of a Subscriber for non-human system components and organizations that are named as public key Certificate subjects. The PKI Sponsor is responsible for registering system components with the Registrar. See Section 3.2.3.3.

[7] For purposes of this section, the primary provisions of the abridged CPS applicable to, and binding upon, Relying Parties include those of the following sections and their sequential numerical subsections: 1.4, 4.9.6, 4.9.10, 4.9.11, 9.2.4, 9.5 through 9.16 and Section 10 (Certificate and CRL Formats).

The PKI Sponsor is also responsible for the operation and control of the component and assumes the obligations of Subscriber for the Certificate associated with the system component, including but not limited to a duty to protect the private key of the component at all times. See Section 9.6.3.

The PKI Sponsor is not considered a Trusted Role.

The identity of a PKI Sponsor will be validated in accordance with a Subscriber's identity receiving a public key Certificate issued under this CPS.

1.3.5.2 PKI Point of Contact (POC)

PKI Point of Contact ("POC") is the person designated by the Subscriber's Organization to whom Subscribers surrender their hardware Cryptographic Modules when leaving the organization.

A PKI POC is a Trusted Role. In the majority of cases, a Trusted Internal Correspondent (see Section 1.3.2.1) is also the PKI POC for the Organization; if a Trusted Internal Correspondent is not available, Personnel Office representatives, Security Officers or Management within the Organization may become PKI POCs after they have fulfilled the requirements in Section 5.3.1 and 5.3.2 of this CPS.

The PKI POC has the obligation to zeroize or destroy the hardware Cryptographic Module promptly upon receipt. IdenTrust requires PKI POCs to have an IdenTrust ECA Certificate issued at the highest assurance level which the associated Subscribing Organization receives. Using his or her IdenTrust ECA Certificate, the PKI POC notifies the IdenTrust RA Operator of the surrendered Cryptographic Module destruction and request the revocation of all Certificates associated with the surrendered Cryptographic Module.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Appropriate Certificate uses include client authentication to web services, digital signature, and encryption through key exchange. Certificates may be used to support security services (confidentiality, integrity, authentication and technical non-repudiation) to a wide range of applications that protect various types of information, up to and including sensitive unclassified information. The security services provided by public key Certificates alone, however, may be insufficient by themselves to provide sufficient protection in all circumstances. For example, when a requirement exists to verify the authenticity of a signature beyond the Certificate validity period, such as contracting, other services such as trusted archival services or Trusted Timestamp may be necessary. Each Certificate-enabled solution is application-dependent and should be evaluated by Subscribers and Relying Parties in accordance with section 1.4.3.

1.4.2 Prohibited Certificate Uses

Certificates issued under the provisions of this CPS may not be used for: (i) any application requiring fail-safe performance such as: (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; (ii) transactions where applicable law prohibits the use of Certificates for such transactions or where otherwise prohibited by law; or (iii) applications that are classified or process classified data.

1.4.3 Applicability

Certificates issued by IdenTrust as an ECA enable the services described in section 1.4.1 of the ECA CP.

This CPS applies only in relation to Certificates that are:

(1) ECA Certificates, i.e. Certificates that list one or more of the OIDs specified in section 1.2 above;

(2) Certificates issued by the IdenTrust ECA, i.e. Certificates that list "IdenTrust ECA," or a variation thereof, in the issuer field as described in Section 10; and

(3) Certificates issued by an IdenTrust CA, which in turn has been issued a Certificate by the DoD ECA Root CA.

IdenTrust does not offer PIV-I or Group/Role Certificates at this time.

This CPS does not apply in relation to any other Certificates.

1.4.3.1 Level of Assurance

As an ECA, IdenTrust issues Certificates having three distinct levels of assurance, Medium Hardware Assurance Certificates, Medium Assurance Certificates and Medium Token Assurance Certificates. The level of assurance that IdenTrust provides for each level is in accordance with section 1.4.1.1 of the ECA CP.

1.4.3.2 Factors in Determining Usage

As specified in section 1.4.1.2 of the ECA CP, the question whether to rely on a Certificate issued by IdenTrust is for a prospective Relying Party to determine in view of various risk factors. Those factors include such things as the value of the information secured, the threat environment, and any additional protection of the secured information environment.

1.4.3.3 Threat

In determining whether to rely, a prospective Relying Party is advised to consider the security threat under the circumstances. Further information to guide such considerations is found in section 1.4.1.3 of the ECA CP.

1.4.3.4 General Usage

As an ECA, IdenTrust issues Certificates having the three levels of assurance specified in section 1.4.1.4 of the ECA CP, namely, Medium Hardware Assurance Certificates, Medium Token Assurance Certificates, and Medium Assurance Certificates. As the ECA CP provides:

- **The Medium and Medium Token Assurance Levels** are intended for applications handling sensitive medium value information, with the exception of transactions involving issuance or acceptance of contracts and contract modifications. Examples of medium and medium token assurance applications include: non-repudiation for small and medium value financial transactions other than transactions involving issuance or acceptance of contracts and contract modifications; authorization of payment for small and medium value financial transactions; authorization of payment for small and medium value travel claims; authorization of payment for small and medium value payroll; and acceptance of payment for small and medium value financial transactions.
- **Medium Hardware Assurance:** This level is intended for all applications operating in environments appropriate for medium assurance but which require a higher degree of assurance and technical non-repudiation. Examples of medium assurance hardware applications include: all applications appropriate for medium assurance Certificates; mobile code signing; and applications performing contracting and contract modifications.

It is advisable that each prospective Relying Party evaluate the assurance level of Certificates carefully.

1.5 Policy Administration

1.5.1 Organization Administering the Document

IdenTrust's Policy Management Authority oversees the administration and application of this CPS with IdenTrust. That Policy Management Authority also has charge of the future development and amendment of this CPS, as provided in this section 1.5 and in section 9.12.

1.5.2 Contact Person

Questions regarding this CPS should be directed to:

IdenTrust Policy Management Authority
5225 Wiley Post Way Suite 450
Salt Lake City, UT 84116
ecaservices@identrust.com
(888) 248-4447

1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

As provided in section 1.5.3 of the ECA CP, the EPMA determines the suitability of this CPS as part of the ECA accreditation process.

1.5.4 CPS Approval Procedures

This CPS is approved by the IdenTrust Services PMA by majority vote held during one of its scheduled meetings see also section 9.12. The EPMA will then be provided with an approved CPS to make the determination that it complies with the corresponding Certificate Policy for a given level of assurance. This compliance analysis shall be performed by an independent party.

1.5.5 Waivers

In the event IdenTrust desires a waiver in relation to any provision of this CPS, IdenTrust shall apply to the EPMA for such waiver. Any waiver granted by EPMA applicable to this CPS shall be subject to the provisions of section 1.5.5 of the ECA CP.

When acting in any PKI participant's role provided for under section 1.3 of this CPS, IdenTrust shall act in conformity with the obligations set forth in section 9.6 of this CPS that are applicable to such role; provided, however, in the event the EPMA grants IdenTrust a waiver under the provisions of section 1.5.5 of the ECA CP, IdenTrust will act in accordance with the provisions of such waiver in connection with the subject matter of such waiver.

1.6 Definitions and Acronyms

See Sections 13 and 14.

2. Publication and Repository Responsibilities

2.1 Repositories

In providing its Repository, IdenTrust will:

(1) **Maintain availability of the information** as required by the relevant stipulations of the ECA CP and this CPS.

(2) **Provide access control mechanisms** sufficient to protect Repository information as specified in section 2.4 of the ECA CP and this CPS.

2.2 Publication of Certification Information

IdenTrust provides an on-line Repository that is available to Subscribers and Relying Parties and that contains:

- Issued digital signature and encryption Certificates that assert one or more of the policy OIDs listed in this CPS;
- The most recently issued CRL(s);
- IdenTrust's Certificate(s) for its Certificate signing key(s);
- IdenTrust's Certificate(s) for its CRL signing key(s);
- Other Certificates issued to IdenTrust by the Root CA;
- A copy of the CP, including any waivers granted to IdenTrust by the EPMA; and
- An abridged version of this CPS under which IdenTrust operates (covering all sections required to be covered by the ECA CP and that IdenTrust deems to be of interest to the Relying Parties (e.g., mechanisms to disseminate ECA trust anchor, to provide notification of revocation of ECA root or ECA Certificate) but omitting specific operational details that could weaken IdenTrust security posture.

CA Certificates and associated CRLs are available 24 hours a day, 7 days a week. IdenTrust ensures an availability of no lower than 99.5% a year with a scheduled downtime not exceeding 0.5% annually. This availability is accomplished by building and maintaining fully redundant components and architecture in its primary facility (see Section 5.1.1.1.1.) All information and processing travel through parallel paths throughout the system; failure of any component or path results in an instant switchover to the redundant component or path. In addition to the redundant architecture at the primary facility, IdenTrust maintains a secondary disaster recovery facility, which is geographically diverse (see Sections 5.1.1.1.2 and 5.1.6). The part of the Repository where the CA Certificate and CRLs are kept fails immediately to the secondary site to ensure that end users experience no impact as a result of a disaster for critical systems.

2.3 Time or Frequency of Publication

The public version of this CPS will be published after the EPMA has approved it and before IdenTrust issues any ECA Certificate. Amendments to the public version of the CPS will be published as specified in section 9.12.

The IdenTrust ECA will publish the chain of Certificates required to verify the authenticity of IdenTrust-issued ECA Certificates in the Repository before the IdenTrust ECA issues an ECA Certificate. The IdenTrust ECA will publish each ECA Certificate that it has issued to a Subscriber shortly after the Subscriber accepts it, but may discontinue its publication after it ceases to be valid.

The IdenTrust ECA publishes CRLs as specified in section 4.9.7.

2.4 Access Controls on Repositories

IdenTrust's Repository is protected by multiple layers of access control mechanisms designed to ensure that:

Persons acting without IdenTrust's authorization are not able to alter information in the Repository. IdenTrust provides the Repository to its users on a read-only basis only.

Persons and processes are unable to interfere with the reliable operation and online availability of the Repository.

Read access to the Repository does not require user authentication or login.

The published directory is a read-only replica of an original directory, which is not accessible from the Internet. That read-only replica is protected from modification by the layered security, firewalls, intrusion detection and OS-specific controls that are described in sections 6.5 and 6.7 for this and all other hosts. The unpublished original directory is accessible only to IdenTrust employees acting in Trusted Roles, and only via the local area network at IdenTrust's data center via Secure Shell ("SSH") and discretionary access control requiring individual identification and authentication for logins.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

ECA Certificates issued by IdenTrust identify the issuer (the IdenTrust ECA) and the Subscriber using distinguished names ("DN") as defined in ITU Recommendation X.500 and related standards. Certificate DNs conform to the format specified in the Certificate profiles in Section 10.

Full details of the attributes listed in those distinguished names, their data content, and their interpretation can be found in section 7.1.4 of this CPS. The format for a common name identified in an ECA Certificate used for personal authentication of Subscribers or encryption by a Subscriber is different from the common name identified in a Certificate used to secure communications from a component such as a web server that supports SSL.

ECA Certificates issued by IdenTrust also identify the Subscriber in the subjectAltName field (e.g. with an e-mail address for Individuals or a domain name for components).

3.1.2 Need for Names to be Meaningful

The identifiers in a Certificate for Subscriber and Issuer have the meaning specified in section 7.1.4. By interpreting an IdenTrust-issued ECA Certificate in light of the relevant Certificate profile, a Relying Party can infer the following, among other things, that:

The subject:commonName field lists the Individual Subscriber of the Certificate, together with the disambiguating number explained in section 3.1.5. In the case of a component Certificate, the subject:commonName field identifies the component by its fully qualified domain name. The content of the commonName field is readily understandable by humans. In the case of an individual, it is the individual's legal name, i.e. the name by which they are commonly known in business contexts.

A subject:organizationalUnitName lists the Subscribing Organization with which the Individual Subscriber is affiliated. Section 10 explains how to identify which of the several organizationalUnitName fields is the one for the Subscribing Organization. The affiliation between the Individual Subscriber and the Subscribing Organization can consist of any of the relationships specified in section 3.2.2.2 of this CPS.

A subjectAltName:rfc822name lists the Subscriber's e-mail address, *i.e.* the address at which the Subscriber can receive messages via SMTP, assuming the connectivity required for that protocol to function correctly.

A subjectAltName:otherName:userPrincipalName, depending on the specifics of the implementation, may list a Subscriber's unique identifier in the form "unique name@domain", where unique name is a unique identifier and the domain is in the form prescribed by [IETF RFC 822]

Section 10 specifies additional name fields and explains the above-listed names in greater detail.

IdenTrust retains discretion to refuse to issue Certificates listing names that may, in IdenTrust's opinion, be defamatory, indecent, illegal, or pejorative.

IdenTrust's naming practices operate within a name space prescribed by the EPMA (or its appointed naming authority) and are subject to the EPMA's oversight. The IdenTrust ECA only issues Certificates with subject names within the prescribed name space. The ECA is configured such that a Certificate outside of the prescribed name space cannot be issued. Where necessary, the IdenTrust operations personnel will coordinate with the EPMA to resolve naming issues for a particular Subscriber.

3.1.3 Anonymity or Pseudonymity of Subscribers

The IdenTrust ECA does not issue anonymous or pseudonymous Certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are listed in the Certificate profiles of Section 10. Those Certificate profiles are consistent with those prescribed by the EPMA and/or its naming authority; however, in the event of an inadvertent inconsistency, the name interpretations authorized by the EPMA take precedence.

Further information about naming conventions are found in the [ITU-T X.500] series of standards, as well as in [IETF RFC 2822] (formerly RFC 822, specifying the format of Internet e-mail messages), [IETF RFC 2616] (on HTTP). [IETF RFC 2253] explains how an X.500 distinguished name is represented in text, including most user interfaces.

3.1.5 Uniqueness of Names

In Certificates issued by IdenTrust, distinguished names in the issuer and subject fields are unique to the entity identified therein.

In the case of the issuer field, preventing ambiguity is simple: The EPMA assigns a name to IdenTrust which is unique among the ECA-approved CAs, and that name appears in the Certificate issued to IdenTrust by the ECA Root CA. Within the ECA PKI, the IdenTrust ECA issues no Certificates to any other Certification Authority so it determines no issuer names. Consequently, the only issuer distinguished name determined by IdenTrust is an exact match to the field already assured by the ECA Root CA to be unique in the ECA PKI.

The range of disambiguation required for Subscriber names is limited for the set of Certificates issued by IdenTrust. That range is referred to as the "IdenTrust name space" in this section. To ensure further that the subject: DistinguishedName is unique within the IdenTrust name space, the combination of the subject:CommonName and subject:Organization fields are used.

IdenTrust appends a disambiguating number after the colon character in the subject:CommonName field. The disambiguating number can be generated either by IdenTrust or provided by the Subscribing Organization.

When IdenTrust generates the number, it consists of three components:

(1) IP Address of the CA system (4 bytes);
(2) Current Date and time (8 bytes); and
(3) Sequence number (4 bytes).

The resulting value is expressed as a 32-digit hexadecimal number.

When the number is assigned by the Subscribing Organization, it consists of a unique identifier within the Subscribing Organization (8 to 20 digits). The resulting value is expressed as an 8 to 20-digit numeric string.

Together the Individual Subscriber's name in the subject:CommonName field, the disambiguating number and the subject:Organization field render a Subscriber distinguished name unique.

A Subscriber's disambiguating number is used as part of the subject:CommonName field for:

- Initial Signing and Encryption Certificates;
- All subsequent renewals of Signing and Encryption Certificates; and
- All subsequent rekeying of Signing and Encryption Certificates.

For IdenTrust-generated disambiguating numbers

If the Subscriber is no longer a holder of a valid IdenTrust ECA Certificate, and subsequently applies for new Certificates, IdenTrust generates a new disambiguating number for that Subscriber, even though the Subscriber had Certificates from IdenTrust with another disambiguating number in it. As a result, a Subscriber's disambiguating number does not persist to new Certificates issued to the Subscriber after revocation or expiration of the Subscriber's earlier Certificates. Consequently, the subject:CommonName field (combination of the name and the disambiguating number):

- Persists between a Subscriber's Signing and Encryption Certificates;
- Persists for all renewals of a Subscriber's Signing and Encryption Certificates;
- Persists for all rekeying of Signing and Encryption Certificates;
- Does NOT persist to Certificates issued after Revocation; and
- Does NOT persist to Certificates issued after Expiration.

For Subscribing Organization-generated disambiguating numbers

Because the Subscribing Organization unequivocally assigns unique identifiers to applicants and ensures that the numbers remain the same during the applicant's tenure in the Organization, the Subscriber's disambiguating number, based on the unique identifier, persists to new Certificates issued after revocation or expiration of the Subscriber's earlier Certificates. Consequently, the subject:CommonName field combined with the disambiguating number.

- Persists between a Subscriber's Signing and Encryption Certificates;
- Persists for all renewals of a Subscriber's Signing and Encryption Certificates;
- Persists for all rekeying of Signing and Encryption Certificates;
- Persists to Certificates issued after Revocation; and

- Persists to Certificates issued after Expiration.

3.1.6 Recognition, Authentication, and Role of Trademarks

IdenTrust does not perform trademark searches before issuing a Certificate. The information in Certificates issued by IdenTrust is supplied in large measure by the Subscriber and/or Subscribing Organization. By providing that information and/or approving issuance of a Certificate, the Subscribing Organization consents to the use of its trademarks in that Certificate.

However, some of the information included in a Certificate could give rise to trademark problems involving third parties. IdenTrust does not knowingly issue a Certificate that includes a name or other data that has been judicially determined to infringe another person's trademark. Moreover, in response to a complaint from a third party, IdenTrust will revoke a Certificate if that third party:

Presents proof that data in a Certificate issued by IdenTrust is a trademark that is registered by the US Patent and Trademark Office to an entity other than the Subscribing Organization listed in the Certificate; or

Proves to IdenTrust's reasonable satisfaction that another entity is widely known by the alleged trademark and confusion on the part of Relying Parties will likely result.

Before revoking, however, IdenTrust will confer with the Subscribing Organization to resolve doubt or confusion, if there is any in a given case. However, nothing in this CPS requires IdenTrust to obtain legal or expert opinion on a trademark issue, or to have such an issue adjudicated or otherwise decided by any forum.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

To Confirm that a prospective Subscriber holds the private key that corresponds to the public key to be included in an ECA Certificate the following steps are followed:

(1) An account password is submitted by the prospective Subscriber or the PKI Sponsor during a Server-authenticated SSL/TLS encrypted session at a secure site maintained by IdenTrust. (See definition of "Server-authenticated SSL/TLS" in Section 14: Glossary for more specifications).

(2) If the Certificate application is approved, an Activation Code is sent to the prospective Subscriber.

(3) The prospective Subscriber uses the Activation Code and account password to authenticate to the IdenTrust ECA. For a signature key, the applicant generates a Certificate request in the form prescribed by RSA PKCS #10.[8]

[8] For Component Certificates, the PKI Sponsor submits a base-64 encoded PKCS#10 during the first Server-authenticated SSL/TLS session (at step 1 instead of at step 3), as described in section 4.1.2.7.

(4) The IdenTrust ECA verifies the Individual Subscriber's digital signature on the RSA PKCS #10 Certificate request using the algorithm specified in the request and the public key included in the request.

(5) IdenTrust then issues the requested Signature Certificate, while the applicant is still online.

(6) An encryption key is generated by IdenTrust and delivered along with both Signing and Encryption Certificates during the same Server-authenticated SSL/TLS session as explained in sections 4.3.1 and 6.1.2. The applicant installs the Certificates and encryption key pair by downloading them into the applicant's Certificate store or Cryptographic Module.

These processes are described in further detail in section 4.1 below.

3.2.2 Authentication of Organization Identity

3.2.2.1 Confirmation of Organization's Existence

In applying for a Certificate, the Subscriber supplies the name of the Subscribing Organization to be listed in the Certificate, as well as that Organization's address and other payment and contact details.

IdenTrust[9] Confirms the existence and name of a Subscribing Organization in one of the following ways:

(1) A reference to a source unrelated to the prospective Subscribing Organization such as a secretary of state or other governmental registry, or a commercial database of business information such as Dun & Bradstreet.

(2) Presentation to IdenTrust of a copy of a governmentally issued[10] document attesting to the Subscribing Organization's legal existence, together with reasonable proof of the authenticity of that document. Secretaries of state in the United States generally issue "certificates of good standing" to the effect that the organization in question is in existence at the time the certificate is issued. Such a certificate is signed by an official representative of the secretary of state. Documents submitted for this purpose must be "fair on their face", *i.e.* bear no apparent indication of forgery, fraud, tampering, etc.

(3) 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.

[9] Although confirmation of an Individual Subscriber's identification is often performed by Trusted Correspondents rather than IdenTrust, ordinarily IdenTrust itself confirms the corporate identity of a prospective Subscribing Organization. Often IdenTrust performs this confirmation when concluding a contract for public key Certificate issuance and revocation services with that Subscribing Organization.

[10] The document specified in the main text must be from the government entity which incorporated the company. A tax identifier (such as a federal employer identification number), a tax return, and any other document that assumes valid incorporation is not acceptable unless proof from the incorporating entity is not obtainable within a reasonable time.

(4) IdenTrust may independently obtain (without reference to the data provided by the Applicant for a Certificate) the name, address and telephone number of the organization, which are confirmed by a telephone call with a representative of the organization made to the telephone number independently obtained by IdenTrust.

The name appearing in the reference or document confirming existence must match the name of the Subscribing Organization to be listed in the Certificate. As illustrated in Figure 1, the IdenTrust RA Operator Confirms the existence of the Subscribing Organization and establishes a parent account for that organization in the Subscriber Database before issuing the first Certificate listing that Organization in the Certificate's subject field.

Establishment of a Parent Account for a Subscribing Organization

IdenTrust reconfirms an organization's existence based on the ongoing business relationship between IdenTrust and the Subscribing Organization which is maintained through correspondence or a payment stream and maintenance of a bank account.

3.2.2.2 Authentication of the Individual-Organization Affiliation

IdenTrust does not issue ECA Certificates to Individual Subscribers having no organizational affiliation or who are acting in a personal capacity and not a professional capacity. See section 1.3.3. However, the organization need not be incorporated, but it must conduct business. An organization must not be an individual acting as a consumer in a personal capacity. An individual acting in a business capacity as a sole proprietor, professional consultant, or fictitious entity (e.g., "dba" as allowed by local law), may be considered "the organization" for the purposes of the OU attribute in the subject field of the Certificate. If the Subscriber is located outside the United States, IdenTrust may impose, through the Subscriber Agreement, additional restrictions in view of other jurisdictions' laws governing privacy, consumer protection, and other rights of individuals. For example, if an individual is located within the European Community, the Subscriber Agreement may contain an additional attestation from the individual that the information provided shall be considered business data rather than personal data under European Directive 95/46/EC and/or that the individual gives his/her unambiguous consent to the processing of such data by IdenTrust.

The affiliation between the Individual Subscriber and the Subscribing Organization is one, in which the Individual Subscriber is an employee, member or officer of, partner in, or is otherwise affiliated with the Subscribing Organization. Because it is the Individual Subscriber that holds the private key, any verifiable digital signature created by that private key is attributable to the Individual Subscriber. Whether that digital signature can be relied on to bind the Subscribing Organization in a given transaction depends on whether the Individual Subscriber has authority to sign for the Subscribing Organization in the transaction in question. That authority cannot be inferred from an ECA Certificate issued by IdenTrust. IdenTrust does not issue Certificates that assert roles or authorizations.

In other words, IdenTrust's ECA Certificates do not imply any grant of authority by the Subscribing Organization to the Individual Subscriber to act on behalf of the Subscribing Organization in any given transaction. A Relying Party can infer from verification of a digital signature by reference to a valid ECA Certificate issued by IdenTrust that a digital signature is attributable to the Individual Subscriber listed in that Certificate. A Relying Party cannot, however, infer from an ECA Certificate that the Individual Subscriber has the authority to act on behalf of the affiliated Subscribing Organization in a given transaction; instead, the Relying Party would need to refer to the applicable laws relating to agency as well as non-certificate information (e.g. contractual arrangements between Subscribing Organization and Relying Party separate and independent of any relationship under the CP and CPS and documents contemplated thereunder) to make its determination as to whether the Individual Subscriber has authority to act on behalf of the Subscribing Organization in relation to the given transaction.

Although an ECA Certificate issued by IdenTrust does not permit attribution of a digital signature to the Subscribing Organization listed in that Certificate, IdenTrust does not issue a Certificate to an Individual Subscriber without first obtaining both of the following with respect to the Certificate to be issued:

The approval of the Subscribing Organization with which that Individual Subscriber is affiliated. The approval enables the Subscribing Organization to manage its internal PKI and infrastructure but it is not in itself a grant of any authority. In its contract with IdenTrust, the Subscribing Organization authorizes one or more persons to give this approval.

Confirmation of the existence of affiliation between the Subscribing Organization and the Individual Subscriber. This consists of confirmation of employment. IdenTrust Confirms this affiliation through a third party within the Subscribing Organization, usually through the Trusted Internal Correspondent where such exists. Otherwise, IdenTrust initiates communication with the Subscribing Organization using an independently verified point of contact, i.e. IdenTrust obtains telephone numbers for the Subscribing Organization from a trusted, independent third-party source of such information, such as Dun & Bradstreet or Lexis-Nexis. The third party may be the Human Resources department or any individual in a capacity within the Subscribing Organization to Confirm the affiliation.

IdenTrust records performance of this confirmation in an auditable log.

3.2.2.3 Authentication of Component-Organization Relation

As detailed in section 7.1.4.1 and Section 10, Component Certificates list the component in the subject:CommonName field and the Subscribing Organization in a subject:OrganizationUnitName. In effect, then, the Certificate asserts a relation between the Component and the Subscribing Organization. That relation can consist of any of the following:

Ownership or possession: The Subscribing Organization owns or possesses the Component identified in subject:CommonName.

Operation: The Subscribing Organization operates the Component or has outsourced its operation to a service provider on a hosted or outsourced basis, and that service provider operates the Component for the Subscribing Organization.

IdenTrust Confirms that relation between the Subscribing Organization and the Component by matching information found in databases of third-party organizations dedicated to the registration of Component names (i.e., domain name registrars) and the information provided during the application process, which includes an authorization letter to IdenTrust from the Subscribing Organization on its letterhead. In cases that the Component common name is not recorded in databases external to the Subscribing Organization, an authenticated digitally signed email or a form letter on letterhead from the Subscribing Organization signed by a Trusted Correspondent (preferably by a Trusted Internal Correspondent) or counter-signed by a notary may be used.

3.2.3 Authentication of Individual Identity

Before the IdenTrust ECA issues a Certificate, the identification of the Individual Subscriber of that Certificate must be confirmed by a Registrar as prescribed in this section.

3.2.3.1 In-Person Authentication

IdenTrust requires confirmation of a Subscriber's identification through appearance in-person before a Registrar within the 30 days prior to the application of the CA's signature to the Subscriber's Certificate (except when re-issuing a Certificate within the time limits set forth in section 3.2.3.2). Additional details related to the enforcement of this 30-day requirement and processing of Certificate applications may be found below in section 4.3.1.

3.2.3.1.1 Who May be a Registrar

IdenTrust uses the term "Registrar" to mean the person performing the in-person confirmation of the Subscriber's identification. Who may be the Registrar varies depending on whether the Certificate is a Medium Hardware Assurance Certificate, Medium Token Assurance, or a Medium-Assurance Certificate without the corresponding private key being kept in a hardware Cryptographic Module:

For a Medium Hardware Assurance Certificate, IdenTrust requires that the Registrar before whom the Subscriber appears must be either (1) a Trusted Correspondent or (2) an employee performing the Trusted Correspondent role or an RA Operator, provided that the employee would not be precluded from acting as Registrar by the Separation of Role requirements of section 5.2.4. A notary may not act as Registrar for this type of Certificate (unless they are also a Trusted Correspondent).

For a Medium Token Assurance Certificate, the Registrar may be any of the individuals permitted to act as Registrar for a Medium Assurance or a Medium Hardware Assurance Certificate.

For a Medium-Assurance (non-hardware) Certificate, the Registrar may be any of the individuals permitted to act as Registrar for a Medium Hardware Assurance Certificate. The Registrar may also be a notary commissioned or otherwise permitted to practice in

the jurisdiction in which the in-person appearance occurs. Moreover, in some cases, citizens of countries other than the United States and residing in the country of citizenship, a United States embassy or consular officer may act much as the notary. Trusted Correspondents in accordance with Section 3.2.3 of this CPS or authorized DOD employees in accordance with Section 11 of the ECA CP may Confirm non-U.S. citizens who are not citizens of Australia, Canada, New Zealand, or the United Kingdom (these applicants must be located in the U.S. when confirmed).

In any case, whichever type of Registrar is appropriate; the IdenTrust RA Operator approves issuance of the Certificate only after receiving documentation demonstrating that an appearance in person before the required Registrar took place within the 30 days preceding issuance.

Unless otherwise agreed in advance, IdenTrust does not reimburse a Subscriber for any notarial or other fees incurred for the services of the Registrar.

3.2.3.1.2 In-Person Registration Procedure

All of the operations described in this section must be completed before the Certificate can be issued for use.

The prospective Individual Subscriber must appear in person before the Registrar required in the foregoing subsection. The Subscriber must:

(1) **Present two official identification documents** issued by governmental authorities having the jurisdiction to issue such documents. At least one of the documents must include a photograph of the prospective Individual Subscriber such as a state-issued driver's license, U.S. federal government employee picture identification card or passport. The documents must support not only identification of the prospective Individual Subscriber but also must enable the Registrar to Confirm the prospective Individual Subscriber's residency and citizenship. For U.S. citizenship, only the following credentials may be accepted:

- U.S. Passport;
- Certified birth certificate issued by the city, county, or state of birth[11], in accordance with applicable local law;
- Naturalization certificate issued by a court of competent jurisdiction prior to October 1, 1991, or the U.S. Citizenship and Immigration Service (USCIS), formerly the Immigration and Naturalization Service (INS), since that date;
- Certificate of Citizenship issued by USCIS;
- Department of State Form FS-240 – Consular Report of Birth; or
- Department of State Form DS-1350 – Certification of Report of Birth.

[11] A certified birth certificate has a Registrar's raised, embossed, impressed or multicolored seal, Registrar's signature, and the date the certificate was filed with the Registrar's office, which must be within 1 year of birth. A delayed birth certificate filed more than one year after birth is acceptable if it lists the documentation used to create it and is signed by the attending physician or midwife, or lists an affidavit signed by the parents, or shows early public records.

For citizenship verification of non-US citizens, the applicant must present passport(s) issued by the country(ies) of citizenship.

Procedures and requirements for identity verification of US citizens in foreign countries and non-US citizens whether in the US or in a foreign country are fully detailed in Section 11 of this CPS.

(2) **Sign an In-Person Identification Form**.[12] Section 4.1 describes the Certificate application process in detail. The prospective Individual Subscriber must sign the In-Person Identification Form in the presence of the appropriate Registrar. The In-Person Identification Form records the identification of the Individual Subscriber and his or her acceptance of the responsibilities of a Subscriber in relation to the Certificate to be issued, including the responsibility to provide accurate information. The prospective Subscriber's signature must be in ink. By signing, the Individual Subscriber attests to the accuracy of the information on the form. After signing, the Individual Subscriber gives the original, signed In-Person Identification Form to the Registrar for identity confirmation and endorsement under subsection (3) below.

(3) **The accuracy of the identifying information provided in the ID form is confirmed** as indicated in this section. Unless otherwise provided below, these tasks are completed in the presence of the prospective Individual Subscriber.

(a) **Registrar examines the official identification documents** provided by the Individual Subscriber. Those documents must be free of any apparent defect on their face; and, at least one of them must be within their validity period as of the date that the in-person identification is performed. The photograph must be a likeness of the prospective Individual Subscriber. The documents must also be without obvious inconsistencies with each other and with the ID form, unless the prospective Individual Subscriber has a reasonable explanation for inconsistencies (such as intervening name change, change of address, etc.). In cases of doubt, the Registrar has discretion to require additional documentation of identification, or to check company records or other available sources of information.

(b) **When Subscribing Organization-generated disambiguating numbers are used, the Registrar positively matches the Individual Subscriber to his/her internal unique identifier** documented in the ID form, using the applicable Subscribing Organization's databases or documents (e.g., work badge)[13]

[12] This form is available online at http://www.identrust.com/certificates/eca/eca_downloads.html.

[13] As employees for the Subscribing Organization, Trusted Internal Correspondents have access to Subscribing Organization databases and training that allows them to accurately confirm the match. When a Trusted Internal Correspondent is not available, Trusted External Correspondents, trusted employees of IdenTrust or IdenTrust RA Operators may be granted authorization to access the same databases and training for its use.

(c) **Registrar endorses and dates the ID form** if sufficient documentation meeting the requirements of subsection (1) is on hand and, when necessary, the unique identifier has been matched to the Individual Subscriber.

In confirming the identification of a prospective Individual Subscriber, the Trusted Correspondent or RA Operator has discretion to do any or all of the following:

- Require additional information or evidence from the prospective Subscriber before approving issuance of the Certificate.
- Delay issuance of the Certificate to obtain additional information, consult with a supervisor, legal counsel, or a risk manager, or for any other reason. The reason need not be explained to the prospective Subscriber.
- Decline to proceed with the registration of a specific Individual Subscriber, with or without giving a reason.

In all cases, the Trusted Correspondent or RA Operator must exercise that discretion in a way that does not discriminate in an illegal way or violate the ECA CP or this CPS, laws or rules governing privacy and confidentiality, and similar constraints. The Trusted Correspondent or RA Operator must also document all actions taken in the exercise of the above discretion.

The foregoing confirmation procedures are in addition to the other tasks described in section 4.3.1 for processing of a Certificate application.

Email verification is also required and it can be done one of two ways; electronically and manually through a list submitted by a Trusted Correspondent.

Electronic Verification of Email: When a Subscriber submits an application through a secure online form, an automated email is sent to the email address provided. Within that automated email message there are two components with instructions on how to use them for the verification process; a link to a Server-authenticated SSL/TLS secured web site and a numerical code. Once the Subscriber selects the link they will be redirected to an IdenTrust page that requires the numerical code and the Subscriber generated account password.). The numerical code requested is specific to the Subscriber and unique for each application submission and the account password was created by the Subscriber within the application. When the Subscriber provides and submits the numerical code and the account password accurately, the email provided during the application phase will be updated automatically within the account as verified.

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

All ECA Certificate applications require verification of the email address on the application. If the email verification is not completed the application will not be approved.

If the Trusted Correspondent or RA Operator Confirms the identity and if other requirements of section 4.1.2 are satisfied, then the request for a Certificate may be approved; see sections 4.2 and 4.3. That approval takes the form of a handwritten endorsement of the application or may be a digitally signed input into the Certificate issuance process, (submitted as a digitally signed document or XML data structure by the Trusted Correspondent, or in the case of IdenTrust acting as RA, the RA Operator's approval of issuance communicated over client-authenticated SSL/TLS to the CA system). In either event, the Trusted Correspondent or RA Operator documents the confirmation process in a form capable of being archived as required in section 5.5.

A prospective Subscriber that is a minor or not competent to perform face-to-face registration alone shall be accompanied by a person already certified by IdenTrust's ECA, who will present information sufficient for registration at the level of the Certificate being requested, for both himself and the person accompanied.

3.2.3.2 Electronic Authentication of Individuals

The identification of an Individual Subscriber for certain re-key and Certificate renewal events may be based on a request authenticated by the prospective Individual Subscriber's digital signature described in section 3.3.1 if the following are all true:

(1) **Signature verification**: IdenTrust can verify the Individual Subscriber's digital signature by reference to a valid ECA Certificate issued by IdenTrust and having an assurance level equal to the Certificate to be issued for the Individual Subscriber. This is accomplished by an automatic check of the Certificate against the configuration of that Certificate type within the Subscriber Database.

(2) **In-person identification not required**: The Individual Subscriber is not due for another in-person identification. Each Individual Subscriber must be re-identified by a Registrar satisfying the requirements of section 3.2.3.1.1 and following the procedure specified in section 3.2.3.1.2 at least once within the time periods listed below:

Every nine years in the case of an Individual Subscriber who does not hold a private key associated with a Medium Hardware Assurance Certificate. In addition, a Certificate may be issued based on a digitally authenticated request. In other words, for Medium Assurance and Medium Token Assurance Certificates an Individual Subscriber may be digitally authenticated for Certificate renewal events for the period of nine years between in-person identity proofing events.

Every three years in the case of an Individual Subscriber of a Medium Hardware Assurance Certificate.

To ensure that the validity period of a Certificate issued on the basis of an electronic authentication does not extend beyond the in-person identification limits stated above, the IdenTrust ECA system does the following:

- counts the number of digitally authenticated issuances since the last in-person identification;
- compares the date of the Subscriber's last in-person identification stored in the Subscriber Database to ensure that the Certificate's proposed validity period will not extend beyond the next in-person identity proofing deadline; and
- sends the Subscriber re-key notification e-mails with instructions to appear in-person before a Registrar for identity proofing beginning 90 days prior to Certificate expiration.

(3) **Information from Authentication Certificate Remains Unchanged:** IdenTrust will issue a new Certificate containing the same (i) Subject Distinguished Name, (ii) Certificate Policy OID, (iii) Subject Alternative Names, and (iv) CountryOfCitizenship (whenever that subfield of the SubjectDirectoryAttributes field is present).

3.2.3.3 Authentication of Component Identities

Component Certificates identify a device rather than an individual. The component is identified in the subject:CommonName field in the manner specified in section 7.1.4.1. Component Certificates also list the name of the Subscribing Organization associated with the device; see section 3.2.2.3.

The components identified in Component Certificates are operated or controlled by an individual in the role of PKI Sponsor, who performs the functions of a Subscriber for the Component Certificate that the Component itself cannot perform. In particular, before a Component Certificate can be issued, the PKI Sponsor must be authenticated by IdenTrust according to the procedure specified in section 3.2.3.1.1 and provide to IdenTrust or a Trusted Correspondent correct information including the following:

Identification of the component, including all identifiers for the Component to be listed in the Certificate to be issued;

The public key to be listed in the Certificate to be issued;

Contact information to enable the IdenTrust and/or the Trusted Correspondent to communicate with the PKI Sponsor when required.

IdenTrust Confirms the accuracy of the information using the following steps:

Digitally signed statements by the PKI Sponsor (who must already be a Subscriber authenticated according to procedure specified in 3.2.3.1). IdenTrust verifies the digital signatures on the statements of the PKI Sponsor using the PKI Sponsor's Valid Certificate, which must be an IdenTrust-issued Certificate of equal or greater assurance than the Certificate requested for the Component.

Confirmation of Authorization. The PKI Sponsor is required to establish authorization to obtain a Component Certificate by submitting an Authorization Agreement signed by a representative of the Sponsoring Organization. Contact information for confirming

authorization (address and telephone number of Organization) is independently obtained from IdenTrust records or a third-party database. IdenTrust contacts the registered domain administrator, human resource manager, or the authorizing official listed in the Subscribing Organization's contract with IdenTrust to ensure that the PKI Sponsor is authorized to request a Certificate for the Component.

In the event that a PKI Sponsor is replaced, the new PKI Sponsor is required to establish authorization to manage the specific Certificate(s) by submitting a new Authorization Agreement. The new PKI Sponsor may provide the Authorization Agreement proactively at any time. Alternatively, IdenTrust will request a new Authorization Agreement during re-key and revocation lifecycle events when requested by a different PKI Sponsor.

Verification of Ownership. If a registered Domain Name or IP address is to be used in the Certificate, a WHOIS check and/or a reverse lookup is performed to Confirm that the Sponsoring Organization owns or controls the Domain Name or IP address. If the Certificate will identify a particular Component name, that name is also confirmed with the Sponsoring Organization.

Verification of Request. IdenTrust calls the PKI Sponsor via telephone at a number obtained independently from the Organization to verify that the PKI Sponsor requested a Certificate and to verify the details provided by the PKI Sponsor when he or she applied for the Component Certificate.

IdenTrust may also request additional information in the form of a signed letter printed on letterhead of the Sponsoring Organization that attests to accuracy of the additionally requested information. Component Certificates issued by IdenTrust do not contain equipment authorizations and attributes.

3.2.4 Non-Verified Subscriber Information

Certificates do not contain information that is not verified.

3.2.5 Validation of Authority

Certificates issued to Subscribers do not assert authority to act on behalf of the organization in an implied capacity.

3.2.6 Criteria for Interoperation

Decisions to interoperate with other PKIs are within the purview of the EPMA.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Whenever a Certificate is issued based on confirmation performed for an earlier Certificate, the limits specified in section 3.2.3.2 apply. Thus, the *not After* date field in a

Certificate may not go beyond the next in-person identity proofing date. This is restricted by ECA system as explained above in section 3.2.3.2.

During re-keying, renewing or updating, the Subscriber must present his or her currently valid IdenTrust-issued ECA Certificate to establish a Client-authenticated SSL/TLS-encrypted session. IdenTrust's ECA validates the authenticity of the Certificate presented by verifying that the Certificate was issued by the IdenTrust ECA, that the Certificate is still valid in the relational database, and by comparing the subject name in the Certificate with the subject name in the Subscriber Database. (See definition of "Client-authenticated SSL/TLS in Section 14: Glossary.) If confirmation of a new Certificate is based on a digital signature, section 3.2.3.2 requires that that digital signature be verifiable by a valid ECA Certificate issued by IdenTrust with an assurance level equal to the Certificate to be issued. This is accomplished by an automatic check of the Certificate against the configuration of that Certificate type within the Subscriber Database.

3.3.2 Identification and Authentication for Re-Key After Revocation

If confirmation of a new Certificate is based on a digital signature, section 3.2.3.2 requires that that digital signature be verifiable by reference to valid ECA Certificate issued by IdenTrust and having an assurance level equal to the Certificate to be issued for the Individual Subscriber. Consequently, confirmation for a new Certificate must not be based on a revoked Certificate. Requests for Certificate Issuance made with a revoked Certificate will not be honored. In such a case, the Requestor must apply for a new Certificate in accordance with the procedures outlined for initial issuance through in-person identification and authentication in section 3.2.3.1.

3.4 Identification and Authentication for Revocation Request

As provided in the ECA CP, requests to revoke an ECA Certificate that IdenTrust has issued must be authenticated; see sections 3.4 and 4.9 of the CP and section 4.9.3 of this CPS. Requests to revoke a Certificate may be authenticated by verifying a digital signature using the Certificate to be revoked.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

A person who agrees to the terms and conditions of the applicable Subscriber Agreement may submit a Certificate application. Portions of the application may be submitted to IdenTrust by a Trusted Correspondent acting on behalf of the applicant.

4.1.2 Enrollment Process and Responsibilities

Applicant registrations for IdenTrust-issued Signing and Encryption Certificates are initiated through a Web interface on IdenTrust's World Wide Web site (i.e. IdenTrust's ECA Certificate Center); or through a bulk loading process as described in section 4.1.3. Registration is followed by in-person confirmation of identity later during the Certificate application process. Registrations for IdenTrust-issued Component Certificates are initiated only through a Web interface on IdenTrust's World Wide Web site.

In both the online registration process and in the bulk loading process a parent account for the Subscribing Organization must be established. Once a parent account has been created for the Subscribing Organization, the Subscriber's account can be associated with it by reference to the physical address of the Organization's primary business offices and using the domain name listed in the parent account (e.g. via a Subscriber's e-mail address).

4.1.2.1 Information Collection

During the application phase of registration, applicant information is collected in one of the following manners:

- Individual applicants can provide registration information via an online Certificate application process over a Server-authenticated SSL/TLS secured web site hosted by IdenTrust. This is described in section 4.1.2.7 (Process Overview).
- Individual applicants can provide registration information to a Trusted Correspondent, who will forward the information to IdenTrust via the bulk loading process described in section 4.1.3 (Enrollment Process / Bulk Loading by Trusted Correspondents).
- PKI Sponsors can provide registration information via an online Certificate application process over a Server-authenticated SSL/TLS secured web site hosted by IdenTrust (Certificate Application and Issuance Process for a Component Certificate).

All applicants (PKI Sponsor is the applicant for Component Certificates) must provide the following information:

For all Certificates (Signing, Encryption, and Component)

- Applicant Name,
- Subscribing Organization Information, including Name, Entity Type (For-profit corporation, non-profit, government, partnership, LLC, sole proprietorship, etc.), Address (including country), and the name of the jurisdiction under whose law the entity has been organized (i.e. state of incorporation *e.g.* Delaware),
- Applicant's Job Title,
- Applicant's E-mail Address,
- Applicant's Phone Number,
- An account password (see below additional details); and
- Payment information such as credit card details, purchase order number or voucher number.
- When, applicable, an external disambiguating number (see below for additional details).

Only for Signing and Encryption Certificates

- Applicant's Citizenship(s),
- Governmentally issued identifying number for the Applicant such as passport number, social security number, etc.,
- Reason or basis for requesting the Certificate,
- Point of contact for confirmation of information provided; and
- Photo ID number and type as required by section 3.2.3.

Only for Component Certificates

- Server name, and
- RSA PKCS#10 Certificate Signing Request ("CSR").

An account password[14] selected by the applicant and consisting of at least 8 characters, which will be utilized for user authentication along with an Activation Code provided to the Applicant (for use during Certificate retrieval). As part of the registration process, the applicant is required to create three questions and secret answers, which together serve as a mechanism to reset their account password in case they forget it before they are able to download their Certificate. This process is activated by the Subscriber providing his or her Activation Code, which was received initially in a letter when the account was first opened and by clicking on an account password reset URL. This process sends a One-Time-Code (OTC) and specified URL to the e-mail address on file for the Subscriber. After receiving the e-mail, the Subscriber must enter both the Activation Code and the OTC at the specified URL in order to gain access to the three questions that were selected during registration. (The three questions were selected by the Subscriber from a list of ten randomly selected questions that were randomly generated from a pool of password-

[14] This account password is separate from—and should not be confused with—the password required by Section 6.4.1 of the ECA CP and this CPS for protection of a private key stored in a FIPS 140-evaluated Cryptographic Modules. See also section 3.2.1 *above*.

reset questions.) If the answers are correct, the Subscriber is allowed to change the account password, which is immediately hashed and stored in the CA system for further use.

An external disambiguating number assigned by the Subscribing Organization and provided to IdenTrust by the applicant consists of 8 to 20 numbers. Disambiguating numbers are based on Subscribing Organization unique identifiers that: (1) remain unchanged during the applicant's tenure; (2) are decommissioned or made inactive when the applicant is no longer affiliated with the Organization; and, (3) are never re-used by the Subscribing Organization with a different applicant. Prior to accepting unique identifiers from a Subscribing Organization, IdenTrust obtains acknowledgment that the Subscribing Organization complies with the three requirements above. As part of the registration process, the tie between the applicant and the disambiguating number will be confirmed by the Registrar. The IdenTrust system will also automatically compare a new disambiguating number against all accounts in the Subscribing Organization to ensure the number is used for only one Subscriber. IdenTrust also checks that the Organization assigned number with leading zeros added does not match any number assigned by IdenTrust to the Organization.

4.1.2.2 Documents Provided to Applicants

Following submission of the registration information and acceptance of the online Subscriber Agreement[15], the applicant is provided with the Subscribing Organization Authorization Agreement (the "Authorization Agreement") and In-Person Identification Form ("ID Form").

Applicants are instructed to take the ID Form to a Registrar (defined in section 3.2.3.1.1 as either a Notary or a Trusted Correspondent). The applicant will present the completed ID Form and necessary credentials to a Registrar as required by section 3.2.3.1.2. The ID Form contains documentation including a Subscriber acknowledgement, Registrar instructions, and boxes or lines for the Registrar to initial or fill in when verifying the accuracy of the identifying information presented.

4.1.2.3 Verification of Identity In-person by Notary/Trusted Correspondent using the ID Form

The applicant signs the ID Form in the presence of the Notary or Trusted Correspondent. The Notary or Trusted Correspondent performs the following:

Records the type, serial numbers and expiration dates for the identification documents presented by the applicant.

Verifies that the identification document is protected against forgery, modification, or substitution (e.g., holograms and other security features), and that the applicant is the

[15] In addition to the online acceptance of the Subscriber Agreement, all applicants provide traditional ink signatures on the application documentation submitted, indicating acceptance of the Subscriber Agreement and the responsibilities associated with being a Subscriber under the ECA CP and this CPS.

holder of the identification documents presented and that the picture and name on the Photo ID match the appearance and name of the Applicant.

Signs (or notarizes if the Registrar is a notary) the ID Form.

In accordance with Section 3.2.3 of the ECA CP and upon completion of the in-person identity confirmation before the Notary or Trusted Correspondent, the applicant's ID Form will contain (1) a record of the identity of the Registrar; (2) a signed declaration by the Registrar that he/she confirmed the identity of the Subscriber; (3) a record of the method used to Confirm the individual's identity (e.g. ID type and number); and (4) a record of the date of the in-person identity confirmation.

4.1.2.4 Submission of Authorization Agreement and ID Form

The Authorization Agreement required for each applicant must be executed by an officer of the applicant's Subscribing Organization with the authority to bind the Subscribing Organization to its terms. The level of authorization can be gauged based on the officer's job title, function, or other grounds for concluding that authorization is apparent. In doubtful cases or where the law of the Subscribing Organization's jurisdiction does not recognize apparent authority, a power of attorney may be required.

The information collected from the applicant, the ID Form and the Authorization Agreement are submitted to IdenTrust's Registration Department. The ID Form may be submitted to IdenTrust in two ways: (1) Directly by the applicant, or (2) Through a Trusted Correspondent. The ID Form may only be submitted as an original on paper. However, the Authorization Agreement may be digitally signed and submitted via e-mail. In the case in which the Registrar is a notary or consular officer, the applicant may submit all the application information directly to IdenTrust. In the case in which the Registrar is a Trusted Correspondent, the Trusted Correspondent will submit the information to IdenTrust in a mail package containing the original paper document.

4.1.2.5 Review of Documentation by RA Operator

IdenTrust's RA Operator will: (i) review the information submitted to assess the adequacy and recency of the in-person identity confirmation, (ii) populate the in-person identification date field in the Subscriber Database with the date on which in-person identity confirmation was performed (to prevent Certificate issuance in the event that more than 30 days transpire between in-person identification and the attempt to retrieve the Certificate), (iii) review the Authorization Agreement for organizational affiliation, and (iv) verify the signature of the Registrar who performed the in-person identity confirmation in accordance with section 3.2.3.1. Confirmation of a Trusted Correspondent's signature will consist of a visual confirmation of the Trusted Correspondent's manual signature on the in-person identification form. Confirmation of a notary's or consular officer's signature will consist of reasonably assuring the validity of the notary's or consular officer's seal or stamp and signature. The signature verification and revocation checking capabilities of a PDF program will be used to verify the digital signatures on Authorization Agreements that are submitted electronically.

4.1.2.6 Delivery of Activation Code and Retrieval Kit

If the application is approved, the applicant is notified and the IdenTrust RA Operator sends the applicant—via email, mail or courier—a 10-digit long, randomly generated, not previously used number[16] ("Activation Code") and instructions needed to generate and retrieve either a Medium Assurance Certificate, Medium Token Assurance Certificate, or a Medium Hardware Assurance Certificate. A retrieval kit may be sent that includes a Cryptographic Module containing unique identifier (e.g., the manufacturer serial number) that is recorded in the Subscriber Database and, optionally, the Activation Code mentioned above. Cryptographic Modules are sent via a courier delivery method that allows tracking and confirmation of delivery to the applicant (e.g., US certified mail, UPS, or similar). The retrieval phase begins once the applicant has received his or her retrieval kit enabling him or her to generate keys and obtain a Certificate. The processes for key generation, public key submission and Certificate retrieval are explained in sections 3.2.1, 4.1.2.7, and 4.3.1.

4.1.2.7 Process Overview

This section presents two processes, one for Signing and Encryption Certificates and one for Component Certificates. Each process is listed in a numerical list below.

The first process includes the standard steps that are required for Signing and Encryption Certificate application and retrieval. This section does not describe the bulk-load registration process performed by a Trusted Correspondent, which is described in section 4.1.3.

In-Person Registration:

1. The Applicant accesses the secure (https://) web site[17]
2. The Applicant fills out the online secure registration form.
3. An Account Record is created.
4. The Applicant prints the ID Form and Authorization Agreement (see section 4.1.2.2 above).

Identity Proofing:

5. The Applicant personally appears before a Registrar.

[16] The Activation Code is a 10-digit number generated using a 48-bit seed, which is modified using a linear congruential formula. This number is compared against all previous numbers to ensure it has not previously generated. If the number has previously been used, the process is repeated until a number is created that has not been generated.

[17] The applicant's SSL-enabled client software confirms the identity of the IdenTrust secure server by reference to a Certificate issued by an IdenTrust CA that is listed in the client software's list of trusted, high assurance Root Certificates (e.g., IdenTrust Commercial Root CA), which are embedded in the most widely distributed commercial browsers. The client software checks the validity of the secure server's Certificate according to SSL protocols (e.g. whether Certificate subject name matches server name being used) and negotiates a session key to be used for encryption.

6. The Applicant signs ID Form in presence of the Registrar (see section 4.1.2.3 above).

7. The Registrar authenticates applicant and signs the form.

8. A representative of the Subscribing Organization signs the Authorization Agreement (see section 4.1.2.4 above).

9. If the Registrar is a Notary, Applicant submits ID Form and Authorization Agreement to IdenTrust, or if the Registrar is a Trusted Correspondent, then the Applicant may submit the ID Form and Authorization Agreement to the Trusted Correspondent who then submits them to IdenTrust.

10. IdenTrust RA Operator Confirms the Trusted Correspondent's manual signature, authority and active status, or reasonably assures the validity of the notary seal and signature, and reviews the ID Form and Authorization Agreement submitted to determine compliance with sections 3.2 and 4.1 (see section 4.1.2.5 above). If an application is rejected, the applicant is sent a letter explaining the reasons why.

Certificate Issuance:

11. IdenTrust generates an Activation Code and delivers it to the applicant in accordance with section 4.1.2.6 above.

12. The applicant enters the account password and Activation Code at a secure IdenTrust retrieval web site (https://).

13. During that same secure SSL/TLS-encrypted session, the applicant's Cryptographic Module generates a key pair for the Signing Certificate, sends a PKCS #10 to IdenTrust, and IdenTrust verifies that the public and private keys correspond to each other using the PKCS#10, then the IdenTrust ECA issues and downloads the Signing Certificate to the applicant. (See section 6.1.2 for an explanation of the processes used to generate and deliver the encryption key pair and Certificate to the Subscriber.)

14. IdenTrust's secure web site prompts the applicant to install the IdenTrust ECA Certificate, and the Root ECA Certificate within the Subscriber's key store (browser or hardware).

15. Upon review and acceptance of the Certificate by the Subscriber, IdenTrust publishes the Certificate to its Repository.

Below the second process overview includes steps required for Component Certificate application and retrieval:

In-Person Registration:

1. The Applicant accesses the secure (https://) web site.

2. The Applicant/PKI Sponsor fills out the information for the PKI Sponsor and Component, provides a RSA PKCS#10 Certificate signing request, and an account password on the online form (see section 4.1.2.1 above).

3. An Account Record is created.

Identity Proofing:

4. The IdenTrust RA Operator Confirms the information submitted in the application to determine compliance with sections 3.2.2 and 3.2.3. This check includes identity proofing of the PKI Sponsor and the device. The PKI Sponsor is verified in accordance with section 3.2.3.1.2, and the device is verified in accordance with section 3.2.3.3. If an application is rejected, the applicant is sent a letter explaining the reasons why.

Certificate Issuance:

5. IdenTrust generates an Activation Code and delivers it to the applicant in accordance with section 4.1.2.6 above.

6. The applicant enters the account password and Activation Code at a secure IdenTrust retrieval web site (https://).

7. During the server-authenticated session, IdenTrust issues the Certificate, publishes it in the Repository, and delivers a PKCS#7 to the PKI Sponsor for installation in the server.

4.1.3 Enrollment Process / Bulk Loading by Trusted Correspondents

Each Trusted Correspondent (or, in the case of a Trusted Internal Correspondent, their employing Subscribing Organization) must enter into an agreement with IdenTrust pursuant to which he or she is obligated to Confirm and communicate Subscriber identity information to IdenTrust, as described in section 1.3.2.1 above. IdenTrust registers a Medium Token Assurance Certificate or Medium Hardware Assurance Certificate to each Trusted Correspondent for authentication of his or her digital signature upon communications to IdenTrust regarding applicants and Subscribers. (The issuance process for this Certificate follows the normal procedures for Certificate issuance of such Certificates—with the understanding that Medium Hardware Assurance Certificates may only be approved by Trusted Correspondents who hold Medium Hardware Assurance Certificates—i.e., using an assurance level commensurate with the Certificate level being requested which is checked manually by an RA operator). Following this issuance, IdenTrust Confirms in writing that the Trusted Correspondent has been duly appointed by his or her employer. IdenTrust then adds the thumbprint of the Trusted Correspondent's Certificate to an Access Control List for Trusted Correspondents.

Enrollment of a Trusted Correspondent

The Trusted Correspondent performs in-person identification of applicants and collects the information required by sections 3.2.2 and 3.2.3. A Trusted Internal Correspondent may also Confirm the affiliation between an applicant and the associated Subscribing Organization. The Trusted Correspondent gathers the Certificate application information identified in section 4.1.2.1, including name, address, phone number, e-mail address, Subscribing Organization name and organizational affiliation, into a bulk Certificate issuance request. The Trusted Correspondent Confirms the accuracy of the photograph on the photo ID against the appearance of the applicant. The bulk Certificate request is digitally signed by the Trusted Correspondent and delivered in a secure manner to the RA

Operator so as to preserve the confidentiality of the applicant's data during transport. The two options for secure manner of transport used are: 1) uploading the information to IdenTrust using a Client-authenticated SSL/TLS connection, or 2) sending the bulk Certificate request in a signed and encrypted email to the RA Operator using the Medium Token/Medium Hardware Assurance Certificates. This signature will be verified as valid and belonging to the Trusted Correspondent before it will be accepted by the RA Operator.

Trusted Correspondent Bulk Loading Enrollment Process

The Trusted Correspondent seals paperwork such as In-Person Identification Form(s) and signed declarations/agreements in a sealed overnight delivery package commonly used by domestic and international couriers for delivery via overnight mail to IdenTrust. The RA Operator at IdenTrust reviews the In-Person Identification Forms and any other documentation, compares them with the bulk-loaded file signed with the verified Trusted Correspondent's ECA Certificate, and determines whether to approve the issuance of the requested Certificates. Upon approval, Activation Codes are generated and retrieval kits are assembled and delivered to the applicants for use during Certificate retrieval in accordance with section 4.3 below.

4.1.4 Delivery of Subscriber's Public Key to Certificate Issuer

Each Subscriber generates his or her own Signing Key Pair and transmits the public key to IdenTrust as described in section 4.3.1. Subscriber encryption key pairs are generated in accordance with section 6.1.2.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The identification is examined by one of the types of Registrars identified in section 1.3.2 or an RA Operator.

For Certificates issued to Individual Subscribers, the Registrar or RA Operator examines the identification documents for the applicant as specified in section 3.2.3.1.2. When Registrars perform this function, they sign the ID Form and forward it to IdenTrust's RA Operator for review and processing as explained in Section 4.1.2.5.

For Certificates issued to Components, the Registrar or RA Operator examines the identification document for the PKI Sponsor as specified in section 3.2.3.1.2. When Registrars perform this function, they sign the ID Form and forward it to IdenTrust's RA Operator for review and processing as explained in Section 4.1.2.5. For the Component itself, the RA Operator examines the documentation as specified in Section 3.2.3.3.

4.2.2 Approval or Rejection of Certificate Applications

The RA Operator reviews the ID Form, business authorization forms, and any other supporting documentation submitted by applicants or Registrars to determine for each applicant whether the identifying information is (i) internally consistent, and (ii) consistent with the information contained in the application for the Certificate.

The RA Operator may approve Certificate issuance if all required steps in sections 3.2.1, 3.2.2, 3.2.3, 4.1.1, 4.1.2, and 4.1.3 (when applicable) have been completed successfully.

The RA Operator will reject a Certificate application if:

- one of the required steps in section 3.2.1, 3.2.2, 3.2.3, 4.1.1, 4.1.2, and/or 4.1.3 (when applicable) cannot be successfully completed;
- the applicant fails to respond or does not provide requested documentation within a reasonable timeframe;
- payment has not been received or other satisfactory payment arrangements have not been made; or
- the RA Operator reasonably believes that issuance of the Certificate may create an unnecessary risk to the reputation of IdenTrust.

Upon approval of the Certificate by the RA Operator, an Activation Code is generated for use during Certificate issuance, as described in Section 4.3.

4.2.3 Time to Process Certificate Applications

Because only thirty days may elapse between in-person identity confirmation and retrieval of a Certificate, IdenTrust's RA Operator will respond promptly to all Certificate applications and Certificates will be made available for retrieval by applicants following completion of the steps listed in this section 4.2 (provided that the applicant promptly responds to a notice from IdenTrust that Certificate issuance has been approved and that the Certificate is ready for retrieval). If the Applicant does not respond within the thirty day time frame, they must apply again using the processes listed in section 3.2 to be verified in order to receive another activation code. The previous activation code expires and is disabled to prevent any use or reissuance.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Issuance of an IdenTrust ECA Certificate occurs once an application for that Certificate has (1) been approved by a Registration Authority Operator, (2) IdenTrust delivers a retrieval kit to the Subscriber in accordance with section 4.1.2.6, and (3) the Subscriber initiates the web-based retrieval process. The retrieval kit delivered to a Subscriber contains a unique Activation Code generated by IdenTrust as well as retrieval instructions. It may contain a Cryptographic Module meeting or exceeding the minimum requirements required for the assurance level of the Certificate. The Cryptographic Module will be recorded in the Subscriber Database by the unique identifier (e.g., serial

numbers) and that identifier is used in the retrieval process to confirm it is a known hardware Cryptographic Module.

For each Certificate issuance to an Individual, the following occurs during the same Server-authenticated SSL/TLS session:

1. The Subscriber initiates the Certificate retrieval by accessing via a browser a URL ("Retrieval URL") provided within their retrieval kit. In the resulting web session, the IdenTrust CA system authenticates itself to the Subscriber and encrypts all communication utilizing a Server-authenticated SSL/TLS encrypted channel verifiable by a Certificate issued by a distinct IdenTrust Certification Authority natively trusted in browsers.
2. The Subscriber authenticates herself to the web server used in the retrieval process by supplying the Activation Code delivered within the retrieval kit together with the account password selected by the Subscriber during application process described in section 4.1.2.1. Both pieces of information are required for all Certificate retrievals by a Subscriber from IdenTrust.
3. Upon authentication of the Subscriber to the Retrieval URL and verification of 'approved' status of the Subscriber's Certificate application and that not more than 30 days have transpired since in-person identity confirmation, the Subscriber may proceed with the retrieval[18]. In order to accomplish subsequent steps, IdenTrust downloads an IdenTrust-written browser component (e.g., ActiveX control) over the secure session.
4. Using the browser component IdenTrust assures that the Cryptographic Module is hardware when Medium Token and Medium Hardware assurance Certificates are issued. This verification for hardware is done through application programming interface checks (e.g., CSP and PKCS#11) which ensures the software being used in the session is the type expected as well as verifying that the unique identifier extracted from the Cryptographic Module and the identifier previously recorded in the Applicant's account are the same. For all assurance levels, IdenTrust performs key generation for encryption key, which is securely transported to the client, as described below in section 6.1.2. Subsequently, Signing Keys are generated locally on the Cryptographic Module. The resulting public Signing Key is encapsulated in a Certificate request in the form prescribed by RSA PKCS#10.
5. The PKCS#10 Certificate request for the Signing Certificate is submitted to the IdenTrust ECA for Certificate generation. The PKCS#10 is not accepted if the key length is less than 2048 bits, if the public exponent is outside of the allowed range specified in FIPS 186-3, or if the key is a known weak key (e.g. blacklisted Debian key). The confirmed information in the Subscriber Database, which has been configured based on the appropriate Certificate profile, and the verified information provided during the identity-proofing process is used and the Subject

[18] The 30-day period is calculated based on the in-person identification date value entered into the Subscriber Database by the IdenTrust RA Operator (based on the review of the In-Person Identification Form as described in section 4.1.2.5). If more than 30 days have passed since the in-person appearance, the system prevents the Subscriber from proceeding with key generation and notifies them that in-person identification must be repeated.

DN information submitted in the PKCS#10 is overridden. However, the binding between the public key within the PKCS#10 Certificate request and the private key is maintained—the signature on the PKCS#10 Certificate request is verified by the CA to ensure that it was signed with the corresponding private key prior to building the Certificate.

6. IdenTrust delivers the Subscriber's Certificates to the Subscriber's Certificate store (in either a browser or a hardware Cryptographic Module) using a format adhering to RSA PKCS #7. The Encryption private key is delivered encrypted based on processes listed in section 6.1.2.
7. In addition, IdenTrust delivers the Root ECA Certificate and the IdenTrust ECA Certificate in RSA PKCS #7 format with instructions to download them into the Subscriber's Certificate store. On supported platforms, the installation of both the Root ECA and IdenTrust ECA Certificates are automated via a web interface.
8. Installation of the Subscriber's Signing Certificate and IdenTrust ECA Certificate is confirmed by initiating a Client-authenticated SSL/TLS session between IdenTrust's Retrieval URL and the Subscriber's client platform. Upon successful installation of the Subscriber's Certificates, both Signing and Encryption Certificates will be published in IdenTrust's Repository.
9. Installation of the Subscriber's signing Certificate and the IdenTrust ECA Certificate is confirmed at the end of the retrieval process by having the Subscriber verify the Certificate retrieval. The Subscriber will be asked to click on a link that directs him or her to a web page for which the IdenTrust webserver requests a Client-authenticated SSL/TLS session. The Subscriber's web browser will ask him or her to present a Certificate. If the web browser is able to successfully establish a Client-authenticated SSL/TLS connection, the web page outputs a message indicating that the Certificate was successfully tested. If the web browser is not able to establish a Client-authenticated SSL/TLS connection, the web page outputs a message indicating that the Certificate was unable to be tested, how to re-test, and to call IdenTrust if they are unable to complete the test.

For the issuance of a Component Certificate, the PKI Sponsor needs to follow only steps 1 and 2 above. (Note that the PKI Sponsor generates the key pair for the Component and submits the PKCS#10 Certificate request as an initial step during registration). The Certificate issuance process described in this section will ensure that this CPS is in compliance with the ECA CP and that the following has occurred for both Signing and Encryption Certificates:

(1) IdenTrust has confirmed the source of the Certificate request.

(2) IdenTrust has confirmed the authenticity and authority of the source of information contained within the Subscriber's Certificates.

(3) IdenTrust has built and signed the Subscriber's Certificates in a secure manner.

(4) IdenTrust has delivered the Subscriber Certificates, the IdenTrust ECA Certificate, and the root ECA Certificate to the Subscriber.

(5) IdenTrust has published the Subscriber's Certificates to IdenTrust's Repository.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

An online notification process occurs during Certificate issuance which informs the Subscriber that the Certificates have been successfully generated, retrieved and delivered to the Subscriber's Cryptographic Module.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

At the time of application for a Certificate, IdenTrust requires the applicant to agree—by acknowledging assent with a "click" to accept—to the Subscriber Agreement, which requires the Subscriber to perform his responsibilities under Section 9.6.3 of the ECA CP and this CPS in applying for, reviewing, and using the Certificate. The Subscriber is also required to request revocation when appropriate.

Upon issuance and installation of the Certificate, IdenTrust requires the Subscriber to review the Certificate and affirmatively communicate acceptance of its content. For the Encryption Certificate, in addition to the acceptance of the Certificate content, the Subscriber will be informed about the escrow of the encryption key. IdenTrust escrows all encryption keys generated and retrieved by a Subscriber.

4.4.2 Publication of the Certificate by the CA

Pursuant to section 2.2, IdenTrust publishes CA and Subscriber Certificates in its Repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers shall not use the signature key after the associated Certificate has been revoked or has expired. However, they may continue to use the private encryption key solely to decrypt previously encrypted information after the associated Certificate has been revoked or has expired.

Subscribers shall only use of the private key in accordance with the key usage and extended key usage extensions in the corresponding Certificate for that key. For example, the OCSP Responder private key shall be used only for signing OCSP responses.

4.5.1 Relying Party Public Key and Certificate Usage

Relying parties shall ensure that each public key Certificate is used only for the purposes indicated by the key usage or extended key usage extension in the Certificate corresponding to that public key.

4.6 Certificate Renewal

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

After Certificate renewal, the old Certificate is not revoked by IdenTrust and the Subscriber may or may not request revocation. In any case, the system automatically, or, for Certificates used for the PKI system the Operations group procedurally, prevents the Certificate to be renewed again, re-keyed or modified.

4.6.1 Circumstance for Certificate Renewal

IdenTrust does not offer renewal for Subscribers' Certificates.

OCSP Responder Certificates are renewed on a monthly basis as long as use of the corresponding key pair has not extended its usage period, see section 6.3.2, the Certificate has not been revoked, and the Subscriber (i.e., OCSP Responder) name and attributes are still correct.

4.6.2 Who May Request Renewal

OCSP Responders are operated within IdenTrust facilities and are managed by the IdenTrust CA Administrator who requests that the OCSP Responder Certificate is renewed.

4.6.3 Processing Certificate Renewal Requests

Prior to expiration of each OCSP Responder Certificate, its signing key is re-signed during a Certificate renewal ceremony performed in the secure room under controls described in Section 5.1.2.1.1 and 6.1.1.

4.6.4 Notification of New Certificate Issuance to Subscriber

CSAs are operated within IdenTrust facilities and are managed by the IdenTrust CA Administrator who requests that the OCSP Responder Certificate is renewed.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The CA Administrator accepts the OCSP Responder Certificate by allowing it to be published in the Repository and installing the newly issued Certificate to the OCSP Responder to be sent out with the responses.

4.6.6 Publication of the Renewal Certificate by the CA

Pursuant to section 2.2, IdenTrust publishes the OCSP Responder Certificate in its Repository.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

No other entities are notified of Certificate issuance by the CA.

4.7 Certificate Re-Key

Certificate re-key consists of issuing a new Certificate with a different public key and serial number and expiration date while retaining all other information in the original Certificate that describes the subject (i.e., Subject DN, Subject Alternative Name) and the policies under which it was issued. The new Certificate may be assigned different key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

After Certificate re-key, the old Certificate is not revoked by IdenTrust and the Subscriber may or may not request to revoke it.

4.7.1 Circumstance for Certificate Re-Key

Whenever a Certificate is issued based on confirmation performed for an earlier Certificate, the limits specified in section 3.2.3.2 apply. Thus, the *not After* date field in a Certificate may not go beyond the next in-person identity proofing date. This is restricted by ECA system as explained above in section 3.2.3.2.

Certificate re-keying may be performed at any time provided that the lifetime of the new Certificate does not extend beyond the time at which the Subscriber must re-appear before a Registrar for in-person identity proofing.

The Subscriber's account in the database is updated when a Certificate is used to request a re-key. The RA Operator, through manual examination of the Subscribers account; or, the system itself, through automated query of the database, obtains all Certificate records for the Subscriber and verifies that a Certificate being presented has not been used previously in a prior re-key request. If the presented Certificate has not been used to request any of the Certificates, the Subscriber is allowed to re-key.

If confirmation of a new Certificate is based on a digital signature, section 3.2.3.2 requires that that digital signature be verifiable by reference to a valid ECA Certificate issued by IdenTrust and having an assurance level equal to the Certificate to be issued for the Individual Subscriber. This is accomplished by an automatic check of the Certificate against the configuration for that Certificate type within the Subscriber Database.

4.7.2 Who May Request Certification of a New Public Key

The Subscriber or the RA may request the re-key of a Subscriber Certificate.

4.7.3 Processing Certificate Re-Keying Requests

During re-keying, the Subscriber must present his or her currently valid IdenTrust-issued ECA Signing Certificate to establish a Client-authenticated SSL/TLS-encrypted session. IdenTrust's ECA validates the authenticity of the Certificate presented by verifying that it was issued by the IdenTrust ECA, by comparing the status of the Certificate in the relational database to Confirm it is not revoked, and from the same database verifying the Certificate is still valid. The database utilized for this process is the same one used to issue the CRLs and provides a real-time check of the Certificate status to verify its validity (see definition of "Client-authenticated SSL/TLS in Section 14: Glossary.)

IdenTrust offers re-keying services through—"subscription renewal" rekeying. Beginning ninety (90) days prior to the expiration of the Certificate, e-mails are sent to the Subscriber directing him or her to a Certificate management interface where the currently valid IdenTrust-issued ECA Signing Certificate is used to authenticate the Subscriber through a Client-authenticated SSL/TLS-encrypted session.

During subscription re-keying, the Subscriber will complete the process by following the steps provided below. If the Subscriber successfully uses their Certificate to enter the Certificate management interface, they will complete the re-key online through an automated process. This process is completed when the Subscriber (i) checks to ensure that no information in the Certificate has changed, (ii) reviews and accepts the terms of the Subscriber Agreement, and (iii) makes arrangements to pay for the new Certificate.

If the Subscriber changes any information during the process, their re-key application will be referred to an RA Operator for manual review. If it is determined that the Subscriber has changed their name,affiliation, or any data contained in the Certificate, they will need to appear for in-person identity proofing and may not re-key. If the information is determined as minimal and is not information included in the Certificate, (such as a telephone number), the RA Operator will approve the re-key request and send a notification with instructions on how to proceed with the re-key via courier or U.S. mail first class.

If the Subscriber cannot present their Certificate or changes specific information, related to verification (can, organization affiliation, etc.) he or she must appear for in-person identity proofing and may not rekey.

Subscription renewal re-keying is provided for IdenTrust's Medium Assurance Certificates, for Medium Token Assurance Certificates, and for Medium Hardware Certificates.

Subscription re-keying applies to both the Signing and Encryption Certificates simultaneously. Though the initial request is effected by the presentment of the Signing Certificate, the Subscriber Database contains records that associate both the Signing and Encryption Certificates to the Subscriber ensuring subscription renewal re-keying covers both of them.

4.7.4 Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Pursuant to section 2.2, IdenTrust publishes CA Certificates and Subscriber encryption Certificates in its Repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Certificate modification means creating a new Certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old Certificate. A Certificate may be modified if some of the information other than the DN, such as e-mail address or authorization, has changed or was transcribed into the Certificate incorrectly (e.g. a malformed Certificate extension does not match format specified in the Certificate profile). IdenTrust only supports Certificate modification through the re-keying process described above in section 0.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

As described in the ECA CP, an Individual Subscriber may request revocation of his/her Certificate at any time for any reason. A Subscribing Organization may request revocation of a Certificate issued to its Individual Subscriber at any time for any reason. The PKI Sponsor of a Component Certificate may request revocation of that Certificate at any time for any reason.

A Subscriber or a Subscribing Organization is responsible for promptly requesting revocation of a Certificate as soon as any of the following events occurs:

(1) Any name or any other information in the Certificate becomes inaccurate or is discovered to be inaccurate;

(2) The private key corresponding to the public key in the Certificate, or the media holding that private key is known to have been compromised or such a compromise is suspected; or

(3) The Individual Subscriber named in a Certificate is no longer affiliated with the Subscribing Organization.

The Subscriber and Subscribing Organization assume the risk of any failure to request a revocation required above.

IdenTrust will also revoke a Certificate upon discovery or reasonable suspicion that:

(4) the private key corresponding to the public key listed in the Certificate has been compromised;

(5) the Subscriber (or the Subscribing Organization, where applicable) has failed to meet its obligations under the ECA CP, the public version of this CPS, or an applicable agreement, regulation, or law;

(6) the Certificate was not issued in accordance with the ECA CP and/or IdenTrust's ECA CPS, including that the Certificate was obtained by fraud or mistake or that it was not otherwise properly requested or accepted by the Subscriber;

(7) the Certificate contains inaccurate information, is defective in form, or has become unreliable for reasons including, but not limited to, material information in the application for a Certificate or in the Certificate itself change or become false or misleading (e.g., the Subscriber changes his or her name); or

(8) a governmental authority has lawfully ordered IdenTrust to revoke the Certificate.

When any of the circumstances listed above in this section occur, IdenTrust revokes the relevant Certificate. In addition, if the private keys of any Certificate used to request other Certificates are determined to have been compromised at the time of request of any Certificate, those Certificates for which the compromised key was used to sign the request and that chain back directly or indirectly to it, will be revoked. For example, as described in section 4.9.3.2, upon compromise of a RA Operator or a Trusted Correspondent, any Certificates that were approved at the time and after the private key was compromised will be revoked. Similarly, if the private key of a PKI Sponsor is compromised, any Component Certificates approved at the time or after the related private key was compromised will also be revoked as described in Section 4.9.3.1. Revoked Certificates are included on all new publications of the CRL until the Certificates expire.

4.9.2 Who Can Request a Revocation

The following persons may request the revocation of a Certificate:

- the Subscriber;
- a Trusted Internal Correspondent, the PKI POC or an official or supervisor within the Subscribing Organization listed in the Certificate;
- the Trusted Correspondent who performed the identity confirmation preparatory to issuance of the Certificate;
- the PKI Sponsor of a Component Certificate; or
- the DOD, including but not limited to the ECA Liaison Officer and any person appointed by the EPMA.

IdenTrust may revoke any Certificate that it has issued for any of the reasons identified in section 4.9.1. Also, whenever IdenTrust receives a revocation request that is signed on behalf of or otherwise reliably authenticated to a Subscribing Organization, such as a

request from a Trusted Internal Correspondent or other authorized individual in the Subscribing Organization, which is in a form specified by IdenTrust, then IdenTrust will revoke the specified Certificate. For example, a personnel office may request revocation of a Certificate issued to a former employee.

IdenTrust will provide a written notice and brief explanation for the revocation, which is sent to the Subscriber's email address of record, after the revocation has been completed.

4.9.3 Procedure for Revocation Request

A revocation request should be promptly communicated to IdenTrust, either directly or through a Trusted Correspondent or PKI POC. Self-service revocation is available to the Subscriber through IdenTrust's Certificate management interface (to the Subscriber of a valid ECA Signature Certificate). Otherwise, a revocation request should be initiated through a digitally signed email to helpdesk@identrust.com and a phone call to IdenTrust's help desk at 1-888-882-1104 (within the U.S.) or 1-801-924-8141 (non-toll free/outside the U.S.).

For implementations using cryptographic hardware modules, a Subscriber ceasing its relationship with a Subscribing Organization will, prior to departure, surrender to the Subscribing Organization (through any accountable mechanism) all cryptographic hardware Cryptographic Modules that were issued to him. The Cryptographic Module will be zeroized or destroyed promptly upon surrender and will be protected from malicious use between surrender and zeroization or destruction. The Trusted Correspondent or PKI POC receiving the Cryptographic Modules will notify IdenTrust of Cryptographic Module zeroization or destruction and request revocation of all Certificates associated with the Subscriber's DN. This notification will occur during the revocation request as explained in the procedures below.

Whenever a Subscriber is no longer affiliated with his Subscribing Organization, such as by termination of employment, the Subscribing Organization will issue a prompt request for revocation of his Certificates, regardless of whether any Cryptographic Module containing them can be secured and destroyed. If the Cryptographic Module is not returned by the Subscriber, the Subscribing Organization will inform IdenTrust about this situation. In cases when the Cryptographic Module is not returned or the Subscribing Organization fails to notify IdenTrust, IdenTrust will revoke the Certificates belonging to the Subscriber and assign a reason of Key Compromise.

Regardless of the means by which a revocation request is communicated to IdenTrust, when IdenTrust has validated the request as set forth below, the Certificate will promptly be revoked and the revocation noted in the status information recorded in the CRL. A valid revocation request for a Signing Certificate results in revocation of the Signing Certificate and its associated Encryption Certificate Revocation is executed manually by the RA Operator who accesses the Subscriber account information in the RA system and identifies both Certificates through their description. Revocation is explicitly selected as a status change for each Certificate. When the self-service revocation is requested, the system uses the records in the database to logically link both the Signing and Encryption Certificates.

The Repository is updated with a CRL pursuant to section 4.9.7. Information about a

revoked Certificate will remain in the status information until the Certificate expires.

4.9.3.1 Subscriber or PKI Sponsor Revocation Procedure

A Subscriber's revocation request must be communicated electronically to IdenTrust by either authenticating through the IdenTrust Certificate management interface using the Certificate to be revoked, or by sending a digitally signed email with the private key of the Certificate to be revoked or, in the case of a Component Certificate, with the PKI Sponsor's Certificate. If the request is sent by email, then as a redundant measure, the request must also be submitted by calling the IdenTrust Help Desk line as described above.

The digitally signed message may be submitted to IdenTrust's Help Desk, the Subscribing Organization's authorized Trusted Correspondent or the Subscribing Organization PKI POC. In any case, including revocation through the Certificate management interface, the Subscriber must provide a reason for revocation. If the revocation is being requested for reason of key compromise or suspected fraudulent use of the private key, then the revocation request must so indicate.

- In case the e-mail is addressed directly to IdenTrust, on positive verification of digital signature an IdenTrust RA Operator will revoke the Subscriber's IdenTrust ECA Certificate used to create the signature. If the signature belongs to the PKI Sponsor who initially requested the Certificate (see Section 3.2.3.3) and whose contact information is recorded in the Certificate account for the Component, the Component Certificate(s) identified as approved by the compromised Certificate in the message will be revoked.
- In case the email is addressed to the Trusted Correspondent or the PKI POC, he or she will verify the Subscriber or PKI Sponsor's signature, ensure a revocation reason is provided, collect and zeroize any hardware Cryptographic Module, create a record and submit the request to IdenTrust's Help Desk via a signed e-mail and phone call.

The Trusted Correspondent or PKI POC will provide the Subscriber's or PKI Sponsor's information, the domain name (Fully Qualified Domain Name for Component Certificates) of the Certificate(s) to be revoked, a revocation reason, attach the original signed request and digitally sign the message with her IdenTrust ECA Certificate. For Medium Token Assurance Level and Medium Hardware Assurance Level Certificates, the request must indicate if the Cryptographic Module was returned and zeroized by including its serial number.

IdenTrust's RA Operator will verify the Trusted Correspondent's or PKI POC's digital signature, Confirm completeness of information, and ensure that the Trusted Correspondent is authorized by the Subscribing Organization by matching the Certificate's thumbprint from the request email's signature with the record in the Access Control List that was created after the Trusted Correspondent' appointment by the Subscribing Organization (see Section 4.1.3). On positive confirmation the RA Operator will revoke the Subscriber's or Component Certificate(s) using the RA system.

If the Subscriber or PKI Sponsor cannot authenticate to the Certificate management center or digitally sign a revocation request (i.e., locked or lost Cryptographic Module), the individual must contact its authorized Trusted Correspondent or PKI POC in person and provide proof of identity equivalent to the proof provided during initial registration. If the request is for a Subscriber Certificate, after confirming the Subscriber's identity, the Trusted Correspondent will submit a digitally signed revocation request to IdenTrust's Help Desk as explained above. If the request is for a Component Certificate, in addition to identity confirmation, the Trusted Correspondent or PKI POC must verify the PKI Sponsor's authority to request revocation with his or her supervisor or contract manager. On positive verification the Trusted Correspondent or PKI POC will submit a signed message to IdenTrust's Help Desk.

4.9.3.2 Subscribing Organization Revocation Procedure

A Subscribing Organization must request revocation through its authorized Trusted Correspondents or PKI POC, if either one exist. The Trusted Correspondent or PKI POC is responsible for authenticating requests from all requesters within the Subscribing Organization. The Trusted Correspondent or PKI POC may confirm the identity of the requester using the method explained in section 3.2.3.1.2 or by using a message from the Requestor digitally signed with an IdenTrust ECA Certificate. Revocation may be requested by a person with authority. The Requestor's authority is established by verifying a supervisory relationship to the Subscriber or the PKI Sponsor. Authority is also established if the Requestor is an officer, a member of the personnel office or a security officer of the Subscribing Organization.

After confirmation of the request, the Trusted Correspondent or PKI POC will create a record with the Subscriber or PKI Sponsor's name, email, reason for revocation (including if they key has been compromised), the Fully Qualified Domain Name for Component Certificates, and for Medium Token and Medium Hardware Certificates if the Cryptographic Module has been returned and zeroized and its serial number. The record will also include the Requestor's name, e-mail address, title, and identification information. The Trusted Correspondent or PKI POC will submit a digitally signed revocation request and call to the IdenTrust's Help Desk. After verification of the request, an RA Operator will revoke the Certificate.

If for exceptional reasons, within a Subscribing Organization neither the Trusted Correspondent nor the PKI POC has control over their keys; a Trusted Correspondent or the PKI POC still can submit a revocation request for herself. In this case, an IdenTrust RA Operator will confirm the Requestor's identity by comparing the information provided against the information gathered during the process used to nominate, approve and configure the Trusted Correspondent's or PKI POC's status, which includes: identity information, wet signature, contact information and supervisor's contact information. Additionally, IdenTrust will contact other, if any, Trusted Correspondents or PKI POC on record or the Trusted Correspondent's or PKI POC's supervisor on record to verify the authority of the Trusted Correspondent or PKI POC.

In exceptional cases when the Subscribing Organization does not have immediate access to a Trusted Correspondent or PKI POC (i.e., the Trusted Correspondent or PKI POC is being terminated), a Subscribing Organization's representative not appointed to the PKI

POC can request revocation directly via a signed e-mail and call to the Help Desk, or mail to the Registration Desk on company letterhead containing a notarized signature. The communication should include the information about the Subscriber's Certificate to be revoked. If the revocation is being requested for reason of key compromise or suspected fraudulent use of the private key, or if the cryptographic hardware module could not be collected and zeroized, then the revocation request must indicate key compromise. IdenTrust will contact the Subscribing Organization's personnel office or the Requestor's supervisor and Confirm the Requestor's authority for revocation.

When an RA Operator or a Trusted Correspondent Certificate is revoked because of a compromise, all Subscribers' Certificates that were directly or indirectly authorized for issuance by the person will also be revoked by the IdenTrust ECA. Identification of the Subscribers affected by the revocation of an RA Operator Certificate is performed by querying the RA system about all the Subscriber Certificates authorized by the RA Operator since the compromise date. In the case of a Trusted Correspondent Certificate being revoked, electronic records (i.e., bulkload spreadsheets or XML data structures) that hold the information of requested Certificates will be consulted. Revocation is performed individually for every Certificate by an IdenTrust RA Operator. The reason code for the CRL will be populated with a KeyCompromise. Returning Cryptographic Modules is not necessary since they will be reused to generate and store replacement Certificates.

4.9.3.3 DOD Revocation Procedure

The IdenTrust help desk will maintain a list of individuals who are authorized by the DOD to request revocation of any Subscriber or CA Certificate. The list will include the ECA Liaison Officer and any other persons appointed by the EPMA for such purpose.

The initial person in the list is the ECA Liaison Officer whose Certificate's information (e.g., thumbprint) is added to the list based on an ongoing relationship (e.g., prior email exchanges and matching such email to email extracted from the digital signature). The list will include the thumbprint of his or her Certificate, full name and telephone number. In the case of a new liaison officer, IdenTrust will contact the ECA Program Office, via a known DISA email address, such as pkieca@disa.mil. DISA then will reply with the serial number or thumbprint from the Certificate of the new liaison officer. Additional Requestors may be added by the Liaison Officer by sending a request in a digitally-signed email. The request will include the name, contact information, and Certificate of the new person. After verifying the validity of the liaison's signature and the match of the thumbprint, the new person will be added to the list with the information used to Confirm their authority (including the thumbprint and DN from the Certificate).

These individuals shall use the procedure specified above in Section 4.9.3 (digitally signed e-mail and telephone call to the IdenTrust help desk). Revocation support to the DOD will be available on a 24x7 basis via telephone.

If a Certificate needs to be revoked after-hours (nights, holidays and weekends), then the person calling the IdenTrust help desk should tell the person answering the phone that a Certificate has to be revoked immediately. IdenTrust will then begin efforts to Confirm the requesting individual's identity, authority and basis for requesting revocation of the

Certificate.

4.9.4 Revocation Request Grace Period

There is no grace period for an ECA revocation request. IdenTrust will revoke a Certificate as quickly as practical upon validation of a revocation request. IdenTrust's Subscriber Agreement requires Subscribers to notify IdenTrust of the need for revocation as soon as it comes to their attention.

Verified revocation requests will be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. IdenTrust will always revoke Certificates within the time constraints described in section 4.9.5.

4.9.5 Time Within Which CA Must Process the Revocation Request

IdenTrust processes all revocation requests within one hour of notification as explained in Section 4.9.3. CRL issuance frequency is addressed in Section 4.9.7.

4.9.6 Revocation Checking Requirements for Relying Parties

Reliance upon revoked Certificates is always hazardous and could have damaging or catastrophic consequences in certain circumstances. IdenTrust assumes no liability for reliance upon a revoked Certificate; it is therefore advisable to check for revocation in every instance before relying on a Certificate. If it is temporarily infeasible to obtain current revocation information, then the Relying Party must either reject use of the Certificate, or assume all risk, responsibility, and consequences of reliance upon it.

A Relying Party must check the most recent CRL each time reliance is to occur upon a Certificate. Reliance on an outdated CRL can cause a recent revocation to escape the Relying Party's notice. The thisUpdate field indicates when a CRL was issued and nextUpdate when the next version is to be issued.

4.9.7 CRL Issuance Frequency

CRLs are generated and issued at least every 12 hours and are posted immediately to a Repository, even if there are no changes from the prior CRL, to ensure timeliness of information. In addition:

- Although CRLs are issued every 12 hours, IdenTrust may issue a CRL more frequently, such as following revocation for reasons such as a key compromise;
- A new CRL is created that consists of all the revocations processed since the previous CRL issuance; and all the revocations in the last CRL, except for the Certificates that have since expired. The new CRL replaces the previous CRL in the Repository; and
- All issued CRLs will have validity of 24 hours.

A CRL distribution point in each Certificate points each Relying Party to the directory containing the CRL. Both that directory and the IdenTrust public web site also publish

this CPS to advise Relying Parties how to obtain revocation information with respect to a Certificate they may wish to rely upon.

4.9.8 Maximum Latency for CRLs

The CRL shall be posted immediately and in no case more than four hours after generation.

4.9.9 On-line Revocation/Status Checking Availability

IdenTrust will deploy a Certificate Status Authority using On-Line Certificate Status Protocol ("OCSP") responders to enable Certificate revocation status checking of IdenTrust ECA Subscriber Certificates only. For each instance IdenTrust ECA signs its own Certificate, which in turn is used by an OCSP Responder to provide signed status responses for all End Entity Certificates issued by the ECA. For more information on the brand and model of the OCSP Responders see Appendix G. Such OCSP Responder cannot validate the Certificate status of the IdenTrust ECA itself. Instead, the validation of the IdenTrust ECA is provided by the ECA Root using the methods defined by the EPMA. Therefore, Certificate chain validation requires that, at a minimum, the CRL from the ECA Root also be checked for revocation of the IdenTrust ECA's Certificate.

The OCSP Responders used in IdenTrust's CSA will sign all OCSP responses with private keys protected commensurately with the assurance level of the Certificate being checked. The Signing key is generated and stored in a Cryptographic Module validated as conforming to FIPS 140 as explained in section 6.1.1. The OCSP Responder key will be held under strict controls as explained in section 5.1.2.1.1. The OCSP Responder Certificate will be signed with the same CA key as the Certificate being validated.

The OCSP Responders will ensure that accurate up-to-date Certificate status information is provided in the revocation status response. The OCSP server will download the most recent CRL every two hours and use it to create the response. If for any reason the OCSP Responder is unable to obtain that CRL, the responder will use the most recent valid CRL until it expires, then it will return an error or invalid status code as response.

The address of the OCSP Responder for a given Certificate can be ascertained from its AuthorityInformationAccess extension.

4.9.10 On-Line Revocation Checking Requirements

Relying Parties must check Certificate status using either CRLs or OCSP. If a Relying Party cannot use OCSP, then it should check the most recently issued CRL. If a Relying Party is using OCSP, then there is no need obtain or process CRLs.

Relying parties (including CMAs) shall only rely upon OCSP Responders approved in accordance with the requirements of the CP.

4.9.11 Other Forms of Revocation Advertisements Available

IdenTrust does not support any other method for obtaining Certificate status information than those described in sections 4.9.7 and 4.9.9.

4.9.12 Special Requirements Related to Key Compromise

IdenTrust has the ability to transition any reason code in a CRL to compromise. However, IdenTrust does not confirm the accuracy of the reason given by the Subscriber or Subscribing Organization for revocation of the Certificate.

IdenTrust will not utilize the CertificateHold (6) code.

4.9.13 Circumstances for Suspension

Not Applicable.

4.9.14 Who Can Request Suspension

Not Applicable.

4.9.15 Procedure for Suspension Request

Not Applicable.

4.9.16 Limits on Suspension Period

Not Applicable.

4.10 CERTIFICATE STATUS SERVICES

No stipulation.

4.11 END OF SUBSCRIPTION

Subscription is synonymous with the Certificate validity period. The subscription ends when the Certificate is revoked or expired.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

IdenTrust's ECA key escrow recovery practices are described in its Key Recovery Practices Statement.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

IdenTrust does not support key escrow and recovery using key encapsulation techniques.

5. Physical, Procedural, and Personnel Security Controls

5.1 Physical Controls

IdenTrust dedicates a computer system specifically to its PKI operations. IdenTrust dedicates a hardware and software system for ECA's CA function. The CA system is logically and physically separated from all other IdenTrust CA operations, and can only be accessed physically within the secure room. IdenTrust shares the RA function, databases, networking and physical housing with other certification systems. The ECA operation is serviced by trusted IdenTrust personnel as are other certification systems. All trusted IdenTrust personnel meet the requirements of the ECA CP for Trusted Roles.

Subscribers and Relying Parties do not have access to the PKI-specific ECA platform. Logs, lists of Certificates issued and revoked, and the directory tree information are located on a dedicated certification system, where they are not accessible for modification by anyone other than IdenTrust personnel functioning in their respective Trusted Roles.

IdenTrust collects data from those databases and directories to broader, more comprehensive compilations for billing, Repository, and similar purposes. Those wider systems are not operated from a PKI-exclusive system. Some such systems are available to Subscribers and Relying Parties to a controlled extent by agreement with IdenTrust.

Each Cryptographic Module housing a private key used for IdenTrust's ECA services is used for no other purpose. They are handled by the same IdenTrust trusted staff and kept in the same secure storage locations as other Cryptographic Modules, but ECA Cryptographic Modules are used only for ECA keys. Moreover, their activation data differs from that used for other Cryptographic Modules.

IdenTrust's ECA equipment, including all Cryptographic Modules, is located in Utah, which has statutes against computer trespass and intrusion. In addition, federal computer security legislation applies. Together, those laws generally forbid unauthorized use and access to IdenTrust computer equipment; however, legal advice should be obtained in specific cases.

IdenTrust has three facilities dedicated to host CMA equipment. In selecting the appropriate facilities, risk management techniques have been used and controls have been designed to mitigate specific risks IdenTrust's CA and CSA equipment are hosted in a primary facility that provides the highest-risk protection. IdenTrust's RA equipment is hosted in a high-risk protection facility different from the primary facility where the CA and CSA are located. For purposes of disaster recovery, a third facility in a geographically-diverse location has been selected and provides risk protection equivalent to the primary facility hosting the CA/CSA equipment.

Physical security controls protecting the certification platform and Cryptographic Modules are described in the remainder of this section. These physical security controls are intended as protection against theft, loss and unauthorized use.

5.1.1 Site Location and Construction

IdenTrust has three facilities dedicated to hosting CA, CSA and RA equipment. In selecting the appropriate facilities, risk management techniques have been used and controls have been designed to mitigate specific risks. IdenTrust's CA, CSA and the RA's server-side equipment are hosted in a primary facility that provides the highest-risk protection. The RA's client-side equipment is hosted in a high-risk protection facility different from the primary facility where the CA, CSA and RA's server-side are located. For purposes of disaster recovery, a third facility in a geographically-diverse location has been selected and provides risk protection equivalent to the primary facility. Physical security controls protecting the certification platform and Cryptographic Modules[19] are described in the remainder of this section. These physical security controls are intended as protection against theft, loss and unauthorized use.

5.1.1.1 IdenTrust's CA and CSA sites

5.1.1.1.1 Primary Facility

IdenTrust's CA, CSA and RA server equipment is located in Salt Lake City, Utah, in the United States. It is housed in an unmarked building; the site is not identified as housing IdenTrust equipment in a publicly visible way.

The building is a "zone 4" essential facilities building as established by the Uniform Building Code ("UBC"), capable of withstanding an earthquake in the 7.0 to 8.0-magnitude range. The computing facility is built on base Dynamic Isolation Systems ("DIS") seismic isolators, a rigid exterior steel-braced frame, and heavy concrete floor slabs which minimize motion in the case of earthquake. The building has ready access to two electrical power substations and two conduit entrances and provides increased layers of security as an individual comes in closer contact to the critical assets and computer system in the secure room.

The data center is located in the second floor and resides within an area with no windows. The secure room, where ECA's CA, CSA and RA server equipment is hosted, is built within the data center. The room has only one restricted-access point and its ceiling and floor are protected by chain link fencing.

Six layers of security surround the CA, CSA and RA server equipment: A chain link fence around the property with only two access gates that are under 24x7 surveillance; the internal and external building access doors configured in a mantrap system; and the controlled access doors to the office suites. A separate layer of security is required for access to the computer room (which contains the secure room where the ECA equipment resides); an additional layer of security is required for access to the secure room itself. Roof access is through an internal stair well in a mantrap and is kept locked.

[19] Hardware Cryptographic Module private key storage practices are discussed in Section 6.2.2.

5.1.1.1.2 Disaster Recovery Facility

IdenTrust's disaster recovery data center is located in Denver, Colorado in the United States. This area is not prone to environmental hazards such as tornadoes, earthquakes, hurricanes, forest fires etc. The data center is housed in a concrete, unmarked building; the site is not identified as housing IdenTrust equipment in a publicly visible way. The data center is located in the first floor within an area with no windows. The secure room is in the center of the data center floor at a distance of no less than 50 feet from the external walls.

Three layers of security surround the CA, CSA and RA server equipment in the disaster recovery center: Bollards surround the building and three access points are under 24x7 surveillance with internal and external cameras; the main entrance to the data center is configured in a mantrap system and dual access control is required; and an additional layer of security is required for access to the Secure Room itself and is within a chain fence walls with motion-sensor under the floor.

5.1.1.2 IdenTrust's RA site

RA client-side equipment is located in a building geographically separated from the CA site. It is housed in an unmarked building; the site is not identified as housing IdenTrust equipment in a publicly visible way. RA client equipment is located in an isolated and restricted-access room in the second floor of the building.

Three layers of security surround the RA client equipment: External building doors with restricted access (or under receptionist/security guard surveillance during normal business hours); internal floor door with restricted access (proximity card controlled); and, RA room door with further restricted, card-based access.

5.1.2 Physical Access

5.1.2.1 Physical Access to CA, CSA platforms

5.1.2.1.1 Primary Facility

The building is located on fenced and guarded grounds. One guard post is within 50 feet, in a clear line of sight, from the main entrance to the building. The building entryways and passageways are under continuous recorded video surveillance. The facility is manned 24x7x365 and is never left unattended.

The data- center- provider staff members perform checks of the facility once per shift (three times daily), covering the facility's access points, cameras, and other aspects of a physical walk through. Additionally, IdenTrust's Security Officers perform a weekly check and review of the security integrity of the secure room to ensure that alarms, access points, biometrics, safes (containing Cryptographic Modules and activation materials), video cameras, storage containers, access logging, etc., are operational and functioning correctly. A record of the weekly review is kept that describes the type of checks performed, the time, and the person who performed them. Records are kept for no less than one year to meet the hosting facility's audit standards, and are reviewed with

external auditors on an annual basis as part of the WebTrust for Certificate Authorities audit.

IdenTrust personnel require pass cards to enter through the external property gate and to enter the mantrap at the building entrance. The pass card and PIN number are required to enter the building. Entry to IdenTrust areas within the building also requires pass cards. Pass cards for IdenTrust personnel working in the building are granted upon authorization from IdenTrust security officers.

Employees are prohibited from permitting unknown or unauthorized persons to pass through doors, gates, and other entrances to IdenTrust-restricted areas when accessing the facilities. Authorization to enter the IdenTrust-controlled areas of the facility must be obtained in advance from the Operations Management.

Visitors are allowed within the fence only with authorization from the guard in the control center after properly identifying themselves and their purpose for the visit. Also, visitors are only allowed to access IdenTrust offices after their visit's purpose and identities have been verified; they have signed an entry log; and an IdenTrust employee escorts them. Visitors are not allowed to roam in IdenTrust-controlled areas without escorts.

The secure room is physically secured with two-person, dual-factor authentication including biometrics. The room is also equipped with a 24x7x365 camera system monitored by operators. Only authorized Trusted Role employees are granted access to the secure room. In some instances a visitor may be authorized to enter the secure room. In those cases the visitor(s) will be pre-authorized by the CIO or the Security Office, must present valid identity at the colocation center's front desk and be given a visitor's badge to be worn visibly at all times. At no time is any individual able to gain access or be left alone in the secure room. Two approved, Trusted Role employees will accompany any approved visitors or contractors at all times.

The secure room is required to be under 2-of-M person control at all times when an individual is present in the room. By policy, M is kept to the lowest number of Trusted Role employees that still allows for enough personnel to cover the needs of IdenTrust's diverse customer base. Two-person control is enforced through strict policy and biometric access control authenticators positioned at the entry and exit of the secure room. Both individuals are required to present two-factor authentication including biometrics before gaining entrance to the room. At no time is any individual able to gain access or be left alone in the secure room. Two approved, Trusted Role employees will accompany any other personnel or contractors at all times.

Access to storage safes located inside the IdenTrust Secure Room that contain the ECA cryptographic keys is controlled through separation-of-duties/multi-party control. The cryptographic keys are kept separate from one another in secure bags as well as separate mini-vaults. No single individual can access one or any of the ECA cryptographic keys under these controls. For more information on the controls on the ECA cryptographic keys and their storage, see Appendix G.

All entry and exit from the secure room is logged with the respective times, date, and reason for access. The process for exiting the secure room requires that personnel check

that all physical protection is in place, that all sensitive materials are securely stored, and that the alarms are properly armed.

CA, CSA and RA server equipment is located inside locked computer cabinets within the IdenTrust secure room. Cabinet keys are maintained by the same number of Trusted Role employees who have access to the Secure Room. CA and CSA Cryptographic Modules are secured in the locked computer cabinets within the IdenTrust secure room when in use. When not in use the CA Cryptographic Modules and activation data are stored either in separate safes within the secure room or in the secure off-site facility as described in section 5.1.6.

Security officers review the following on a periodic basis to determine if any secure room access violations have occurred:

- Written access logs;
- Video surveillance tapes; and
- Biometrics logs, which are maintained by IdenTrust Security Officers and are available to Security Officers for review on an as needed basis.

5.1.2.1.2 Disaster Recovery Facility

Disaster recovery hosting facility personnel check the facility twice per eight-hour shift, covering the facility's access points, cameras, and other aspects of a physical walk through. Electronic records of the walkthroughs, including items checked, anomalies found, and the person doing the walkthrough, are kept electronically by the hosting facility, and are kept according to the facility's operating standards. Processes and records are kept for no less than one year and reviewed with external auditors on an annual basis as part of the WebTrust for Certificate Authorities audit.

IdenTrust personnel require pass cards to access the building. Entry to IdenTrust areas within the building also requires pass cards. Pass cards for personnel working in the IdenTrust-controlled areas of the building are granted upon authorization from IdenTrust security officers.

Access to the data processing areas of the building requires two-factor authentication. The secure room is also physically secured and requires two-person control with two-factor authentication including biometrics from each individual. The building is equipped with cameras which cover exterior the room 24x7x365 and is continually monitored by operators. The room is also equipped with a video camera system monitored by IdenTrust Trusted Role personnel during operations. Only previously authorized Trusted Role employees are granted access to the secure room. Each Trusted Role employee's authorization is granted and preregistration in the secure room security system is performed using the same procedures as listed in the section 5.1.2.1.1 for the primary facility's secure room. In some instances a visitor may be authorized to enter the secure room. In those cases the visitor(s) will be pre-authorized by the CIO or the Security Office, must present valid identity at the colocation center's front desk and be given a visitor's badge to be worn visibly at all times. At no time is any individual able to gain access or be left alone in the secure room. Two approved, Trusted Role employees will accompany any approved visitors or contractors at all times.

Within the secured room the following equipment is kept:

CA, CSA and RA server equipment is located inside locked computer cabinets within the IdenTrust secure room. By policy, access to computer cabinet keys are for persons authorized by the Security Office and the CIO only and this number is kept at a minimum number of persons necessary for proper maintenance of the system.

CA, CSA, and other keys are kept separate and accessed under two-person control by IdenTrust personnel at this facility (including the module and PIN Entry Device ("PED") keys which are stored separately in the same manner as described in section 5.1.2.1.1). The security controls and locations of each of these keys stored at this facility are described in Appendix G.

5.1.2.2 Physical Access to RA room

RA client-side equipment is located in a building separate from the CA site. The equipment is stored in a building not identified as housing IdenTrust equipment in a publicly visible way. The entryways and passageways for the building where the RA equipment resides are monitored and recorded by video camera 24 hours a day. IdenTrust's security officers perform periodic checks and review 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 type of checks performed, the time, and the person who performed them. Records are kept for no less than one year and reviewed with external auditors on an annual basis as part of the WebTrust for Certificate Authorities audit.

IdenTrust personnel require pass cards to access the building and the RA room. Pass cards for personnel working in IdenTrust's offices are granted upon authorization from IdenTrust security officers based on the employee's Trusted Role and subsequent access needs to perform that role. 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 RA room after properly identifying themselves and their purpose for the visit. Visitors are not allowed to roam without escorts.

RA client equipment is located in an isolated and restricted-access room in the second floor of the building. Three layers of security surround the RA client equipment: external building doors with restricted access based on either pass card access or under receptionist/security guard surveillance during normal business hours; internal floor door with restricted access controlled by pass card; and the RA room door with further restricted, card-based access only granted to employees with a role requiring access to that room (Help Desk Representatives, Authorized RAs, and other roles as deemed fit by IdenTrust).

All entry to the RA Room is logged with the respective times and date of access.

Cryptographic Modules used to access RA workstations require activation data that is memorized and never written down. When not in use, modules are locked or under control of its primary user.

5.1.3 Power and Air Conditioning (Environmental Controls)

5.1.3.1 Primary Facility

The facility housing the IdenTrust CMA equipment is supplied with air conditioning and power that is sufficient to provide a reliable operating environment. The following controls are in place to ensure that sufficient power is available to have a graceful shutdown and complete pending actions before lack of power causes a shutdown:

Under normal conditions, the building has ready access to two electrical power public substations and two conduit entrances.

In case of public power failures, a full battery backup and a diesel generator with a 4,000-gallon fuel tank for tertiary power redundancy are available. The uninterruptible power supply ("UPS") provides temporary power for the facility and automatically activates the generator when a power failure is detected. The fuel tank can be refueled on the go for continuous service. This system is tested under load weekly.

The Secure Room (where the IdenTrust ECA system is located) is humidity and temperature controlled by an HVAC environmental system and is kept within 2 degrees of 72 F. The relative humidity is maintained within 10% of 35%.

Monitors for the environmental protection of equipment are located in the building Control Room and display the current status of the Secure Room environment. Operators receive visual and audible alarms when a problem is detected.

5.1.3.2 Disaster Recovery Facility

The disaster recovery facility housing the IdenTrust CA, CSA and RA equipment is supplied with air conditioning and power that is sufficient to provide a reliable operating environment. The following controls are in place to ensure that sufficient power is available to have a graceful shutdown and complete pending actions before lack of power causes a shutdown:

In the event of a major power outage the datacenter is equipped with a dual battery powered un-interruptible power supply system. These power supply system are adequate to provide power the datacenter until the generator is delivering power.

A full battery backup and a diesel generator for tertiary power redundancy are available. The generator can be refueled on the go for continuous service.

The datacenter where the secure room is located contains 10 HVAC units that control temperature keeping it within 2 degrees of 70 F. The relative humidity is maintained within 2% of 40%.

5.1.4 Water Exposures

5.1.4.1 Primary Facility

To mitigate the risks of water damage, multi-user computers and communications facilities for the CA and CSA system are housed on the second floor. Equipment sits on a raised floor standing 18" above the concrete flooring. No water lines exist within the

ceiling or overhead in any way. All environmental equipment, such as cooling units, is located around the outside perimeter of the datacenter. Restroom facilities are not located directly above the areas hosting ECA systems.

A braided cable is located below the floor and is capable of detecting the smallest amount of water and alerting, via an annunciation panel, the datacenter operations staff.

The IdenTrust Secure Room fire suppression provides non-liquid oxygen evacuation to stifle combustion. The only water threat to systems is humidity control equipment that employs a water-based environmental maintenance system. The water leads and piping for this equipment are below a raised floor, protecting the computational equipment, and behind a 4-inch concrete reservoir with leak detection strips, isolating under-floor wiring from potential plumbing hazards.

5.1.4.2 Disaster Recovery Facility

In the disaster recovery facility, equipment sits on a 24" raised antistatic flooring. All HVAC adjacent areas are monitored with moisture sensors. Braided moisture sensing cable is installed in areas that pose a risk to moisture.

5.1.5 Fire Prevention and Protection

5.1.5.1 Primary Facility

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.
- Intergen (inert noble gas) fire suppression in the Secure Room.
- 24x7 onsite operators with fire control console/panel access.
- Seismic separation between the Secure Room and office space also serves as an interstitial gap to thwart fire spread.

In addition, computer rooms (such as the Secure Room where the IdenTrust ECA system is housed) are equipped with riot doors, fire doors, and other doors resistant to forcible entry.

A description of IdenTrust's disaster recovery plan in the event a fire disaster should occur is described in section 5.7.4.

5.1.5.2 Disaster Recovery Facility

The disaster recovery facility offers the following features for fire prevention and protection:

- 24x7 onsite operators with fire control console/panel access.
- Dual action, pre-action dry pipe system.
- Certified computer room smoke detection system.

5.1.6 Media Storage

Sensitive ECA information (including audit and archive data) written to magnetic tape, hardware Cryptographic Modules, or other storage media, is stored at an off-site location situated inside a solid granite mountain. This facility was specifically constructed and dedicated solely to vital records and information protection. The vault is designed to be unaffected as a result of floods, earthquakes, fires, and man-made disasters.

The storage vault is constructed of cement, steel and solid granite. Environment-related storage mechanisms include but are not limited to constant temperature and humidity, air circulation and filtration, prohibited storage of flammable items, ionization detectors, fire extinguishers, and independent power sources. The entrance is protected by three (3) separate security gates and a 12,000 pound vault door.

There is only one point of ingress and egress for the facility and for the vault proper. Any attempt to use explosives to force the gates and vault door would be detected by heat detectors and seismic sensors that terminate in an alarm system. Mantraps, card readers and sign-in logs are utilized for physical access control and auditing.

An armed security force supports the vault. It is also under 24-hour electronic surveillance, and it is regularly patrolled by local law enforcement in off-hours. An armed guard escorts all persons entering the facility and the vault area proper. All access to the vault requires 24-hour advance notice.

Records are maintained in a temperature and humidity controlled environment and the vault meets or exceeds all federal requirements for archival storage.

Some ECA sensitive information, such as security audit logs and other audit materials, are stored in a separate area within the vault and are restricted to IdenTrust's Security Officer. These logs are stored on non-rewriteable format (CD-ROM/DVD-ROM) within tamper evident bags and tracked via custody records including a documented matrix of individuals and departments involved with the equipment used in the process.

Backup copies of PKI materials, including CA and CSA hardware Cryptographic Modules and activation data, are stored locally within safes within IdenTrust's secure room. In addition to the restricted access to the datacenter facility and even tighter restrictions for access to the secure room, the safes are also tightly controlled and require both a key and a PIN to access them. All removal or additions to the safes are tracked with logs requiring two Trusted Role employees to sign them acknowledging such actions. Cryptographic materials and activation data are contained in different safes.

Tertiary copies of CA Cryptographic Modules and activation data are also stored in the offsite location, but they have unique procedures to ensure segregation between the backup tapes and CA Cryptographic Modules and activation data. The procedures include shipment within mini safes and storage at the secure offline storage facility of an interior vault that is isolated from the storage for backup tapes.

Shipment to and from the off-site location is conducted via bonded couriers to limit who has access to materials stored there.

IdenTrust adheres to a strict "clean desk" policy by which all hardcopy sensitive ECA information is locked in file cabinets, desks, safes, or other furniture. Likewise, all computer media (such as floppy disks, tapes, or CD-ROM's) containing sensitive ECA

information is locked in similar enclosures when not in use or when not in a clearly visible and attended area.

5.1.7 Waste Disposal

After it is no longer needed, all sensitive ECA information is securely destroyed using procedures that are approved by the Security Officer and are consistent with the ECA CP requirements outlined below. Employees are prohibited from destroying or disposing of potentially important ECA records or information without specific advance management approval.

All outdated or unnecessary copies of printed ECA sensitive information are shredded or disposed of in a secure waste receptacle that is shredded on-site by a bonded company that specializes in disposing of sensitive information.

When sensitive ECA information is erased from a disk, tape, or other magnetic storage media, the erasure is followed by a repeated overwrite operation that prevents the information from later being scavenged. This method is known as "secure delete." Because it is not sufficient simply to "erase" files from computer magnetic storage media, approved secure delete programs are used. Alternatively, degaussers, shredders, or other equipment approved by the Security Officer are employed.

The Security Officer is contacted for assistance in disposing of media and equipment no longer being used by the ECA system. 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. This would include being stored in a safe within the IdenTrust secure room that is under separation-of-duties/multi-party control. *See* section 5.1.2.1.1.

Hardware Cryptographic Modules remain in locked safes within the secure room; sensitive backup tapes remain in the off-site 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, but are not limited to:

- Incineration of Cryptographic Modules;
- Crushing of Cryptographic Modules;
- Shredding of magnetic tapes; and
- Shredding of paper.

5.1.8 Off-site Backup

The ECA system is backed up at the primary facility in Utah, using industry-standard commercial software. These system backups provide the capability to recover from a system failure. Incremental backups are performed daily. Full system backups are performed every weekend. Backups are sent to an off-site, hardened, secure, mountain storage vault described in section 5.1.6.

At least annually, backup tapes are consolidated and archive media is identified and stored in the off-site storage vault described in earlier in the section and in section 5.1.6 to satisfy the 10 1/2 year data retention schedule.

Components needed to restore the ECA system are stored in separate areas of the secure vault facility, see section 5.1.6. The most sensitive material, including CA Cryptographic Modules and activation materials, and password copies, are stored in separate mini-vaults. Each module resides within controlled security bag, secured separate from each other in the safes and the combinations to the mini-vaults are solely under IdenTrust control. These controls include required two-person control by IdenTrust personnel to access each mini-vault. Different groups are authorized to access different safes, each containing a different key (PIN, PED, etc.), depending upon the material and its relevancy to the group accessing the materials. No single individual can access any of the keys. The controls of these keys are the same as described in Appendix G in sections 5.1.2.1.1 and 5.1.2.1.2. Other materials are locked in metal boxes with no external hinge and secured with two locks, with keys maintained under IdenTrust's normal two-person control procedures. Box labeling is generic not to reveal their contents.

Only those IdenTrust employees in Trusted Roles, and only with a need-to-know status, as authorized by the Vice President of Operations or CIO, are authorized access to the off-site storage facility. In cases where a request is made to deliver backup material to IdenTrust facilities, the request is verified by a member of the Security office, the Vice President of Operations, or the CIO and is different than the Requestor. Two Trusted Role employees, upon identification, receive any delivery of PKI materials such as Cryptographic Modules and PED keys.

5.2 Procedural Controls

5.2.1 Trusted Roles

All employees, contractors, and consultants of IdenTrust who have access to or control over ECA cryptographic operations that may materially affect the issuance, use, revocation of Certificates, including access to restricted operations of ECA systems shall, for purposes of this CPS, be 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 ECA operations. The functions and duties performed by these persons are also separated and distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI (see sections 5.2.2 and 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.

Prior to assigning any IdenTrust personnel to a Trusted Role that person must be identified as such to the IdenTrust Human Resource department and approved and authorized by the senior manager over the division, which includes Operations Management, Professional Services Management and the CEO. The Human Resource department maintains lists of all persons filling Trusted Roles, including name of person, position they are serving in and their contact information, information and for audit

purposes, the Vice President of Operations and Security Officer have an up to date copy of the list. This list will be made available during a compliance audit:

- CA Administrator,
- RA Operator,
- System Administrator,
- Network Engineer,
- Security Officer,
- Help Desk Representative; and
- Operations Management Personnel.

5.2.1.1 Certification Authority (CA)

All Certificates issued under the IdenTrust ECA Certificate Policy are issued by the IdenTrust ECA, operating under the control of the IdenTrust Operations Management. The responsibilities for the Certification Authority functions are carried out by IdenTrust employees acting in their Trusted Roles.

The CA Administrator is a Trusted Role defined by IdenTrust. The IdenTrust CA Administrator's roles, 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 only);
- Configuration of CRL parameters;
- Configuration of Certificate Profiles;
- Key Pair generation and seeking the certification of the new public key by the ECA Root CA;
- Activation of CA private key;
- Hardware Cryptographic Module management (performed under two-person control); and
- Generation of keys and Certificates used by RA software applications and distribution of activation data for hardware Cryptographic Modules holding RA keys.

IdenTrust will maintain redundancy in the role of CA Administrators. Multiple CA Administrators are maintained in case a primary CA Administrator is on vacation, sick leave, etc.

These roles maintain strict separation-of-duties/multi-party control and management approval is required prior to use and access of key materials. All such controls are audited annually by a third party auditor as part of the AICPA/CICA WebTrust Program for Certification Authorities, in compliance with the ISO/ANSI X9.79 PKI Practices and Policy Framework standard. IdenTrust also performs Registration Authority functions. The responsibilities fall on a Registration Authority Operator (RA Operator) explained in the following section.

5.2.1.2 Registration Authority ("RA")

The RAs operating under the ECA policy are subject to the stipulations of the ECA CP and this CPS. The responsibility for RA operations within IdenTrust is carried out by employees acting in Trusted Roles.

RA Operator is a Trusted Role defined by IdenTrust. IdenTrust Operators are required to comply with the practices pertinent to their functions in this CPS. IdenTrust RA Operator's roles, responsibilities and operating procedures, as they relate to RA operations, are as follows:

- Verifying identity, either through personal contact or via review and approval of documents submitted by notaries or Trusted Correspondents;
- Entering Subscriber information, and verifying correctness;
- Securely communicating requests to and responses from the ECA;
- Receiving and distributing Subscriber Certificates;
- Authentication of Subscriber identity (upon revocation request);
- Archival of Subscriber authentication information (i.e., copies of paper forms, etc.);
- Approval by the RA to the CA of Subscriber Certificate requests;
- Approval by the RA to the CA of Subscriber revocation requests;
- Operation of the RA system; and
- Management of the RA Operator Cryptographic Module.

Controls are in place such as approvals for deviation from established Identification & Authentication (I&A) procedures, for example. Deviations from established policies and procedures require approval from Operations Management and the Risk Management Committee roles prior to such deviations and no deviations will be permitted that are in conflict with the ECA CP. All such controls are audited annually by a third party auditor as part of the AICPA/CICA WebTrust Program for Certification Authorities, in compliance with the ISO/ANSI X9.79 PKI Practices and Policy Framework standard.

5.2.1.3 Certificate Status Authority ("CSA")

IdenTrust, as a CSA that operates under the ECA policy is subject to the stipulations of the ECA CP and of this CPS. The responsibilities for the CSA functions are carried out by IdenTrust employees acting in Trusted Roles.

The CA Administrator is the Trusted Role within IdenTrust to carry out the CSA responsibilities. The IdenTrust CA Administrator's roles, responsibilities and operating procedures, as they relate to CSA Operations, are 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
- Operation of the CSA equipment

Furthermore, IdenTrust CSA functionality is provided through an OCSP Responder that provides revocation statuses. The responses are signed using private keys and algorithms consistent with section 6.1.5 that support authentication and integrity at the assurance level of the Certificate being validated or higher.

IdenTrust will manage its ECA CSA systems and equipment following the procedures outlined herein for its Certification Authority.

5.2.1.4 Other Trusted Roles

IdenTrust defines several other Trusted Roles for employees performing functions related to the operation of the CMA.

5.2.1.4.1 System Administrator

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.

Controls are in place requiring the approval for root level access or other such access from the Security Officer or Operations Management prior to such access being granted. All such controls are audited annually by a third party auditor as part of the AICPA/CICA WebTrust Program for Certification Authorities, in compliance with the ISO/ANSI X9.79 PKI Practices and Policy Framework standard.

Segregation of duties between System Administrators and CA Administrators is further enforced separating the CA servers' root-level access and administrative passwords for the CA. Without the cooperation of both administrators, IdenTrust software is inoperable for purposes of processing requests, generating responses, generating Certificates and CRLs, re-keying and designation of RA Operators (see sections 5.2.2 and 5.2.4).

5.2.1.4.2 Network Engineer

Network Engineers are responsible for:

- Initial installation and configuration of the network routers and switching equipment, configuration of initial host and network interface;
- Installation, configuration, and maintenance of firewalls, domain name services ("DNS"), and load balancing appliances;
- Creation of devices to support recovery from catastrophic system loss; and
- Changing the host or network interface configuration.

Controls are in place, for example, approvals for changes to firewall rules are required by the Security Officer or Operations Management roles prior to implementation by a Network Engineer. All such controls are audited annually by a third party auditor as part of the AICPA/CICA WebTrust Program for Certification Authorities, in compliance with the ISO/ANSI X9.79 PKI Practices and Policy Framework standard.

5.2.1.4.3 Security Officer

The Security officer is 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. 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 or IdenTrust databases;
- Receipt of improper messages;
- Suspicious modifications;
- Internal auditing and assessment;
- 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.

5.2.1.4.4 Help Desk Representative

Help Desk Representatives perform the following duties:

- Troubleshooting of Certificate lifecycle events problems;
- Providing Subscriber account information; and
- Initiating key recoveries and revocation processes.

5.2.1.4.5 Operations Management Personnel

A list of IdenTrust's Operations Managers (i.e., IdenTrust's VP of Operations and other Operations designees below the VP of Operations), is kept at all times as approved and authorized by the Chief Operating Officer ("COO"), Chief Information Officer ("CIO") or Chief Executive Officer ("CEO"). Operations Management role performs the following duties:

- Provides Internal Audit oversight, and working closely with external auditors as needed;
- Handles approval/removal of Network, System and CA administrators as well as Help Desk Representatives and RA Operators;
- Acts as custodian of the activation data for the Certificate that administers the Certification Authority 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.

5.2.1.4.6 Trusted Correspondent

The identity of a Trusted Correspondent is confirmed through the same steps used for issuance of an ECA Certificate to the Trusted Correspondent at an assurance level equal to or higher than the Certificates for which the Trusted Correspondent will act as Registrar (section 3.2.3.1.1). This role is further described in section 1.3.2.1.

5.2.1.4.7 PKI POC

The identity of a PKI POC is confirmed through the same steps used for issuance of an ECA Certificate to a Subscriber of, at least, Medium Assurance level (section 3.2.3). This role is further described in section 1.3.5.2.

5.2.2 Number of Persons Required for Task

IdenTrust has procedural and operational mechanisms in place to ensure that no single individual may perform sensitive CA activities alone. These mechanisms apply principles of separation-of-duties (see section 5.2.4 below) and require the actions of multiple persons to perform such sensitive tasks as:

- Handling of CA keys throughout the entire CA key lifecycle from generation and activation, into secure storage, through to eventual destruction;
- Non-automated (manual) Certificate issuance processes; and
- Physical and logical access to CA Cryptographic Modules.

See Sections 5.1.2.1 and 6.2.2. Persons with access to CA Cryptographic Modules do not have access to the activation data needed to operate them. Generation, backup, or activation of the CA Certificate signing private key requires the actions of at least two individuals, one of whom is a CA Administrator and who may not be a Security Officer.

5.2.3 Identification and Authentication for Each Role

The physical identity vetting of IdenTrust personnel in Trusted Roles is 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. In accordance with IdenTrust's security policies, IdenTrust's 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 any component of the CA system.

Each of these access methods (i.e. Certificates and system accounts) are: (i) directly attributable to the trusted individual; (ii) password/account 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. CA operations cannot be accessed outside of the secure room through remote access or a shared network.

5.2.4 Roles Requiring Separation of Duties

IdenTrust employees are assigned specific roles for the ECA system. As explained in previous sections, IdenTrust will utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards.

Roles requiring separation of duties include (but are not limited to):

- **CA/CSA Administrator.** No person participating as IdenTrust CA Administrator will assume the role of RA Operator, Security Officer, Help Desk Representative, or Operations Management.
- **RA Operator.** An RA Operator may not serve in a CA Administrator, System Administrator, Network Engineer, Security Officer, or management oversight role (Operations Management, Human Resources, or Executive Management).
- **System Administrator.** A System Administrator may not assume the RA Operator, Security Officer, Help Desk Representative, or Operations Management role.
- **Network Engineer.** The Network Engineer may not assume the RA Operator, Security Officer, Help Desk Representative, or Operations Management role.
- **Security Officer.** The Security Officer may not serve in the roles of CA Administrator, RA Operator, Systems Administrator, or Network Engineer
- **Help Desk Representative.** Help Desk Representatives may not serve in the role of CA Administrator, System Administrator, or Network Engineer
- **Operations Management Personnel.** The Operations Management may not serve as CA Administrator, Systems Administrator, RA Operator, or Network Engineer.

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.

Additional Separation-of-Duties/Multi-Party Control and Split Knowledge information are addressed in section 5.2.1.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

All personnel for any Trusted Role, as described in section 5.2.1, are selected on the basis of loyalty to the United States, their trustworthiness and integrity. All persons that are Trusted Role employees are U.S. citizens with the exception of PKI POCs and Trusted Correspondents. Trusted Correspondents are U.S. Citizens unless qualified for the allowances listed in section 11.3. While operating as an ECA, all CA Administrators or RA Operators must be under the direct control of IdenTrust.

ECA Operations are administered by the IdenTrust's Operations Management as identified in sections 1.3.1.5 and 5.2.1.4.5. The personnel and equipment for an ECA installation are within the administrative control of the Operations Management group. Personnel appointed to operate CMA equipment meet the following requirements:

- Have successfully completed an appropriate training program as evidenced by Certificates of completion issued by the facility providing training;
- Have demonstrated the ability to perform their duties as indicated by annual performance reviews;
- Appear trustworthy as initially determined by security clearance or background investigation;

- Have no other duties that would interfere or conflict with their duties as a CMA;
- Have not knowingly been previously relieved of CMA or other trusted duties for reasons of negligence or non-performance of duties as indicated by employment records;
- Have not knowingly been denied a security clearance, or had a security clearance revoked as indicated by an inquiry to the Defense Security Service (DSS);
- Have not been convicted of a felony offense as indicated by a criminal background check; and
- Are appointed in writing by the Operations Management or be party to a contract for PKI services as evidenced by records maintained for such purpose by IdenTrust.

5.3.2 Background Check Procedures

Individuals filling any of the Trusted Roles identified in section 5.2.1 should be trustworthy and of highest integrity. These persons are subject to a thorough background check by a qualified investigator, initiated by IdenTrust Human Resources. The IdenTrust's Human Resources Department engages an outside Third-Party Consumer Reporting Agency to conduct these background checks. The results of these background checks are reviewed by IdenTrust's Resource Department to confirm the results and follow up with the Third-Party Consumer Reporting Agency for any inconsistencies or findings based on the list below. If inconsistencies or discrepancies are found, they are evaluated by Human Resource Department management or escalated the Risk Management Committee to determine the best course of action. These results are handled in an equivalent manner to the standards required in the United States Executive Order 12968, or equivalent. Background checks are kept confidential and are not released except as described in section 9.4 and to the employee who is the subject of the background check at their request.

The background check includes the following items and covers the past seven years:

- A criminal history check is performed through a commercial database and shows no misdemeanor or felony convictions;
- A credit history check is performed through a commercial database and shows that person has not committed any fraud and is financially trustworthy;
- Previous employers are contacted and demonstrate that the person is competent, reliable and trustworthy;
- Professional references demonstrate that the person is competent, reliable and trustworthy;
- High schools, colleges and universities are contacted to verify the highest or most relevant degree; and
- A Social Security trace is performed to determine whether the person has a valid social security number. This check is required only if the country in which the duty is performed has social security number or similar identifier.

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 the ECA computer system. All operative personnel receive appropriate security briefings upon arrival and before beginning their assigned duties.

Security awareness and training programs are developed and implemented in accordance with Federal laws, regulations, and guidelines and ECA security policy and supporting security guidelines.

The following topics are covered in training: operation of IdenTrust software and hardware, operational and security procedures, the stipulations of this CPS and other policies and procedures germane to the operation of a Certification Authority. The specific training required will depend on the equipment used and the personnel selected. Details concerning the procedures and specific vendor manuals for the platform, CA application and Cryptographic Modules that personnel are given to perform their roles can be found in the IdenTrust ECA Operations Manual.

IdenTrust maintains a file that contains signed and dated records from IdenTrust personnel listing their names, roles, training received, and date that training was completed.

Specific areas that are covered for each Trusted Role are outlined below:

CA Administrator:

Any employee serving in the CA Administrator role will be trained in the following areas:

- Sub CA generation (including Key Pair generation and seeking the certification of the new public key by the ECA Root CA), re-keying and revocation;
- Configuration and posting Certificates and CRLs;
- Performing any required daily maintenance or other CA-related administrative functions; and
- Hardware Cryptographic Module configuration and programming.

RA Operator:

Any employee serving in the RA Operator role will be trained in the following areas:

- Verifying identity, either through personal contact or through Trusted Correspondents;
- Entering user information and verifying correctness;
- Securely communicating requests to and responses from CAs; and
- The Certificate issuance process.

System Administrator:

Any employee serving in the System Administrator role will be trained in the following areas:

- Operating systems and software applications used within the ECA system;

- Backup applications and procedures;
- Use of database tools including reporting and maintenance;
- Restriction for privileged system use; and
- Generation of audit data.

Network Engineer:

Any employee serving in the Network Engineer role will be trained in the following areas:

- IdenTrust Network architecture and equipment;
- Proper secure network and switching configuration; and
- Privacy requirements for network transmissions, and intrusion detection monitoring.

Security Officer:

Any employee serving as Security Officer or in the security auditing role will be trained in the following areas:

- Security risk assessment and analysis;
- Security policies and guidelines;
- Logging and auditing;
- Physical security;
- Computer attack trends and vulnerabilities;
- Network and distributed systems trust relationships;
- Open PKI and cryptosystems;
- Firewalls;
- Incident response and contingency; and
- Access, physical controls and security threats.

Help Desk Representative:

Any employee serving in the Help Desk Representative role will be trained in the following areas:

- Proper secure handling of sensitive customer information; and
- Trouble tracking software.

Operations Management Personnel:

Any employee serving in the Operations Management role will be trained in audit oversight and risk management fundamentals.

5.3.4 Retraining Frequency and Requirements

Those involved in filling Trusted Roles will be aware of changes in IdenTrust's CMA operations. Any significant change to the IdenTrust CMA operation will require retraining. Through IdenTrust's change control process (see section 6.6), an awareness plan is prepared for any significant change to the CMA system (e.g., a planned upgrade of CMA equipment or software). IdenTrust's Human Resources Department maintains a file of signed and dated statements from IdenTrust personnel listing their names, roles, re-training received, and date training completed.

All trusted personnel undergo a retraining session every twelve (12) months that includes a review of the applicable provisions of the ECA CP and IdenTrust ECA CPS under which they are operating and a review of applicable policies and procedures (including those that affect the IdenTrust ECA system).

5.3.5 Job Rotation Frequency and Sequence

Job rotation is implemented when in the judgment of Operations Management, it is necessary to ensure the continuity and integrity of the CA, CSA, and RA's ability to continually provide robust PKI-related services.

5.3.6 Sanctions for Unauthorized Actions

Failure of any employee or agent of IdenTrust to comply with the provisions of the ECA CP or this CPS, whether through negligence or with malicious intent, will subject such individuals to appropriate administrative and disciplinary actions, which may include termination as an agent or employee of IdenTrust and possible civil and criminal sanctions.

Any employee performing a Trusted Role who is cited by IdenTrust management for unauthorized actions, inappropriate actions, or any other unsatisfactory investigation results are immediately removed from the Trusted Role pending management review. Subsequent to management review, and discussion of actions or investigation results with employees, employees may be reassigned to their positions, transferred to non-Trusted Roles, or dismissed from employment as appropriate.

5.3.7 Independent Contractor Requirements

All IdenTrust subcontractors providing services for the ECA Program are required to perform in accordance with the ECA CP and this CPS and the contract between IdenTrust and the contracted entity. All subcontractor personnel are subject to all personnel requirements of this CPS, including the ones described elsewhere in this section 5.3. IdenTrust supplies its contracting personnel with documentation sufficient to define duties and procedures for each role will be provided to the personnel filling that role.

5.3.8 Documentation Supplied to Personnel

In accordance with the IdenTrust ECA Operations Manual, personnel filling the roles of CA Administrator, RA Operator, System Administrator, Network Engineer, Security Officer, Help Desk Representative, Operations Management will be provided (have in their possession or have access to) documentation defining the duties and procedures of such roles. The information will be available in print or on-line. Informational material will be derived from several sources, including but not limited to existing internal IdenTrust documentation, system and software documentation, discipline-specific books, treatises and periodicals, and information developed by or supplied to IdenTrust during the course of performance of ECA operations.

5.4 AUDIT LOGGING PROCEDURES

IdenTrust equipment supporting CMA activities records, for purposes of security audit, events as described below, whether the events are attributable to human action (in any role) or are automatically invoked by the equipment. IdenTrust equipment includes CA, RA and CSA equipment used to register Subscribers or generate, sign and manage Certificates and provide revocation information.

IdenTrust Security Officers maintain a separate logging server that records all CA, CSA, RA and Network audit events. These events are written to the local systems as well as to the Security Officers' logging server. The audit logging server is housed in the same facility and has the same physical, computer security, life cycle, and network controls as those listed in section 5.1, 6.5, 6.6 and 6.7. Only appointed IdenTrust Security Officers have access to the audit logging server. These logs are examined for anomalies, completeness and accuracy, through manual and automated tools.

5.4.1 Types of Events Recorded

The events recorded may be attributable to human intervention or automatically invoked by the machine.

At a minimum, the information recorded includes the type of event, the time the event occurred and who and/or what caused the event. In addition, for some types of events it may be appropriate to record the success or failure, the source or destination of a message, or the disposition of a created object (e.g., a filename). Where possible, the audit data is automatically collected; when this is not possible, a logbook or other physical mechanism is used. These logbooks and paper documentation are secured within locked cabinets or secure rooms and managed by the Security Office. The documents are converted to a digital medium to be included with the other digitally logged events discussed in the table below.

IdenTrust systems require identification and authentication at system logon with unique user name and password (or cryptographic key). The accessing of systems, equipment and applications is logged to establish the accountability of system operators who initiate system actions.

All security logs, both electronic and non-electronic, are retained in accordance with requirements of section5.4.3 and will be made available during compliance audits.

Auditable Event	CA	CSA	RA	RAO*
SECURITY AUDIT				
Any changes to the audit parameters, e.g., audit frequency, type of event audited - The operating system and applications automatically record modifications made to audit parameters; including date and time of modification, type of event, success or failure indication and identification of user making modification;	X	X	X	N/A

Auditable Event	CA	CSA	RA	RAO*
Any attempt to delete or modify the audit logs - The operating system automatically records all attempted modifications made to security audit configurations and files, including date and time of modification, type of event, success or failure indication and identification of user making modification.	X	X	X	-
IDENTITY PROOFING	**CA**	**CSA**	**RA**	**RAO**
Successful and unsuccessful attempts to assume a role – The operating system and applications automatically record: date and time of attempted login, username asserted at time of attempted login, and success or failure indication, are automatically logged by the CA, CSA and RA.	X	X	X	N/A
The value of maximum number of authentication attempts is changed - date and time, type of event, and identification of user making modification are logged automatically by the operating system logging facility. Changes in configuration files, security profiles and administrator privileges are logged through a combination of automatic and manual logging. All changes are manually logged through change management procedures.	X	X	N/A	N/A
Maximum number of authentication attempts occur during user login - date and time of attempted login, username asserted at time of attempted login, and failure recorded automatically by the operating system and application audit logs.	X	X	N/A	N/A
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts - date and time of event and identification of account holder and administrator are logged automatically by the operating system.	X	X	N/A	N/A
An administrator changes the type of authenticator, e.g., from a password to a biometric - date and time, type of event, and identification of user making modification are logged automatically by the operating system and manually through change management procedures. Changes in configuration files, security profiles and administrator privileges are logged through a combination of operating system and manual change management procedures.	X	X	N/A	N/A

Auditable Event	CA	CSA	RA	RAO*
LOCAL DATA ENTRY	**CA**	**CSA**	**RA**	**RAO**
All security-relevant data that is entered in the system – the system records the identity of the local operator performing local data entry so that the accepted data can be associated with the operator in the audit log.	X	X	X	N/A
REMOTE DATA ENTRY	**CA**	**CSA**	**RA**	**RAO**
All security-relevant messages that are received by the system - date and time, digital signature/authentication mechanism, and message are automatically logged by the application.	X	X	X	N/A
DATA EXPORT AND OUTPUT	**CA**	**CSA**	**RA**	**RAO**
All successful and unsuccessful requests for confidential and security-relevant information - date and time of attempted access, username or identity asserted at time of attempt, record of success or failure, logged through a combination of automatic and manual logging. Manual logging by Security Team also collects name of person reporting the event and resolution.	X	X	X	X
KEY GENERATION	**CA**	**CSA**	**RA**	**RAO**
Whenever a component generates a key (not mandatory for single session or one-time use symmetric keys) – CA system automatically records all significant events related to CA operations, including key generation and Certificate signing. Additionally, manual and audiovisual records of CA and CSA key generation are created. RA key and Certificate generation events are automatically recorded by the CA system.	X	X	-	-
PRIVATE KEY LOAD AND STORAGE	**CA**	**CSA**	**RA**	**RAO**
The loading of Component private keys – A manual log of all physical access to production CA and CSA HSMs is maintained by IdenTrust, and the log records action taken, date and time action was taken and name of person who performed action. A separate record of authorization to access HSMs is also maintained which specifies date, time, reason for access and name of authorizing person.	X	X	N/A	N/A

Auditable Event	CA	CSA	RA	RAO*
All access to Certificate subject Private Keys retained within the system database for key recovery, backup and restore purposes – Date, time, messages between the CA and the requesting component and indicator of success or failure are automatically logged.	X	N/A	N/A	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE	**CA**	**CSA**	**RA**	**RAO**
All changes to the trusted component public keys, including additions and deletions are automatically logged through the applications and manually through IdenTrust's change management process and access authorization forms.	X	X	X	-
SECRET KEY STORAGE	**CA**	**CSA**	**RA**	**RAO**
The manual entry of secret keys used for authentication – Use of secret keys (PED Keys) for access to the CAs and CSAs' HSMs is recorded manually at the time of Cryptographic Key use and the log records action taken, date and time action was taken and name of person who performed the action. A separate record of authorization to access HSMs is also maintained which specifies date, time, reason for access and name of authorizing person.	X	X	N/A	N/A
PRIVATE AND SECRET KEY EXPORT	**CA**	**CSA**	**RA**	**RAO**
The export of private and secret keys (keys used for a single session or message are excluded) - private and secret key export involving the CA's HSM take place in accordance with the principles of Separation of Duties/Multi-party Control stated in Section 5.2.4. At the time of export a manual log records the action taken, date and time the action was taken, and name of person who performed the action. Separate records of access to HSMs are also maintained that specify the date, time, reason for access, and name of authorizing person.	X	X	N/A	N/A
CERTIFICATE REGISTRATION	**CA**	**CSA**	**RA**	**RAO**
All Certificate requests – date and time of request, type of event, and request information are automatically logged by the application.	X	N/A	X	X
CERTIFICATE REVOCATION	**CA**	**CSA**	**RA**	**RAO**

Auditable Event	CA	CSA	RA	RAO*
All Certificate revocation requests – date and time of revocation request, sender/requester DN, Certificate serial number, subject DN of Certificate to revoke, revocation reason, 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 requests for revocation 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	N/A	X	X
CERTIFICATE STATUS CHANGE APPROVAL	**CA**	**CSA**	**RA**	**RAO**
The approval or rejection of a Certificate status change request - identity of equipment operator who initiated the request, message contents, message source, destination, and success or failure indication are automatically logged by the application.	X	X	X	N/A
COMPONENT CONFIGURATION	**CA**	**CSA**	**RA**	**RAO**
Any security-relevant changes to the configuration of a system component – date and time of modification, name of modifier, description of modification, build information (i.e. size, version number) of any modified files and the reason for modification are manually logged during change management process.	X	X	X	X
ACCOUNT ADMINISTRATION	**CA**	**CSA**	**RA**	**RAO**
Roles and users are added or deleted – date and time, type of event, and identification of user making modification are logged automatically and manually. Changes roles are logged through a combination of automatic and manual logging. All changes are manually logged through change management procedures. Change management records capture date and time and type of change, reason for change of role, and authorization and approval records.	X	X	-	-
The access control privileges of a user account or a role are modified – date and time, type of event, and identification of user making modification are logged automatically and manually. Changes in configuration files, security profiles and administrator privileges are	X	-	-	-

Auditable Event	CA	CSA	RA	RAO*
logged through a combination of automatic and manual logging. All changes are manually logged through change management procedures. Change management records capture date and time and type of change, reason for modification and authorization and approval records.				
CERTIFICATE PROFILE MANAGEMENT (Including both CA and CSA)	**CA**	**CSA**	**RA**	**RAO**
All changes to the Certificate profile - Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	X	N/A	N/A
REVOCATION PROFILE MANAGEMENT	**CA**	**CSA**	**RA**	**RAO**
All changes to the revocation profile - Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	N/A	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	**CA**	**CSA**	**RA**	**RAO**
All changes to the Certificate revocation list profile - Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	N/A	N/A	N/A
MISCELLANEOUS	**CA**	**CSA**	**RA**	**RAO**
Appointment of an individual to a Trusted Role – date of the appointment, name of the appointee and authorizing signature are manually logged.	X	X	X	X
Appointment of an individual to a multi-person Role – date of the appointment, name of the appointee and authorizing signature are manually logged.	X	-	N/A	N/A
Training of individuals in Trusted Roles – date of training, trained individual's name, train topic are manually logged.	X	X	X	X
Installation of the Operating System -date and time of server installation, name of installer, and details of installation process are manually recorded during installation. The automatic security auditing capabilities of the underlying operating system hosting the software are enabled during installation. All changes are also	X	X	X	X

Auditable Event	CA	CSA	RA	RAO*
manually logged through change management procedures.				
Installation of the PKI Application - date and time of installation, name of installer, and details of installation process are manually recorded during installation. All changes are also manually logged through change management procedures.	X	X	X	N/A
Installation of Hardware Security Modules - a manual list of HSMs is maintained, and the list records action taken, date and time action was taken and name of person who performed action.	X	X	X	N/A
Removal of HSMs -- a manual list of HSMs is maintained, and the list records action taken, date and time action was taken and name of person who performed action.	X	X	X	N/A
Acquisition and Destruction of HSMs -- a manual list of HSMs is maintained, and the list records action taken, date and time action was taken and name of person who performed action.	X	X	X	N/A
System Startup – date and time of system startup is automatically logged in the system's event log.	X	X	X	N/A
Logon attempts to PKI Application - CA, RA and CSA application access – date and time of event, type of event, identity of user accessing the system, and success or failure indication are automatically logged by the application.	X	X	X	N/A
Receipt of hardware / software – kept manually in a database that records the hardware and software possessed, licensed or owned.	X	X	X	N/A
Attempts to set passwords – date and time, identity of user, and success or failure indication of attempt to set password is kept automatically by the operating system/application or manually in a password change log.	X	X	N/A	N/A
Attempts to modify passwords – date and time, identity of user, and success or failure indication of attempt to modify password is kept by the operating system/application or manually in a password change log.	X	X	N/A	N/A

Auditable Event	CA	CSA	RA	RAO*
Back up of the internal CA database – date and time of the backup event and location of backup is kept manually in a backup log.	X	-	-	-
Restoration from back up of the internal CA database – date and time of restoration tests is kept in a disaster recovery log.	X	-	-	-
File manipulation (e.g., creation, renaming, moving) – the file system records the identity of the local operator who created or last modified the file so that the creation, renaming or moving of files can be associated with the operator is kept automatically by the operating system audit and logging facility.	X	X	-	-
Posting of any material to a Repository – date and time of posting, transaction identifier and success or failure indication are automatically logged by the application. For CRL generation and publication to directory - date and time of generation, DN of Issuing CA and success or failure of publication of CRL is automatically logged by the application.	X	X	X	-
Access to the internal CA database -- date and time of login, username asserted at the time of attempted login, and success or failure indication, are automatically logged by the database audit log.	X	-	-	-
All Certificate compromise notification requests – date and time of notification, identity of person making the notification, identification of entity compromised, description of compromise are logged manually by the personnel who receive the notification (e.g. Help Desk, RA Operators, etc.) and by RA/RA Operators' system processing logs.	X	N/A	X	X
Loading HSMs with Certificates -- a manual log of all physical access to production CA and CSA HSMs is maintained, and the log records action taken (including transferring keys to or from and backing up the HSMs), date and time action was taken and name of person who performed action. A separate record of authorization to access HSMs is also maintained which specifies date, time, reason for access and name of authorizing person.	X	X	N/A	N/A
Shipment of HSMs – receipt, servicing (e.g. keying or other cryptologic manipulations), and shipping of HSMs is manually recorded for CA, CSA and RA production	X	X	N/A	N/A

Auditable Event	CA	CSA	RA	RAO*
HSMs. Recording contains information regarding action taken, (e.g. return, receipt), date and time action was taken, name of person performing action and reason for action.				
Zeroizing HSMs - a manual list of HSMs is maintained, and the list records action taken, date and time action was taken, name of person who performed action, name and role of person authorizing the action.	X	X	N/A	N/A
Re-key of the Component – CA, CSA and RA systems automatically records all significant events related to their respective operations, including key generation for re-keying. Additionally, manual and audiovisual records of CA key generation are created. RA re-keying and Certificate generation events are also automatically recorded by the CA system.	X	X	X	X
CONFIGURATION CHANGES	**CA**	**CSA**	**RA**	**RAO**
Hardware - All changes are manually logged through change management procedures.	X	X	X	-
Software - All changes are manually logged through change management procedures.	X	X	X	-
Operating System - All changes are manually logged through change management procedures.	X	X	X	-
Patches - All changes are manually logged through change management procedures.	X	X	X	-
Security Profiles - All changes are manually logged through change management procedures.	X	X	X	-
PHYSICAL ACCESS / SITE SECURITY	**CA**	**CSA**	**RA**	**RAO**
Personnel Access to room housing component - a manual recording of physical access to Secure Rooms is maintained through physical logs that include recording of date and time, person accessing the Secure Room, and reason for access.	X	X	-	-
Access to a component (e.g., server, HSM) - logged through a combination of automatic and manual logs based on the type of component and type of access.	X	X	-	-
Known or suspected violations of physical security - any known or suspected violations of physical security – date/time, description of suspected event, name of	X	X	X	-

Auditable Event	CA	CSA	RA	RAO*
person reporting the event and resolution are manually logged by Security Team.				
ANOMALIES	**CA**	**CSA**	**RA**	**RAO**
Software error conditions - date and time of event, and description of event are automatically logged by the application reporting the event or the operating system.	X	X	X	-
Software check integrity failures - date and time of event, and description of event are automatically logged by the application reporting the event or the operating system.	X	X	X	-
Receipt of improper messages - date and time of event, and description of event are automatically logged by the application reporting the event or the operating system.	X	X	X	-
Misrouted messages - date and time of event, and description of event are automatically logged by the application reporting the event or the operating system.	X	X	X	-
Network attacks (suspected or confirmed) - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X	X
Equipment failure - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X	-
Electrical power outages - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X	-
Uninterruptible Power Supply (UPS) failure - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X	-
Obvious and significant network service or access failures - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X	-
Violations of Certificate Policy - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X	X

Auditable Event	CA	CSA	RA	RAO*
Violations of Certification Practice Statement - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X	X
Resetting Operating System clock - date/time, description of suspected event, name of person are automatically logged by the operating systems logging facility.	X	X	X	X

* RAO is RA Operator

5.4.2 Frequency of Processing Log

IdenTrust reviews the audit logs at least once every two months. In order to ensure a thorough review of all data, the Security Officer selects for this review a minimum of 25% of the security audit data generated since the last review for each category of audit data. The Security Officer uses automated tools to scan logs for specific conditions. The Security Officer then reviews the output and produces a written summary of findings. The reviews include date, name of reviewer, description of event, details of findings and recommendations for remediation or further investigation if appropriate. The reviews include CA, CSA, and RA activities.

IdenTrust will make its reviews available to the EPMA and to the compliance auditor in accordance with section 8.6.

Restrictions are applied to the logs to prevent unauthorized access, deletion or overwriting of data. Storage capability is monitored to ensure that sufficient space exists in order to prevent overflow conditions. Alerts are sent to IdenTrust's Security Officer if space available becomes inadequate.

The security audit logs are moved on a monthly basis to archive by IdenTrust's Security Officer in accordance with section 5.4.4.

5.4.3 Retention Period for Audit Log

Audit log information as listed in section 5.4.1 is generated on IdenTrust's ECA equipment and kept on the ECA equipment until it is reviewed by an IdenTrust security officer and he or she archive the information and prepare the archive data to be moved to IdenTrust's the off-site archive facility described in section 5.1.8. This process is conducted on a monthly or as-needed basis when an alert is sent to the security team to indicate storage space is low on the servers that collect this information. IdenTrust also retains an on-site backup record of audit data for a period of time not less than three months.

Electronic audit logs and digital copies of physical manual audit logs are deleted from the security logging server only after they have been reviewed and backed up to archive media. Only Security Officers are authorized to delete these logs from the security

logging server and must first verify that the audit log data has been successfully backed up to archive media.

Before deleting the logs the Security Officer will (i) ensure the integrity of the data, (ii) generate a checksum of the data, (iii) encrypt files (with a passphrase-protected 2,048-bit RSA key and 256-bit AES-CBC), and (iv) record the checksum and write the checksum and data in ISO 9660 format to a CD-ROM. By following these procedures the Security Officer ensures that the data is properly backed up prior to deletion of the original log file and the information is secured for transport to the archive. The assigned Security Officer will make arrangements to transport the CD-ROM to IdenTrust for archival and EPMA audits.

5.4.4 Protection of Audit Log

The security audit logs are automatically written in real-time locally and to a separate audit log server (located physically on the same network segment) via the operating system/application logging facilities of those systems or applications. IdenTrust Security Officers are the system administrators of the security audit log servers. The security audit logs, once generated, are not open for reading by any human, or by any automated process other than IdenTrust Security Officers performing audit reviews. Modification of the security audit log is restricted through access controls and operating system logging facility. The Security Officer has read-only access to the directories where the logs are maintained on the local servers. The local logs are compared with the logs on the security logging server to ensure continuity and completeness. The local logs are deleted by authorized trusted personnel (i.e., the System Administrator and/or Security Officer). The integrity of the archived audit log is ensured with the application of a checksum and time stamp from a trusted time source to the log prior to archival. Monitoring of the hard drive space is continual on local and audit servers for all security audit logs as described in section 5.4.3.

IdenTrust's Security Officer oversees procedures governing the archival of the audit log to ensure that archived data is protected from deletion or destruction prior to the end of the security audit data retention period. Audit data is archived on a monthly basis and moved to a secure offsite storage location identified in section 5.1.8. This audit data is stored separately from the daily backups and access to audit data at the secure offsite location is restricted to Security Officers only through physical access controls.

5.4.5 Audit Log Backup Procedures

IdenTrust makes a backup of the audit log data from the security logging server on a monthly basis, as described in sections 5.4.3 and 5.4.4, in addition to the full system backup performed weekly on each server. Backup copies of the audit log data are transferred to the secure offsite location (identified in section 5.1.8) in a separate, dual-locked metal storage box.

5.4.6 Audit Collection System (Internal vs. External)

Audit logs are generated by the operating system and applications and are collected to an audit logging server that is separate from the CA and CSA as described above in section5.4.4. The external audit collection systems are managed separately by the Security Officer in accordance with 5.4.3. IdenTrust systems invoke audit processes at system startup, which cease only at system shutdown.

Manually collected audit information is gathered and stored by the authorized Registrar. Additionally, RA equipment automatically invokes audit processes at system startup and only cease at system shutdown. The audit logs on the RA workstations are manually collected, examined and archived monthly.

Should it become apparent that an automated security audit system has failed, IdenTrust will manually cease all operations except for revocation processing until the security audit capability can be restored. In order to prevent unauthorized CA functions in that event, the CA Signing key will be taken offline while the investigation is being performed.

5.4.7 Notification to Event-Causing Subject

IdenTrust does not provide notification to Subscribers or Registrars that an event was audited.

5.4.8 Vulnerability Assessments

IdenTrust's Security Officer, System Administrators and other operating personnel monitor attempts to violate the integrity of the CMA systems, including the equipment, physical location, and personnel. The audit log is checked for anomalies in support of any suspected violation and reviewed by the Security Officer for events such as repeated failed actions, requests for privileged information, attempted access of system files and unauthenticated responses. The Security Officer checks for continuity of the security audit data. Reviews of the security audit logs are conducted by the Security Officer in accordance with section 5.4.2.

5.5 Records Archival

5.5.1 Types of Records Archived

IdenTrust maintains and archives the following records, in either electronic or paper format. IdenTrust favors the use of electronic records and will electronically archive scanned paper records in every possible case.

Data collected at time of CA system initialization:

- IdenTrust's Certification Practice Statements, including this CPS - Electronic;
- CMA contractual agreements by which IdenTrust is bound - Paper;
- CMA system equipment configuration – Paper;

Data collected during CMA operation:

- Modifications or updates to any of the above items – Paper / Electronic;
- Certificate requests and revocation requests and validation requests are collected and logged automatically as described in sections 4.1.2.1, 4.9.3 and 4.9.9 - Electronic;
- Subscriber identity authentication documentation as required by section 3.2.3 – Paper / Electronic;
- Documentation of receipt and acceptance of Certificates as described in section 4.4.1 - Electronic;
- Documentation of receipt of Cryptographic Modules as described in section 4.1.2.6 – Paper / Electronic (which includes shipment tracking maintained by courier services);
- All Certificates and CRLs (or other revocation information) issued or published - Electronic;
- Security audit data, as described in section5.4.1 – Electronic / Paper;
- Other data or applications sufficient to verify archive contents are archived - Electronic; and
- All work-related communications to or from the EPMA, other CAs, and compliance auditors – Electronic / Paper.

5.5.2 Retention Period for Archive

IdenTrust archive records will be maintained for ten years and six months. To prevent loss of data, storage media are periodically tested and each log is copied to three separate secure locations on different types of media (digital linear tapes and DVDs). IdenTrust follows lifespan recommendations from vendors to determine when logs should be moved to newer media to prevent data loss. A sample storage device is randomly selected and data is retrieved approximately every 3 months for digital linear tapes (DLT) and approximately every 6 months for CD-ROM/DVD over the retention period.

IdenTrust applies a checksum to its archive files and stores them on DLT, CD-ROM or DVD to prevent alteration. No transfer of medium will invalidate CMA applied checksum. Host backups and archives are written using approved drives, media, and encryption tools. Encryption keys are archived on DVD-ROM or other non-modifiable media, and kept within IdenTrust's offsite storage facility, physically separated from the backup archives. Certain data files, such as encryption keys and paper-document images, are archived on DVD-ROM, using ISO 9660 level 3 DVD-ROM images. The files are compressed on the host producing the data files using the Unix compress(1) utility, and are prepared for archiving on the same host using the Unix tar(1) utility.

If the original media cannot retain the data for the required period, a program to periodically transfer the archived data to new media will be defined by IdenTrust.

IdenTrust, prior to the end of the archive retention period, or upon request, will provide archived data to an EPMA-approved archival facility.

Repository information is archived in a human readable form such as compressed Lightweight Directory Interchange Format ("LDIF"). IdenTrust will provide the EPMA with such data or information in a mutually acceptable format (e.g., CD-ROM, DVD, etc.).

IdenTrust favors the use of electronic records. Manual records collected for auditable events are converted into an electronic format and the physical copies are kept at the original location in a secure cabinet until electronically archived. Upon conversion to the electronic format the original physical copies are destroyed. The backup tape drives use Ultrium/LTO drives and cartridges. The backup software and encryption are completed with Veritas NetBackup and the encryption key archival is placed on CD-ROM. Upon conversion to the electronic format the original physical copies are destroyed. Electronic data will be provided in a mutually acceptable format (e.g. CD-ROM, DVD) in either text format or as a PDF file. The text data can be viewed and interpreted using a standard text reader and PDF files can be viewed using Adobe Acrobat Reader. Paper records will be supplied in either their original format or as a PDF image.

5.5.3 Protection of Archive

Archive data is stored in a separate, offsite storage facility identified in section 5.1.8. Manual logs are scanned into electronic form, and are archived in the same manner as machine-generated logs. Archive records are labeled with CA's distinguished name, identification of contents of archive record, sensitivity and date of archive. The contents of the archive can be selectively released upon discretion and approval of the Security Office and IdenTrust based on client request and circumstances. The contents of the archive will not be released in their entirety, except as required by law, as described in section 9.4.6.

Access to the off-site storage facility is strictly limited to authorized individuals and has to be authorized by IdenTrust Operations management. IdenTrust maintains a list of people authorized to access the archive records and makes this list available to its auditors during compliance audits. Certain sensitive materials are stored in a physically separate area within the off-site storage location, and access to the materials is limited to IdenTrust's Security Officers.

In order to protect the integrity of electronic data, IdenTrust applies a checksum to its archive files and records a timestamp from a trusted third party time source as they are stored on digital linear tape ("DLT"), CD-ROM or DVD to prevent alteration. The checksum is kept in the program that applies the checksum. No transfer of medium will invalidate the applied checksum.

5.5.4 Archive Backup Procedures

IdenTrust does not create a backup of its Archive.

5.5.5 Requirements for Time-Stamping of Records

System time for the CA archiving services is updated using the Network Time Protocol ("NTP") to synchronize system clocks. Trusted external time sources operated by

government agencies are used to maintain an average accuracy of one (1) minute or better.

5.5.6 Archive Collection System (Internal vs. External)

IdenTrust's archives of Certificate-related data, including a copy of all Certificates and CRLs are collected internally but stored externally in accordance with section 5.1.8.

5.5.7 Procedures to Obtain and Verify Archive Information

Access to archive data is restricted to IdenTrust's Security Officers in accordance with section 5.5.3. In order to obtain archive information, a duly authorized party must make a signed written request on letterhead of the organization making the request. The request must state with reasonable specificity what portion of the archive is sought and the legal basis or reason for the request. Upon authentication of the request and approval by IdenTrust legal counsel, IdenTrust technical, systems and security personnel will identify the backup tapes on which the requested archive information is located. The backup tapes will be ordered for delivery to the IdenTrust Security Officer from the off-site storage facility. This order is securely transported under lock and key from the archive to the IdenTrust Security Officer. The contents will only be released to the IdenTrust Security Officer once the officers has signed and documented the arrival of the requested archive material. The IdenTrust Security Officer will verify the integrity of the archived data by comparing the checksum recorded with the archive files when they were archived in accordance with section 5.5.3. IdenTrust technical and systems operations personnel will restore the backup tapes to separate servers and extract the requested archive material for delivery to the requesting party in the media and format described above in section 5.5.2. These procedures for obtaining, verifying and delivering archive information apply for all submissions of such information to the EPMA, whether based on a request by the EPMA or based on voluntary provision of the information to the EPMA.

5.6 Key Changeover

After three years of the ECA private signing key's six-year validity, IdenTrust will use the IdenTrust signature key for signing OCSP Certificates and CRLs only. This is because IdenTrust's ECA Certificate validity period must extend one Subscriber Certificate validity period past the last use of the ECA private signing key. To minimize risk of compromise of IdenTrust's signature key, it will be changed every 3 years. To ensure that the older, but still valid, Certificate will be available to verify the IdenTrust ECA's signatures on all Subscriber Certificates signed under it until they have expired, the IdenTrust ECA Certificate will have a lifetime of six years. In other words, IdenTrust will only use its latest signature key to sign Certificates for a period of three years, and IdenTrust will retain the prior signature key for the purpose of signing CRLs and to issue OCSP Responder Certificates.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

Although IdenTrust has undertaken the security measures identified elsewhere in this CPS to ensure that its Private signature keys are not compromised, in the event that such compromise occurs, the measures identified below will be immediately taken to address the compromise.

In the event of an IdenTrust CA key compromise, IdenTrust will take the following actions:

- IdenTrust will notify the ECA Root CA and the EPMA of any such disaster or compromise informally via telephone call immediately. Such call will be followed formally by a Certificate-based communication if possible or otherwise by a written letter sent by courier service;
- IdenTrust will notify all affected parties (e.g., Subscribers, Subscribing Organizations, RAs and Trusted Correspondents) of compromise via signed e-mail immediately;
- IdenTrust will request that the Root ECA revoke IdenTrust's CA Certificates via signed email from the IdenTrust Security Officer or IdenTrust Operations Management Personnel, followed by a written letter signed by IdenTrust Operations Management Personnel sent by courier service;
- IdenTrust will destroy all affected private keys associated with the IdenTrust CA, RA and OCSP Responders. The method used to destroy private keys on Cryptographic Modules will comply with standards outlined by the manufacturer for secure destruction and re-initialization of modules as outlined in section 6.2.10;
- IdenTrust will, after archiving data and prior to re-use, overwrite the hard drives of all CA equipment to erase all data using software compliant with NIST guidelines;
- IdenTrust's ECA will be re-established. IdenTrust will generate new private keys and submit new Certificate requests to the ECA Root for their CA Certificates; and
- IdenTrust will re-issue all RA Operator, Trusted Correspondent, OCSP Responder and Subscriber Certificates. IdenTrust will follow established policies and procedure for re-issuance after revocation as described in section 3.3.2 (i.e. the procedures for initial issuance listed in section 3.2.3).

In the case of a compromise of an OCSP Responder key:

- The IdenTrust ECA will immediately revoke the OCSP Responder Certificate that is compromised;
- IdenTrust will publish a new CRL to its directory;
- IdenTrust will initialize any Cryptographic Modules and destroy the compromised OCSP key. The method used to destroy private keys on Cryptographic Modules

will comply with standards outlined by the manufacturer for secure destruction and re-initialization of modules as defined in section 6.2.10;
- IdenTrust will, after archiving data and prior to re-use, overwrite the hard drives of all OCSP Responder equipment to erase all data using software compliant with NIST guidelines; and
- IdenTrust will generate a new key pair and Certificate for the OCSP Responder. The new Certificate will be installed in the OCSP Responder immediately following generation. IdenTrust will make reasonable best efforts to have a functional OCSP Responder within 4 hours following the compromise of an OCSP Responder key.

If a Trusted Correspondent's or RA Operator's private key has been or is suspected to have been compromised:

- IdenTrust's VP of Operations and/or CIO, IdenTrust's Security Officer and, in the case of a Trusted Correspondent, the Security Officer for the Subscribing Organization will meet to assess and address the situation;
- The Certificate will be revoked if found to have been compromised;
- All Subscribers' Certificates that were directly or indirectly authorized for issuance by the Trusted Correspondent or the RA Operator after the suspected date of compromise will also be revoked after a query is run to identify each Certificate and its relation as issued by the Trusted Correspondent's or RA Operator's key (this process may be manual or automated);
- IdenTrust will identify and remediate the causes of the compromise so that they do not recur;
- IdenTrust will publish a new CRL to its directory; and
- the RA Operator or Trusted Correspondent will generate a new key pair and IdenTrust will issue a new Certificate for the RA Operator or Trusted Correspondent.

In case of the CA or CSA compromise or loss, the Security Officer will conduct an investigation into the causes. A report of the causes, remediation steps and enhancements to the practices to prevent future occurrences is assembled by the incident response team and is provided to the Vice-president of Operations. The Vice-president of Operations will provide to the EPMA a summary of the final report.

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

IdenTrust performs tape back-ups on a daily basis. Back-up tapes and back-ups of CA Cryptographic Modules are stored off-site in a secure location. In the event of disaster whereby both principal and back-up CA operations become inoperative, IdenTrust's CA operations will be re-initiated on appropriate hardware using backup copies of software and Cryptographic Modules. IdenTrust disaster recovery plans are available for review by its auditors and major customers under an appropriate non-disclosure agreement.

5.7.3 Entity Private Key Compromise Procedures

See procedures outlined in section 5.7.1 above.

5.7.4 Business Continuity Capabilities After a Disaster

IdenTrust maintains a detailed Disaster Recovery Plan. The following is an abbreviated summary of IdenTrust's disaster recovery:

- IdenTrust has implemented a completely redundant hardware configuration at its principal site. In the event of a disaster whereby IdenTrust's main CMA operations are physically damaged or otherwise become inoperative, IdenTrust's CMA operations will fail over to the disaster recovery data center site described in Section 5.1.1.1.2 and be recovered to the system state at the point of a disaster declaration, through the use of backup media, system logs and data base transaction logs. Backup copies of the CA's signing keys (see section 6.2.4) will be used to restore CMA services at the disaster recovery data center. Priority will be given to re-establishing validation services and the ability to publish revocation information.
- Pre-disaster vendor agreements provide for a drop shipment of hardware to IdenTrust's principal site following a major incident. The intention of this provision is to restore CMA operations at the principal site as quickly as possible and to avoid a single point of failure that would then exist at the disaster recovery data center. IdenTrust performs tape back-ups on a daily basis. Back-up tapes and back-up Cryptographic Modules are stored off-site in a secure location.
- In the event of disaster whereby the CMA, at both principal and disaster recovery data sites, becomes inoperative, IdenTrust's CMA operations will be re-initiated on appropriate hardware using backup copies of software, backup data and backup Cryptographic Modules. Priority will be given to re-establishing validation services and ability to publish revocation information.
- In the event that the IdenTrust cannot reestablish revocation capabilities prior to the next update field in the latest CRL issued by the IdenTrust ECA, then IdenTrust will report this to the ECA Root CA and EPMA. IdenTrust will report this to the EPMA informally via telephone call as soon as reasonably possible. Such call will be followed formally by a Certificate-based communication if possible or otherwise by a written letter sent by courier service.
- The EPMA will decide whether to declare the ECA private signing key as compromised or allow additional time for reestablishment of revocation capability. If the EPMA declares the ECA private signing key as compromised IdenTrust will follow procedures outlined in section 5.7.1 of this CPS and section 5.7.3 of the ECA CP.
- In the event of a disaster whereby IdenTrust's CMA operations suffer total physical damage beyond disaster recovery or repair (including destruction and compromise of the backup CA keys), IdenTrust will request that its ECA Certificates be revoked. IdenTrust will follow the process and procedures described for a CA key compromise situation section 5.7. The IdenTrust Security Officer will notify the ECA Root CA and the EPMA of any such disaster or compromise informally via telephone call as soon as reasonably possible. Such call will be followed formally by a Certificate-based communication if possible or otherwise by a written letter sent by courier service.

5.8 CA or RA Termination

IdenTrust CA termination will be handled in accordance with section 5.7 above.

If the termination is for convenience, or other non-security related reason, and provisions have been made to continue compromise recovery, compliance and security audit, archive, revocation, and data recovery services, then neither the terminated ECA's Certificate, nor Certificates signed by that ECA, need to be revoked.

If provisions for maintaining these services cannot be made, then the ECA termination will be handled as an ECA compromise in accordance with section 5.7.1 above. In this case, IdenTrust will notify all Subscribers and Trusted Correspondents of termination of IdenTrust operations within as soon as reasonably possible via signed e-mail and out-of-band confirmation, if such contact information is available. IdenTrust will notify the EPMA at least 30 days in advance of such termination.

If possible, IdenTrust will securely transfer its CA signing keys to the EPMA or its designee. Otherwise, IdenTrust will revoke all Certificates it has issued. This revocation list will be published by the IdenTrust's CA and the NextUpdate value will be greater than or equal to the latest expiration date for all Certificates issued by the IdenTrust's ECA. IdenTrust will destroy all private key(s) so that they cannot be compromised or otherwise used. The EPMA will ask the ECA Root CA to revoke the IdenTrust's CA Certificate, since IdenTrust will no longer be in a position to revoke its Subscriber Certificates.

In the event of termination, IdenTrust will transfer its entire audit and archival records to the EPMA. The archived data will be provided in format as described in section 5.5.2 and in accordance with procedures outlined in the same section.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

IdenTrust and Subscribers will generate their own keys in all instances where such is possible. Generation of IdenTrust's CMA public/private key pairs is performed using only approved cryptographic standards published by the National Institute of Standards and Technology in Federal Information Processing Standards Publication, FIPS 140-2, "Security Requirements for Cryptographic Modules," as applicable.

IdenTrust's CA and CSA public/private key pairs are only generated on FIPS 140-2 Level 3 validated hardware Cryptographic Modules. The CA key generation event is documented in writing and is video-recorded as part of physical audit event.

IdenTrust's RA Operators public/private key pairs are only generated on FIPS 140-2 Level 2 validated hardware Cryptographic Modules.

IdenTrust will never generate a Subscriber's signature keys. Private keys for Medium Assurance Signing Certificates are generated by the Subscriber, either in an approved browser or in a Cryptographic Module validated as conforming to at least FIPS 140-2 Level 1. Private Signing keys for Medium Token Assurance and Medium Hardware Assurance Certificates must be generated by the Subscriber on a FIPS 140-2 Level 2 or higher validated cryptographic hardware module. A FIPS 140-2 Level 2 validated hardware Cryptographic Module is used to generate all encryption keys.

In this CPS, IdenTrust means FIPS 140-2 in all cases, except on those explicitly noted for legacy components, where they are noted in this section, the corresponding sections, or in Appendix G.

Private keys will never appear in plaintext form outside of the module in which they were generated.

6.1.2 Private Key Delivery to Subscriber

Subscribers will generate their own key pairs for all Signing Certificates (signature keys) and IdenTrust will create and deliver key pairs for all Encryption Certificates (encryption keys) as described in this section.

The Encryption key pair, along with a symmetric 256 bit key (AES key), are generated on a dedicated FIPS 140-validated hardware Cryptographic Module. For purposes of encryption key escrow, immediately after the encryption key pair is generated, it is encrypted using a 2048 bit RSA Administrative public key embedded in a self-signed Certificate. Additional details can be found in the IdenTrust ECA KRPS.

In the client's side, an IdenTrust-written browser component (e.g., ActiveX control) generates an RSA 2048 bit key pair. The browser component uploads the public key to the IdenTrust system over the Server -authenticated SSL/TLS session at the start of the

retrieval process (see section 4.3.1 for more information about the Server-authenticated SSL/TLS session). The IdenTrust CA transfers it into the dedicated Cryptographic Module to encrypt the AES key using the RSA encryption algorithm. The AES key is used to encrypt the private encryption key for transport, using the AES-256 algorithm.

Both the encrypted-private-encryption key and the encrypted-AES key are downloaded, over a Server-authenticated SSL/TLS session, to the browser component onto hidden fields in a non-cache web page. To complete the insertion process the browser component decrypts the encrypted-AES key to obtain the AES key, which is used to decrypt the encrypted-private-encryption key. The memory location used for this operation is pinned to physical memory by the operation system to prevent writing information to the hard drive. Then, the Cryptographic Module's import function, supported through its application programming interface, is used to insert the encryption private key into the Module (Medium Token and Medium Hardware Assurance) or the key store (Medium Assurance Certificates). After this is complete, the retrieval process will zeroize the memory used to hold the decrypted keys. No copy other than the authorized key escrow copy continues to exist after the insertion process has been completed.

For information on the cryptographic module models used to meet ECA CP requirements, see Appendix G.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered to the CA in a PKCS#10 file which binds the Private and public keys and is submitted to the CA during a Server-authenticated SSL/TLS-Encrypted Session that is secured with a valid SSL/TLS Certificate that chains to one of IdenTrust's Root Certificates (e.g., IdenTrust Commercial Root CA), embedded in the most widely distributed commercial browsers. Three methods are used to bind the confirmed identity to the public key:

(1) During the registration phase outlined in Section 4.1.2.1, the applicant's information, PKCS#10, and hash of the applicant-provided account password are bound together via the Server-authenticated SSL/TLS-Encrypted transmission to the CA. Only the applicant knows the account password because only its hash is stored. After the I&A process, the RA Operator provides an Activation Code to the applicant through an out-of-band confirmed channel as explained in Section 4.1.2.6. The secret account password and Activation Code are used in combination by the applicant to retrieve the Certificate during a subsequent Server-authenticated SSL/TLS-encrypted session as explained in Section 4.3.1. This is a common method for Subscribers of ECA SSL Certificates when they provide a Certificate signing request during the application phase.

(2) Much like the process described above and outlined in Section 4.1.2.1, the second method is much the same with the exception that the PKCS#10 is not created initially when the application is submitted to the CA via a Server-authenticated SSL/TLS Encrypted transmission. The secret account password and Activation Code are used in combination by the applicant to create the PKCS#10 and retrieve the Certificate during a subsequent Server-authenticated SSL/TLS-encrypted session as explained in Section 4.3.1.

(3) During the registration process, either the bulk load (see Section 4.1.3), an RA

Operator enrolls the applicant and approves issuance of a Certificate to the Subscriber. The Activation Code is generated and sent out-of-band to the applicant to a confirmed destination. The secret account password is created by the applicant upon receipt of the out-of-band information including the Activation code. After the account password is confirmed it is used in conjunction with the Activation Code by the applicant in a Server-authenticated SSL/TLS-encrypted session during which the public key is submitted to the RA/CA in a PKCS#10 and a Certificate is returned back during the same session.

6.1.4 CA Public Key Delivery to Relying Parties

Relying Parties may receive and maintain ECA Root CA public key via a Certificate signed by the ECA Root CA itself. Delivery of the ECA Root Certificate is controlled by DISA and the ECA Root Certificate may be downloaded from a DoD global Repository such as: https://crl.chamb.disa.mil/. Relying Parties may also receive and maintain the IdenTrust ECA Subordinate CA Certificate. The acceptable method for the delivery of this Certificate is through an e-mail or other communication may be sent to Relying Parties from IdenTrust directing them to download the CA Certificate at a designated URL on IdenTrust's web site (at the web site, the CA Certificate may be downloaded and Relying Parties instructed to use their web browser to check the hash / thumbprint of the Certificate and compare it with those provided via authenticated out-of-band sources.)

6.1.5 Key Sizes

All public key technology used by IdenTrust to sign Certificates is equivalent to, or of a higher work factor than, 2048-bit RSA keys (as a practical matter, all 1024-bit Certificates expired prior to 2010, since IdenTrust only issued one-year, 1024-bit Certificates until September 2008 when it ceased issuing such Certificates and began issuing 2048-bit Certificates). IdenTrust employs RSA and does not use elliptic curve or DSA.

RSA is supported for 2048 bit, which is currently used as the default. IdenTrust employs 2048 bit RSA when issuing Certificates and CRLs that are valid beyond June 30, 2011. Signatures on Certificates and CRLs that are issued by IdenTrust are both SHA-1 and SHA-256.

SHA-1 is supported for 160 bit and is currently used as the default. When generating SHA-1 digital signatures on Certificates, all their associate CRL and OCSP responses are (and will be) signed using the SHA-1 algorithm. When generating SHA-256 digital signatures on Certificates, all their associate CRL and OCSP responses are signed using the SHA-256 algorithm illustrated in the table below.

	Certificate Signature Algorithm	CRL Signature Algorithm	OCSP Response Signature Algorithm	OIDs Asserted in CA Certificate	OIDs in Certificates Signed by CA
Sub CA for SHA-1	SHA-1	SHA-1	SHA-1	▪ Id-eca-medium ▪ Id-eca-medium-token ▪ Id-eca-medium-hardware	▪ Id-eca-medium ▪ Id-eca-medium-token ▪ Id-eca-medium-hardware
Sub CA for SHA-256	SHA-256	SHA-256	SHA-256	▪ Id-eca-medium-sha256 ▪ Id-eca-medium-token-sha256 ▪ id-eca-medium-hardware-sha256 ▪ Id-eca-medium-device-sha256	▪ Id-eca-medium-sha256 ▪ Id-eca-medium-token-sha256 ▪ id-eca-medium-hardware-sha256 ▪ Id-eca-medium-device-sha256

In all cases where Transport Layer Security / Secure Socket Layer (TLS/SSL) is used AES (128 bits) or equivalent for the symmetric key, at least 2048 bit RSA or equivalent for the asymmetric keys, and SHA-256 (if commercially available as part of TLS 1.2) is used. In addition, the TLS/SSL protocols use cipher suites that are as strong as the keys transported using the protocol (e.g. 2048 RSA bit with AES 128, AES 256, or triple key DES). IdenTrust uses TLS 1.0, TLS 1.1 and TLS 1.2 in all cases unless a particular version is no longer secure, in which case only the secure versions of the protocol will be used.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters will always be generated and checked in accordance with the standard that defines the crypto-algorithm in which the parameters are to be used.

For Subscriber encryption key pairs, which are generated by the ECA system, IdenTrust currently supports RSA keys using RSA PKCS#1. The Subscriber hardware or software Cryptographic Modules generate signature keys. Subscriber Cryptographic Modules are FIPS validated.

Generation of IdenTrust's CMA public/private key pairs are performed using only approved cryptographic standards published by the National Institute of Standards and Technology in Federal Information Processing Standards Publication, FIPS 140-2. IdenTrust currently supports RSA keys using RSA PKCS#1. 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 X.509 V3 Key Usage Field)

IdenTrust will certify keys for use in signing or encrypting, but not both. The use of a specific key is determined by the key usage extension. The following key usage fields will be used depending on the nature of the Certificate: "digital signature," " non-repudiation," and "key encipherment." The use of a specific key is determined by the key usage extension in the X.509 Certificate. For example, Certificates with "key encipherment" will not set the "non-repudiation" bit. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer or Transport Layer Security) that provide authenticated connections using key management Certificates. Web Server Certificates will have both "digital signature" and "key encipherment" key usage fields included.

6.2 Private Key Protection

6.2.1 Cryptographic Module Standards and Controls

Subscribers will store their Medium Assurance Software Certificates in a module validated as conforming to at least FIPS 140-2 Level 1 and their Medium Token Assurance and Medium Hardware Assurance Certificates in a module validated to at least FIPS 140-2 Level 2 . Higher levels are available if desired. These modules will not allow the user to export key pairs.

Trusted Correspondents and all RA Operators are required to use hardware Cryptographic Modules that are validated as conforming to at least FIPS 140-2 Level 2. These modules will not allow the user to export key pairs.

IdenTrust uses only validated as conforming to FIPS 140-2 Level 3 hardware Cryptographic Modules with PKCS#11 compatibility for the CA Key Cryptographic Module, the OCSP Key ("CSA") Cryptographic Module, and the backup Cryptographic Module. These modules do not allow output of the private asymmetric key to plaintext.

IdenTrust uses only Cryptographic Modules validated as conforming to FIPS 140-2 Level 2 hardware to generate Subscriber encryption keys.

Specific brands and models are provided in Appendix G.

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

The Cryptographic Modules containing the ECA's signature key and the CSA signature key are stored in within one or more dual-locked safes in IdenTrust's secure room, which is under two-person control as described in section 5.1.2.1.1. The PIN Entry Device keys (PED keys) used to activate the Cryptographic Module are kept in separate dual-locked safes in the secure room. No safe contains both the cryptographic materials and the related PED keys; and no individual, acting alone, is able to open any of the safes or have independent access to any key material or any PED key. This separation of duties requires at least one CA Administrator and one System Administrator to access the ECA Cryptographic Module and related CSA keys. A Security Officer is also required for accessing PED keys related to initialization and cloning. These roles are required to

retrieve and activate the ECA, and CSA, signature keys. Once access is obtained, the System Administrator remains to provide system support and record the actions by the CA Administrator. The Security Officer remains to witness the actions of both the System Administrator and CA Administrator. Actions on the private key within the Cryptographic Module are executed only by the CA Administrator. For specific details about the associated duties and keys from each role for this process please see Appendix G.

In addition to the requirement for multi-person access, each safe contains a physical logbook that requires each person to sign for custody of material accessed within the safe. It also requires material be signed back in after use. In addition to the custody requirement, access to Cryptographic Modules also requires each user to file the serialized, signed request for access to cryptographic materials in the logbook and annotate it in a separate section. The request must be signed by a combination of two of the following people: IdenTrust's Vice President of Operations, a Security Officer, or a separate member of the Risk Management Committee, prior to accessing any cryptographic material. These logbooks are periodically audited in accordance with section 5.4.2 of this CPS.

For purposes of disaster recovery, two backups of the ECA signing key are kept. One is secured in a separate safe within the secure room within the primary facility and the other is in the off-site facility. To access either backup two-person controls are implemented as explained in section 5.1.8.

Escrowed encryption keys are extracted from the KED under two-person control. People involved in backup activities are trusted individuals and comply with appropriate controls to ensure that status. Further detail about controls surrounding escrowed encryption keys is provided in the Key Recovery Practices Statement ("KRPS").

6.2.3 Private Key Escrow

Under no circumstances will either IdenTrust or its authorized agent's escrow or keep the private signature key of a Subscriber. For some purposes, such as data recovery, IdenTrust securely escrows encryption keys, which is done in accordance with its Key Recovery Practices Statement, and the ECA Key Recovery Policy.

IdenTrust does not escrow, or has any third party escrow, its CA private keys

6.2.4 Private Key Backup

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.

6.2.5 Private Key Archival

Under no circumstances will a signature key be archived. For some purposes, such as data recovery, it is acceptable to archive encryption keys see also section 6.2.3 and IdenTrust's Key Recovery Practices Statement.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Subscriber’s private signature keys are to be generated by and in a Cryptographic Module.

Encryption keys are generated outside of the Subscriber’s Cryptographic Module. For initial delivery or delivery after a key recovery request, the encryption private key is encrypted using the process described in section 6.1.2. As additional security, the private encryption key will be protected by the use of a Server-authenticated SSL/TLS session during the retrieval process (see section 4.2).

CA and CSA private keys are generated on a FIPS 140-2 Level 3 validated Cryptographic Module that allows for a “cloning” process that creates a copy of the private keys. IdenTrust uses the cloning process to create three copies of the original private keys, the original keys and a copy are used in a redundant configuration in production operations to ensure high availability. Both production private keys and a backup private key are maintained in the same Primary Facility described in section 5.1.2.1.1. The second backup copy is stored in the off-site facility described in section 5.1.6. Cloning of the CA and CSA keys is done under two-person control and the process is documented in writing, approved by management, witnessed, and video-recorded.

RA Operator private keys will be always generated on the Cryptographic Module.

6.2.7 Private Key Storage on Cryptographic Module

All private keys are maintained in Cryptographic Modules evaluated to the standards set forth in section 6.2.1 and must be protected from unauthorized access and use in accordance with the FIPS 140 requirements applicable for the module.

6.2.8 Method of Activating Private Key

For activation of Subscriber private keys, IdenTrust provides empty Cryptographic Modules (no keys in them) to Subscribers and require them to self-select the activation data in accordance with section 6.4.1. Entry of activation data must be protected from disclosure (e.g., the data should not be displayed while it is entered).

CA and CSA private keys reside within a FIPS 140-2 Level 3 validated Cryptographic Module. Activation of the private key requires a PED key to be connected to the module. PED keys that activate the modules are stored securely and separately from the Cryptographic Module and are retrieved and used always under two-person control (see sections 5.1.2.1.1, 6.1.1 and 6.2.2.). The private key is activated by use of one of the PED keys.

6.2.9 Method of Deactivating Private Key

Subscribers, RA Operators, and Trusted Correspondents are notified of their obligation to not leave their Cryptographic Modules unattended or open to unauthorized access while active. Subscribers, RA Operators, and Trusted Correspondents are required to deactivate the modules either by a manual logout or by configuring a passive timeout that does it automatically.

The CA and CSA Cryptographic Modules when active are not exposed to unauthorized access. The modules are maintained in the secure room that requires two-person control. In addition, the modules are enclosed in locked steel cabinets. When not in use, a module is deactivated via logout procedures, removed and stored in accordance with section 5.1.2.1.1.

6.2.10 Method of Destroying Private Key

Subscribers are notified of their obligation to destroy private keys when they are no longer needed. Information on how to destroy the private keys will be provided to Subscribers.

RA Operators use Medium Hardware Assurance Certificates installed in appropriate Cryptographic Modules. RA Operators are provided instruction on the security procedures by which they remove their modules when not in use and configure the automatic passive inactivity timeouts in the module in accordance with the security policy.

CA, CSA, and any RA private keys will be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked. The destruction method will be in accordance with FIPS 140-2 requirements, as applicable. IdenTrust will use the FIPS 140-2 -certified "zeroize" function of the hardware Cryptographic

Module to securely destroy private keys that are no longer needed to sign Certificates or to sign CRLs.

6.2.11 Cryptographic Module Rating

Requirements for Cryptographic Modules are as stated above in Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Archival of public keys is achieved via Certificate archival.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

All Certificates and corresponding keys pairs will have maximum Validity Periods in accordance with the following table:

	IdenTrust ECA	End Entity Certificates	Component Certificate	OCSP Responder Certificate
Certificate Lifetime	6 years	1, 2 or 3 years	1, 2 or 3 year	30 days
Key Usage Period (*)	6 years	1, 2 or 3 years	1, 2 or 3 year	3 years

*See Section 5.6 (Key Changeover), which explains that CA Private Signing Keys are voluntarily retired from signing Subscriber Certificates after three years to accommodate for Key Changeover processes (they are still used to sign CRLs and OCSP Responder Certificates to allow for validation of three-year Subscriber Certificates issued during the first three years of the CA Signing Key's lifecycle).

6.3.3 Subscriber Private Key Usage Environment

The Subscribers shall use their private keys only on the machines that are protected and managed using commercial best practices.

6.4 Activation Data Generation and Installation

6.4.1 Activation Data Generation and Installation

IdenTrust, its RA Operators, and Subscribers are obligated, through policy and contract, to use passwords to protect access to private keys. Policies and contracts will include the obligation to generate passwords and PINs in conformance with the FIPS 140-2.

Subscribers will self-select the activation data for their Cryptographic Modules. Subscribers will receive and acknowledge an advisory statement to help to understand responsibilities for uses and control of the Cryptographic Module, which will include PIN or password creation. Subscriber PINs, when used, shall be 6-8 digits at a minimum. Randomly generated PINs shall be used when possible. If this is not possible, Subscribers who create their own PINs shall be instructed to select PINs that are not related to their personal identity, history, or environment. Sequences, repeated numbers, social security numbers, and date formats, or other easily guessed numbers shall not be used. When alphanumeric pass-phrases are used, an interspersed mix of 8 characters, including at least two interspersed digits, shall be used. The activation data shall not resemble dictionary words; they shall differ from words or names by at least two characters that are not simple number-for-letter substitutions and shall not consist of words or names followed by 1-4 digits. The activation data shall not contain sequences, repeated characters, date formats, or license plate formats.

If a particular implementation enables the CMA to generate the password on behalf of the Subscriber (e.g., protection of escrowed key encryption at issuance. See Section 6.1.2), it will be generated in compliance with the above requirements. IdenTrust transmits those passwords over Server-authenticated SSL/TLS protected channels, encrypted email, or courier service that requires signature-receipt. This delivery will be completed distinct in time and place from the associated Cryptographic Module.

RA Operators and Trusted Correspondents are under obligation to maintain passwords that comply with the foregoing requirements. RA Operators and Trusted Correspondent will self-select the activation data for their Cryptographic Modules. They will receive and acknowledge an advisory statement to help to understand responsibilities for uses and control of the Cryptographic Module.

The Cryptographic Module containing the CA and CSA keys are validated as conforming to at least FIPS 140-2 Level 3. Activation data is contained within a PIN Entry Device key (PED key). Each PED key is imprinted with a unique digital identifier specific to the FIPS 140-2 Level 3 validated device during the initialization process.

6.4.2 Activation Data Protection

IdenTrust informs Subscribers of their obligation to protect their activation data from access by others. Activation data should be memorized, not written down. If written down, it must be secured at the level used to protect the associated Cryptographic Module, and must not be stored with the Cryptographic Module.

RA Operators and Trusted Correspondents are obligated by policy and contract to protect their activation data from access by others. Activation data should be memorized, not written down. If written down, it must be secured at the level used to protect the associated Cryptographic Module, and must not be stored with the Cryptographic Module. RA Operators are under the obligation to secure the activation data at the level of the data the module is used to protect. This level of protection means that Subscribers and Trusted Roles of IdenTrust are under obligation to secure their activation data at all times from unauthorized access.

CA and CSA activation data is contained within the PED key. The PED key is kept under two-person control in the secure room by Trusted Roles (See section 5.1.2.1.1). When not in use, the PED key remains stored in a safe within the secure room.

6.4.3 Other Aspects of Activation Data

The activation data for the Cryptographic Module containing the CA, and CSA keys is entered using a secure entry device. This activation data is contained within a PED key, therefore, the requirement to change the data does not apply to the CA, and CSA activation data.

The activation data for the Cryptographic Module containing the RA Operator keys is changed once every three months in accordance with procedure.

6.5 Computer Security Controls

All IdenTrust CMA equipment will use operating system(s) and third party software that incorporate security enhancements, that is, those that prevent and detect attempts to alter it, or to disable its security functions. For more information on the brand and model numbers of this equipment see Appendix G.

IdenTrust's CA equipment uses operating systems that require authenticated logins, provide discretionary access control, and provide security audit capability. IdenTrust operates systems that have received security evaluations from the National Information Assurance Partnership ("NIAP"), Trusted Product Evaluation Program ("TPEP"), or other comparable information-assurance ("IA") evaluation programs.

IdenTrust hardens all CMA equipment utilizing industry best practices, NSA System Security Configuration Guidelines, and IdenTrust-developed checklists prior to deployment. All unused ports, protocols, services, system and user accounts are disabled in accordance with IdenTrust's configuration guidelines. All IdenTrust CMA equipment is tested and evaluated prior to deployment and assessed periodically afterward for vulnerabilities, anomalies and malicious code, in accordance with IdenTrust's testing and evaluation criteria.

Database protection security controls include:

- OS hardening is performed to IdenTrust CA standards.
- All services are disabled except services required for business transactions.
- All hosts are disallowed except authorized hosts.
- The KED data is encrypted before being placed in its database table.
- Table add/drop protection is controlled by admin userid.
- The database is secured using vendor-recommended best practices
- Administrative access based on the task is restricted by SSH and a Valid Certificate or root access within the secure room.
- The operating system has been certified under the Common Criteria Certification, which includes authenticated logins, discretionary access control, a security audit capability, system self-protection, process isolation, and support for recovery from key or system failure.

- Dual controls and separation of duties are in place.
- Audit controls are in place and logs are sent to a central logging server.
- Central logs located on the security logging server are only available to security staff.

6.6 Life Cycle Technical Control

6.6.1 System Development Controls

IdenTrust has a process in place to minimize the likelihood of any component being tampered with. Vendors selected are chosen based on their reputation in the market, ability to deliver quality product, and likelihood to remain a viable company. Controls are put in place including ensuring management is involved in the vendor selection and purchase decision process. External purchasing paperwork will only generically identify the purpose for which the component will be used.

CMA hardware and software PKI components are shipped directly to a trusted member of the IdenTrust ECA team; and a chain of custody is maintained from that point forward and verified through a serial number affidavit. Cryptographic Modules are shipped in tamper-evident containers and zeroized upon confirmation of the chain of custody and serial number. Other major PKI components (i.e., servers) are shipped under standard conditions and other controls are in place to ensure accountability for the component. Furthermore, when feasible, components are disassembled, inspected, and reassembled, or wiped clean and reloaded, to ensure no extraneous or unspecified parts are contained in them. Storage devices are initialized or formatted and all software is installed in accordance with IdenTrust's policies and procedures as mentioned in section 6.5 and this section 6.6. The CMA equipment is installed with a baseline configuration and hardened to reduce the risk of malicious software being introduced. Intrusion detection systems are installed and continually measure hosting configurations. Any changes to these configurations will send an email alert to security. Subsequent installations of applications or components are documented and verified to prevent installation of software not part of the CA configuration.

IdenTrust develops some PKI software components. A sequential design methodology (e.g., Waterfall) is used to ensure that a formal documented process was followed and security requirements were achieved. Strict quality assurance is maintained throughout the process through a dedicated QA phase and change control cycle. The CIO,or a designee, formally approves each software change as part of the change control cycle. Documentation is maintained supporting the process in a change management system. All code changes are tracked on a revision control system that is securely hosted within the IdenTrust internal network. Development and testing environments are maintained on separate servers in a separate network from the main operational environment with appropriate segregation rights restricting developers and testers from having access to production equipment.

6.6.2 Security Management Controls

CA, RA, and CSA equipment is dedicated to administering a PKI. The configuration of IdenTrust's CA, RA, and CSA equipment, as well as any modifications and upgrades, are documented following a rigorous change control process. Change control processes consist of a change control form that is processed, logged and tracked for any changes to CMA systems, firewalls, routers, software and other Internet access controls. In this manner, IdenTrust can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

IdenTrust uses the following minimum specifications for CA, RA, CSA, and database equipment:

- Unix-compatible server
- Single 650 MHz processor
- 1 GB of RAM
- 36 GB storage

Operating systems are imaged onto CA, RA, CSA, and database systems using a gold image that is maintained in a separate vendor-approved server. In addition, the vendor provides an operating system "fingerprint" database that is used periodically to validate the MD5 hash value of the gold image OS files used at IdenTrust.

Operating system and application files are benchmarked prior to releasing a system into production, using a host-based intrusion detection system. The snapshot of the state of files is recorded. Daily and hourly integrity checks are scheduled against the known state of the tracked files. The Security office is notified immediately, via e-mail and page messages, about changes made on production systems.

IdenTrust uses Trusted Role access through SSH and Certificate authenticated HTTPS for administrative functions for PKI components. For administrative functions in the CA a dedicated console uses SSH and Certificate authenticated HTTPS that allows access to the CA on the same secure network. This console resides within the secure room protected with controls as described in section 5.1.2. The specifications for the SSH server settings for the console are available in Appendix G.

For administrative functions of other components, access through an SSH proxy server is used. Administrative access to all PKI components external to that secure room is controlled individually through key/Certificate based authenticated sessions via the SSH proxy server. The specifications for the SSH proxy server settings are available in Appendix G. All PKI components utilize access controls that allow only connections from the SSH proxy server for administrative functions.

IdenTrust regulates modifications, changes and upgrades to systems and applications using a structured and documented change control process.

First, a need to modify, upgrade or implement a change to a production application, host or system is documented. Second, a risk analysis is performed; then change requests are reviewed by Quality Assurance ("QA"), Engineering, and Operations teams. In addition, the Vice President of Operations and/or CIO approves all changes prior to implementation. If the risk is perceived as higher based on the complexity of the request, another signature will be required from the Operations Management team separate from

the Vice President of Operations or CIO. Third, testing and validation of changes are managed by the QA team using a documented and approved testing plan.

6.6.3 Life Cycle Security Controls

Equipment (hardware and software) procured to operate a PKI is purchased in a fashion to reduce the likelihood that any particular component was tampered with as specified in section 6.6.1.

All hardware and software that supports a CMA is shipped or delivered via controlled methods that provide a continuous chain of accountability as specified in section 6.6.1.

IdenTrust's Trusted Correspondents and RA Operators are required to take reasonable care to prevent malicious software from being loaded on RA equipment through user education coupled with the use of antivirus programs and adhering to the software manufacturers recommended patches applicable to the installed software. Only applications required to perform the organization's mission will be loaded on the RA computer, and all such software will be obtained from sources authorized by local policy. Data on RA equipment is scanned for malicious code on first use and periodically afterward. Equipment updates are purchased or developed in the same manner as original equipment, and are installed by trusted and trained personnel in a defined manner.

6.7 Network Security Controls

IdenTrust's CA system will be connected to at most one network and will be protected against known network attacks. All IdenTrust CA, CSA, RA, and Repository computer systems are located in a secure facility and are also protected by firewalls.

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 applications.

IdenTrust uses boundary firewalls that have been successfully evaluated against the U.S. Government Medium Robustness Firewall Protection Profile (“FWPP”) by a NIAP recognized scheme. In case that IdenTrust is unable to find an appropriate firewall due to limitations of the NIAP lists, a common-criteria-approved component will be selected and evaluated for conformance with the requirements in the CP. Subsequently, IdenTrust will obtain approval by the EPMA for use of such component.

For the selection of its intrusion detection system (“IDS”), IdenTrust reviews the NIAP’s list of approved components and if there are six or more IDSs that have been successfully evaluated against the Intrusion Detection System Protection Profile [IDSPP] by a NIAP recognized scheme, IdenTrust choses one of them. Otherwise, IdenTrust choose an IDS that has been successfully evaluated using Common Criteria at least EAL 2. The chosen IDS will be evaluated to provide: i) audit of security events, ii) protection of security audit log, iii) identification and authentication with secure action upon authentication failure, iv) data confidentiality and integrity during communication with other

components, v) non by-passable, and vi) provide self-protection. The IDS also: vii) enable the ability collect security relevant events, viii) process and output those events in human readable form, and ix) protect those event logs from unauthorized access, modification or deletion

The PKI Network ("PKI Net") supports IdenTrust's Public Key Infrastructure ("PKI") activities. The PKI Net consists of five significant network segments, organized into three tiers:

Outer Tier

PKI External Network

Middle Tier

PKI Demilitarized Zone ("DMZ") Public Network

PKI Demilitarized Zone ("DMZ") Private Network

Inner Tier

PKI Private Networks (secure segments)

Outer Tier – the Internet interface

The PKI Network connects to the Internet through several major Internet Service Providers, which are routed into the computing facilities from separate directions for security and redundancy. The colocation providers provide additional connectivity redundancy if needed. Inbound packet destination is determined by Border Gateway Protocol ("BGP").

The outer tier consists of two enterprise-class routers serving as premise routers, separating the IdenTrust system from the Internet. Each router is connected to one or more ISPs. As well as serving as IdenTrust's Internet connection, these routers perform some initial traffic filtering and screening. The routers are configured as a high-availability team; if the primary member router fails, the standby router takes responsibility for routing packets on all critical segments.

Routing into the PKI network depends on packet destination. The routers run BGP 4 as the External Gateway Protocol ("EGP") and use static routes for internal routing. IdenTrust's configuration of BGP offers real-time load balancing between providers, utilizing BGP's Autonomous System Number ("AS") routes.

The main filtering and screening work is handled by firewalls just inside the border routers. These firewalls are certified under the Common Criteria Certification process, and meet the Application Layer Firewall Protection Profile for Medium Robustness Environments, which is a US National Security Agency benchmark for firewalls. Firewall operation is described in more detail below.

Middle Tier – the DMZ

Fronting the DMZ tier is the pair of firewalls mentioned above, connected on both sides to switches. These firewalls are configured so all ports and protocols are closed by default and only approved ports and protocols are opened based on a host to host basis.

Within this segment IdenTrust also employs network-based intrusion detection systems to identify and warn about attempts on equipment located within this tier of the infrastructure. The IDS sensors scan all traffic traversing the firewall interfaces to identify anomalies and malicious packets. If a packet appears to be malicious, the scanner immediately sends an alarm. All traffic is logged in the same manner as described within the CPS.

Also within this tier of the network, IdenTrust uses two load balancers/content management appliances, configured as a primary and hot standby, to provide load balancing to High Availability ("HA") hosts residing within the PKI Net. This gives fault-tolerance and stability to the PKI infrastructure. The load balancers are configured to distribute load based on service and host availability. Requests intended for HA hosts within the DMZ are passed to the active load balancer. These appliances serve as the gateway between the private and public sections of IdenTrust's DMZ.

Inner Tier – the Secure Segments

The secure segments of the PKI Network are also protected by redundant EAL-4 certified appliance firewalls, which are configured so all ports and protocols are closed by default, and only approved ports and protocols are opened on a host-to-host basis. Connections to the internal network space are proxied through the DMZ. Only limited access is allowed from the DMZ to the private networks.

The firewalls provide the only gateway between the outside and IdenTrust's secure network segments. Two additional switches provide the backbone to the private segments.

Services for All Tiers

IdenTrust has architected the network infrastructure incorporating the principles of Defense in Depth within all segments of the Infrastructure.

During the initial system setup and configuration, all unused ports are turned off. Any needed ports are then documented in a Security Checklist that is logged for each host and specifies the configuration for each server. IdenTrust limits services to the minimum required to run the CA, CSA, and database applications within the secure network environment.

IdenTrust uses Access Control Lists ("ACL") to limit the services configured at the boundary devices. The default configuration is to deny all services and to allow ports protocols and services by exception only. Ports, protocols, and services are permitted to cross boundaries only after a security assessment and review has been completed and approved by IdenTrust's Security Officer, as part of the formal firewall change request process.

IdenTrust uses approved firewall and IDS appliances for these functions; they are described more fully in Appendix G. Each of the appliances produces full auditing of security events, protection of security logs and identification & authentication with action upon authentication failure. The data communicated between the components is secured for confidentiality and integrity. IdenTrust uses Trusted Role access through a proxy for administrative functions of these firewalls. These firewalls utilize stateful packet

inspection on all sessions. IdenTrust utilizes proxies wherever possible and filters only as an exception. Any use of IP filters on the firewalls requires approval from an IdenTrust's Security Officer and Vice President of Operations or CIO. The firewalls use secure and robust filtering of IP packets based on flexible, admin-defined security policies, and perform protocol state tracking.

6.8 Time Stamping

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
- System audit journal entries

System time for servers providing CA, OCSP and CMA services are updated using the Network Time Protocol ("NTP") to synchronize system clocks at least once every 60 minutes. These servers reside within the boundary routers of IdenTrust. Trusted external time sources operated by government agencies are used to maintain an average accuracy of one (1) second or better. Clock adjustments are auditable events, see section 5.4.1.

7. Certificate and CRL Profiles

Section 10 contains the formats for the various Certificates and CRLs.

7.1 Certificate Profile

7.1.1 Version Numbers

All ECA Certificates issued by IdenTrust conform to version 3 of ITU-T X.509.

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in Section 10. The Certificate profiles listed in this CPS conform to the Certificate profile of the ECA CP. This CPS uses and incorporates here the Certificate profile of the ECA CP. The profiles in section 10 of this CPS and the tables in section 7.1.4 provide details and clarification consistent with the ECA CP's Certificate profiles. Any variances from the ECA CP are in accordance with the RFC 5280 and have been approved the EPMA.

The KeyUsage extension is the only extension in IdenTrust-issued ECA Certificates marked as critical. Section 7.1.9 notes some implications of that fact in relation to the CertificatePolicies.

Extended Key Usage is included in the Signing Certificate (Section 10.3), the Encryption Certificate (Section 10.4), and SSL Certificate (Section 10.5.1).

7.1.3 Algorithm Object Identifiers

IdenTrust-issued ECA Certificates will use the following OIDs for signatures.

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates under this Policy will use the following OID for identifying the algorithm for which the subject key was generated.

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

The IdenTrust ECA shall certify only public keys associated with the crypto-algorithms identified above, and shall only use the signature crypto-algorithms described above to sign Certificates, CRLs and OCSP responses.

7.1.4 Name Forms

As required in the Certificate profiles of the ECA CP, each ECA Certificate issued by IdenTrust contains two fields identifying the Subscriber, namely subject, which contains

a distinguished name, and the extension subjectAltName:RFC822Name (for Subscribers), the subjectAltName:uniformResourceIdentifier, the subjectAltName:dNSName, or the subjectAltName:iPAddress (for components). The Certificates also identify IdenTrust in the issuer field by its distinguished name as determined by the EPMA. The following tables specify the content and meaning of these names in detail.

7.1.4.1 Names Identifying the Subscriber

Identifier type:	***with data content of:***	***Indicates:***
Subject:CountryName (C)	The letters "US"	That the Certificate is issued by a PKI operated in the United States.
Subject:OrganizationName (O)	The words "U.S. Government"	That the ECA PKI is sponsored by an arm of the U.S. Government.
subject: OrganizationUnitName (OU)	The letters "ECA"	That the holder of the private key corresponding to the public key listed in the Certificate is a Subscribing Organization in the ECA PKI sponsored by the DOD.
subject: OrganizationUnitName (OU)	The word "IdenTrust,"	(1) That the Subscriber and/or Subscribing Organization is under contract with IdenTrust for public key Certificate issuance and revocation services, and (2) that the identifiers for the Subscriber are as specified in this CPS. This field does not does not provide a basis for inferring that IdenTrust is the Subscriber or imply any affiliation or relation between the IdenTrust and the Subscriber other than certification service provider pursuant to contract.
subject: OrganizationUnitName (OU)	Alphanumeric text	The name of the Subscribing Organization.

Identifier type:	*with data content of:*	*Indicates:*
subject:CommonName (CN)	Alphanumeric text including a colon character (ASCII 58) for Individual Subscribers. A colon is otherwise not permitted in the data content.	In the case of an Individual Subscriber (as opposed to a Component), the name by which the Individual Subscriber is commonly known[20] appears before the colon.[21] The disambiguating number described in section 3.1.5 appears after the colon. In the case of a Component Certificate, the fully qualified domain name of the component or device being certified. If the component is a web server, the URL is always listed in subjectAltName (see below). In the case of an OCSP Responder, the name of the Issuer CA followed by the words "OCSP Responder"
subjectAltName: rfc822name (in a Certificate issued to an Individual Subscriber)	For Individuals, the e-mail address in the form prescribed by [IETF RFC 822] (now superseded; see [IETF RFC 2822])	An e-mail address at which the Subscriber can receive messages via SMTP. An rfc822 name appears in Certificates issued to Individual Subscribers and Components; however, the e-mail address may be for that Individual Subscriber or one or more other persons in the Subscribing Organization.
subjectAltName:otherName: userPrincipalName (in a Certificate issued to an Individual Subscriber)	For Individuals, a unique user principal name, with a structure such as unique.name@domain, where unique name is a unique identifier and the domain is in the form prescribed by [IETF RFC 822]]	A user principal name used as a unique identifier within the Subscribing Organization, which reflect organizational structures and authorization to access the account. The otherName:userPrincipalName name appears in Certificates issued to Individual Subscribers that contain the ExtendedKeyUsage: smartCardLogon purpose.
subjectAltName: uniformResourceIdentifier (in a Component Certificate)	A URI (synonymous with URL) in the form prescribed by [IETF RFC 1630]	The URL of the component or device identified in the Certificate.

[20] The format of the Individual Subscriber's name is as in common usage, specifically:

1. The individual's given names in the order appearing in official documents or formal usage;
2. The individual's surname;
3. A name indicating generation such as "Jr." or "III".

In the event of uncertainty, IdenTrust will be guided by common usage in the Individual Subscriber's locale. The components of an Individual Subscriber's name are separated by space characters (ASCII 32).

[21] In the case of a Subscriber who is a human being, the CommonName is the name by which the person is known for business and/or employment purposes. It consists of at least a given name and the surname.

Identifier type:	*with data content of:*	*Indicates:*
subjectAltName:dNSName (in a Component Certificate) [22]	A fully qualified domain name	The domain name of the component or device identified in the Certificate.
subjectAltName:iPAddress (in a Component Certificate)	A sequence of four bytes (octets) (or 16 bytes for IPv6 addresses)	The IP address of the component or device identified in the Certificate.

Each attribute value in a subject DN will be encoded in a separate RDN. All RDNs will be encoded as printable string. The only exceptions to this rule can be the Subscriber name or Subscriber organization name when they cannot be encoded as printable string. In that case, the RDN that cannot be encoded as printable string will be encoded as UTF-8.

From the subject field, a Relying Party can infer based on the foregoing table either that:

The Individual Subscriber listed in commonName is affiliated with the Subscribing Organization as described in section 3.2.2.2; or

The device listed in the commonName of a Component Certificate is owned, operated, managed, or controlled by the Subscribing Organization, or that the Subscribing Organization has agreed with a contractor for the operation of the device and retains significant rights in relation to its operation see also section 3.2.2.3.

7.1.4.2 Names Identifying the Issuer

IdenTrust is identified in a Certificate as its Issuer by the following subfields within the issuer field:

Identifier type:	*with data content of:*	*indicates:*
CountryName (C)	The letters “US”	that the Certificate is issued by a PKI operated in the United States.
OrganizationName	The words “U.S. Government”	that the DOD, sponsor of the ECA PKI, is an arm of the US Government
OrganizationUnitName (OU)	The letters “ECA”	that IdenTrust is involved in the ECA PKI sponsored by the DOD. IdenTrust’s status as an ECA should be inferred by verifying the Certificate chain up to the ECA Root Certificate and not from this name field.
OrganizationUnitName (OU)	The words “Certification Authorities”	that IdenTrust is a Certification Authority

[22] The subjectAltName field of a Component Certificate contains at least one subfield but is not required to contain more than one.

Identifier type:	*with data content of:*	*indicates:*
CommonName (CN)	The words "IdenTrust ECA" or IdenTrust ECA S2" or IdenTrust Component S2"[23]	that IdenTrust issued the Certificate and type of CA (i.e., "S2" means SHA-2 hash, "Component" means dedicated issuance of Component)

Each attribute value in an issuer DN will be encoded in a separate RDN. All RDNs will be encoded as printable string.

7.1.5 Name Constraints

Not applicable.

7.1.6 Certificate Policy Object Identifier

ECA Certificates issued by IdenTrust assert the OID appropriate to the level of assurance with which it was issued, as specified in Section 1.2 of the ECA CP.

7.1.7 Usage of Policy Constraints Extension

No applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

End entity ECA Certificates issued by IdenTrust contain a CPS pointer qualifier populated with a URL pointing to the location of this CPS.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Consistent with section 7.1.9 of the ECA CP, the ECA Certificates issued by IdenTrust do not mark the certificatePolicies extension as critical. As the ECA CP provides, therefore, Relying Parties whose client software does not process the certificatePolicies extension act at their own risk.

The certificatePolicies extension indicates the ECA CP. The ECA CP requires each ECA to provide a CPS conforming to the ECA CP. This is that CPS for ECA Certificates issued by IdenTrust. This CPS is downloadable from the URL listed in the policy qualifier field of the certificatePolicies extension in each ECA Certificate issued by IdenTrust.

[23] The value of issuer:CommonName in a Certificate issued by IdenTrust (i.e. for SHA-1 "IdenTrust ECA [x]" or "IdenTrust ECA Component [x]"; and for SHA-256 "IdenTrust ECA S2[y]" or IdenTrust ECA Component [y]) matches exactly the value of subject:CommonName in the Certificate issued to IdenTrust by the ECA Root CA (i.e. for SHA-1 "IdenTrust ECA [x]" and for SHA-256 "IdenTrust ECA S2[y]").

7.2 CRL Profile

7.2.1 Version Numbers

ECA CRLs issued by IdenTrust conform to version 2 of [ITU X.509].

7.2.2 CRL and CRL Entry Extensions

ECA CRLs issued by IdenTrust conform to the CRL profiles listed in Section 10. Those profiles are consistent with those of the ECA CP.

7.3 OCSP Profile

Section 10 contains the format (profile) for OCSP requests and responses.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

All of IdenTrust's CMA operations used in performing ECA services as described in this CPS are audited annually, including internal RA functions.

The EPMA may also require one or more special, non-annual audits of IdenTrust's ECA-related operations following a statement of the reason for the additional audit.

8.2 Identity/Qualifications of Assessor

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 the firm's principal business activity. Moreover, the firm must have experience in auditing secure information systems and 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 PKIs, cryptography, certification systems, and the like, as well as Internet security issues (such as management of a security perimeter), operations of secure data centers, 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 in a competent manner.

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

(4) **Disinterest**: The firm must have no financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against IdenTrust.

(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) and require its audit professionals to do the same.

Moreover, in auditing secure information systems, the firm should be guided by generally accepted standards for evaluating secure information systems such as [ISO 27001:2013], Annex B of [ANSI X9.79], AICPA CA WebTrust Criteria, or AICPA SOC 2.

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. 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 auditing professional performing the audit must be certified or accredited as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA) or have other similarly recognized information security auditing credentials.

(2) **Primary responsibility**: The 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 professional active in auditing IdenTrust will conform to the [AICPA Code of Professional Conduct] and other professional rules of the AICPA.

(4) **Professional background**: The professionals assigned to audit IdenTrust must be trained to a standard generally accepted in the auditing field. They must 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 CPSs as well as to the [AICPA CA WebTrustCriteria], and familiarity with those documents is necessary for performing the audit.

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.

8.3 Assessor's Relationship to Assessed Entity

As noted in section 8.2, IdenTrust has a contractual relationship with the auditor for performance of the audit, but otherwise, they are independent, unrelated entities having no financial interest in each other. The AICPA Code of Professional Conduct requires the auditor to maintain a high standard designed to ensure impartiality and the exercise of independent professional judgment, subject to disciplinary action by the AICPA. In addition, the Sarbanes Oxley Act of 2002 regulates American auditors to ensure professional objectivity and independence. The auditor selected will be capable of providing an unbiased, independent evaluation of IdenTrust's compliance with this CPS.

8.4 Topics Covered by Assessment

IdenTrust's engagement of its auditors requires them to audit IdenTrust's ECA operations for conformity to the ECA CP and this CPS and any other MOAs between the ECA PKI and any other PKI, and to be as thorough as the ECA CP requires.

8.5 Actions Taken as a Result of Deficiency

On conclusion of the audit, the auditor sends a report of the outcome of the audit to IdenTrust and to the EPMA. That report notes discrepancies between IdenTrust's operations and the requirements of this CPS and the ECA CP. IdenTrust will notify the EPMA immediately of each such discrepancy and propose a remedy for each, and note the time necessary for completion of that remedy within seven (7) days of receipt. IdenTrust will abide by the EPMA's decision in relation to each discrepancy.

8.6 Communication of Results

IdenTrust provides public key Certificate issuance and revocation services in several projects, of which the ECA program is one. IdenTrust's audit covers all its operations, both for ECA and for other projects. That ECA audit report will be communicated to IdenTrust as well as to the EPMA. If a deficiency is found and a remedy determined as provided in the preceding section, the EPMA may require a special non-annual audit as permitted in section 8.1.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees for Certificate services provided by IdenTrust are either published in fee schedules produced by IdenTrust or are established contractually with Individual Subscribers and/or Relying Parties.

No fees will be charged for directory access for the purpose of retrieving Certificates that are valid at the time of access or the current CRL using implemented protocols (i.e., LDAP, HTTP and OCSP). However, IdenTrust reserves the right to charge for access to archived (i.e. invalid) Certificates, OCSP, or expired CRLs, and for enhanced Repository services, enhanced Certificate assurance, operational security and service levels, consultation and implementation assistance, training, and other services. These fees will be published or agreed in separate documents.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No Stipulation.

9.2.2 Other Assets

No Stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No Stipulation.

9.2.4 Fiduciary Relationships

Issuance of Certificates as described in this CPS does not make IdenTrust, or any Registration Authority, an agent, fiduciary, trustee, or other representative of Subscribers or Relying Parties.

9.3 Confidentiality of Business Information

9.3.1 Scope of Business Confidential Information

Not applicable. The ECA shall not collect business confidential information.

9.3.2 Information Not Within the Scope of Business Confidential Information

Not applicable. The ECA shall not collect business confidential information.

9.3.3 Responsibility to Protect Business Confidential Information

Not applicable. The ECA shall not collect business confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

IdenTrust protects all Subscriber identifying information in accordance with its Privacy Policy stated at http://www.identrust.com/privacy.html. All Subscriber identifying information is maintained in accordance with applicable laws.

9.4.2 Information Treated as Private

IdenTrust obtains certain sensitive information from Subscribers in providing public key Certificate issuance and revocation services. That information includes contact and personal identity information that is not publicly available in a Certificate, billing and payment details, and sometimes information gained in the course of providing consulting, implementation, sales or other support services to the Subscribing Organization. The agreement between IdenTrust and the Subscribing Organization restricts IdenTrust's use and disclosure of that information. Access to sensitive Subscriber-related information within IdenTrust is limited to IdenTrust employees acting in Trusted Roles, other trusted employees within IdenTrust, and IdenTrust's and the EPMA's auditors on a need-to-know basis. Access to that information stored within IdenTrust customer databases is limited using the logical access controls placed on the database structure, role-based access control limits and rights allocated to those databases and tables established based on need-to-know. Logical and physical securities of confidential information are discussed in sections 5 and 6 of this CPS.

9.4.3 Information Not Deemed Private

A Certificate should only contain information that is relevant and necessary to effect secure transactions with the Certificate. Thus, information in a Certificate is not considered private or privacy act information.

9.4.4 Responsibility to Protect Private Information

IdenTrust does not disclose Certificate-related or background check private information to any third party unless authorized by the CP, required by law, government rule or regulation, or order of a court of competent jurisdiction. IdenTrust authenticates all requests for release of information. This section 9.4.4 does not preclude IdenTrust from disclosing the contents of Certificates and Certificate status information (e.g., CRL, OCSP requests and responses).

9.4.5 Notice and Consent to Use Private Information

All notices shall be in accordance with the applicable laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

IdenTrust may release sensitive information as part of judicial or administrative process, or to law enforcement officials as required by law, or pursuant to government rule or regulation, or pursuant to an order of a court or an administrative tribunal reasonably believed by its counsel to have jurisdiction after due review of the relevant documents and circumstances. All disclosure shall be in accordance with applicable laws.

9.4.7 Other Information Disclosure Circumstances

There are no other circumstances under which confidential information is released.

9.5 Intellectual Property Rights

Subscribers and their Subscribing Organizations maintain ownership of their respective public keys and Certificates. A private key will be treated as the sole property of the legitimate holder of the Certificate containing the corresponding public key and their Subscribing Organizations. IdenTrust will provide escrow services for encryption private keys as required by the ECA CP under the controls stipulated in Section 4.12. Subscribers and their organizations authorize IdenTrust to manage the escrowed private keys in accordance with section 5.5.2.

This CPS and related documentation are the intellectual property of IdenTrust, protected by trademark, copyright and other laws regarding intellectual property, and may be used only pursuant express permission from IdenTrust. Any other use of the above without the express written permission of IdenTrust is expressly prohibited.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

In acting as an ECA, IdenTrust will:

(1) Submit this CPS to the EPMA for conformance assessment. IdenTrust will also submit any proposed amendment to this CPS to the EPMA for conformance assessment. After the EPMA has approved this CPS, IdenTrust publishes it by posting a public version of this CPS on its web site. This CPS is subject to change in the manner set out in sections 1.5.4 and 9.12.

(2) Conform to CP and CPS: IdenTrust will conform to the applicable stipulations of the ECA CP and this CPS in providing its CMA services.

(3) Ensure Registration Authorities comply with CP: IdenTrust will ensure that the performance of its RA functions conforms to the requirements of this CPS and the ECA CP. IdenTrust will also provide documentation and training to personnel, and take other

reasonable action, to ensure that they understand their obligations, including obligations to comply with the CP and this CPS.

(4) Confirm accuracy of information: Before issuing an ECA Certificate, IdenTrust will Confirm the accuracy of the facts to be represented in that Certificate as required in this CPS and the CP. IdenTrust is thereby obligated to include only accurate and appropriate information in each ECA Certificate issued by IdenTrust, and to maintain evidence that IdenTrust has exercised due diligence in confirming the information contained in an ECA Certificate that the IdenTrust ECA has issued.

(5) Impose obligations on Subscribers: Before a Certificate issued to a Subscriber becomes Valid, IdenTrust will ensure that the obligations of section 9.6.3 of this CPS are imposed on that Subscriber consistent with the ECA CP. IdenTrust informs Subscribers of the obligations imposed on them and provides documentation and customer support accordingly. IdenTrust also informs Subscribers of the consequences of non-compliance with Subscriber obligations.

(6) Revoke Certificates: IdenTrust will revoke Certificates of Subscribers found to have acted in a manner contrary to Subscriber obligations. Section 4.9.1 accordingly permits IdenTrust to revoke a Subscriber's Certificate when the Subscriber breaches a relevant agreement or when such an agreement terminates.

(7) Provide notice: IdenTrust will notify Subscribers and make public for the benefit of Subscribers and Relying Parties any changes to its ECA operations that may impact interoperability or security. Generally, that notice is given by amending this CPS and publishing it as required in section 2.2 of this CPS.

(8) Provide Repository services: IdenTrust will provide on-line Repository services that satisfy the obligations under Section 2.2 of the ECA CP. IdenTrust does not use a Repository service provider to perform those services.

(9) Publish Certificates and CRLs: IdenTrust will publish Certificates and CRLs to the Repository that it provides; see sections 2.2 and 4.9.7. IdenTrust also publishes notices of revocation via OCSP as described in section 4.9.9.

9.6.2 RA Representations and Warranties

As a Registration Authority performing registration functions in support of IdenTrust's public key Certificate issuance and revocation services, IdenTrust is required to do the following, among other things:

(1) Comply with the applicable requirements of the ECA CP and this CPS.

(2) Perform Certificate request and revocation functions only with persons appointed to Trusted Roles, who understand the applicable requirements and are required to perform accordingly. Those certification functions include the request to issue Certificates, approval of request to issue Certificates, request to revoke Certificates, and approval of request to revoke Certificates.

(3) Confirm the accuracy of information provided in the Subscriber's Certificate request and application, as well as other information provided for inclusion in a Certificate to be issued by IdenTrust.

(4) Confirm that the Subscriber actually requested a Certificate and that the Subscriber's request is authentic, before forwarding the request to the CA for issuance of a Certificate.

9.6.3 Subscriber Representations and Warranties

Subscribers shall:

- Accurately represent themselves in all communications with the PKI;
- Protect their private keys at all times, in accordance with this policy, as stipulated in their Certificate acceptance agreements, and local procedures;
- Use their private keys only on the machines that are protected and managed using commercial best practices;
- Notify IdenTrust, in a timely manner, upon suspicion that their private keys are compromised or lost. Such notification shall be made directly or indirectly through mechanisms consistent with the ECA CP and this CPS;
- Notify IdenTrust, in a timely manner, of any changes to the information contained in their Certificates and
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and Certificates.

PKI Sponsors (as described in section 3.2.3.3) assume the obligations of Subscribers for the Certificates associated with their components.

9.6.4 Relying Party Representations and Warranties

Parties who rely upon the Certificates issued under the ECA CP shall:

- Perform a risk analysis to decide whether the level of assurance provided by the Certificate is adequate to protect the Relying Party based upon the intended use;
- Use the Certificate for the purpose for which it was issued, as indicated in the Certificate information (e.g., the key usage extension);
- Establish trust in the Certificate using certification path validation procedures described in [RFC 5280], prior to reliance; and
- 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. Note: data format changes associated with application upgrades may invalidate digital signatures and shall be avoided.

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 ECA Representations and Warranties

IdenTrust, acting as the subordinate CA, hereby warrants, solely to "IdenTrust-related Participants in the DOD ECA PKI" (as defined on the cover page of this CPS), that its procedures are implemented in accordance with the ECA CP and this CPS, and that any

Certificates issued that assert the policy OIDs identified in this CPS were issued in accordance with the stipulations of the ECA CP and this CPS.

IdenTrust hereby warrants, solely to "IdenTrust-related Participants in the DOD ECA PKI," that any RA or Trusted Correspondent will operate in accordance with the applicable sections of the ECA CP and this CPS.

9.6.5.2 Repository Representations and Warranties

Repositories that support IdenTrust in posting information as required by the ECA CP shall:

- Maintain availability of the information as required by the Certificate information posting and retrieval stipulations of the ECA CP; and
- Provide access control mechanisms sufficient to protect Repository information as described in Section 2.4.

9.6.5.3 Trusted Correspondent Representations and Warranties

A Trusted Correspondent shall perform Subscriber identity verification in accordance with this CPS and the ECA CP.

9.6.5.4 CSA Representations and Warranties

A CSA who provides revocation status and/or complete validation of Certificates that assert one of the policy OIDs defined in this document shall conform to the stipulations of this document and the ECA CP, including:

- Providing to the EPMA a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of the ECA CP and this CPS;
- Ensuring that Certificate and revocation information is accepted only from valid ECAs; and
- Providing only valid and appropriate responses and maintaining evidence that due diligence was exercised in validating the Certificate status.

A CSA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5 of the CP.

9.6.5.5 PKI Point of Contact Representations and Warranties

A Subscriber Organization may appoint a PKI Point of Contact (POC) (e.g. a Trusted Internal Correspondent, Personnel Office representative, Security Officer, etc.) to provide a single trusted point of contact with IdenTrust. The PKI POC shall comply with the stipulations of the ECA CP and this CPS. The PKI POC may request revocation of Certificates issued to the Subscribers within the POC organization. The PKI POC may receive Subscriber hardware Cryptographic Modules for zeroization and/or destruction.

A PKI POC who is found to have acted in a manner inconsistent with the stipulations of the ECA CP or this CPS is subject to removal as PKI POC. Failure to address the

deficiencies of the PKI POC may result in revocation of any or all Certificates issued to the Subscriber organization.

9.7 Disclaimers of Warranties

Except to the extent that the ECA CP, this CPS, or other applicable law require otherwise, 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.

IDENTRUST SHALL HAVE NO LIABILITY FOR LOSS DUE TO USE OF AN IDENTRUST-ISSUED ECA CERTIFICATE, UNLESS THE LOSS IS PROVEN TO BE A DIRECT RESULT OF A BREACH BY IDENTRUST AND IDENTRUST'S AGENTS OF THIS CPS OR A PROXIMATE RESULT OF THE NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT OF IDENTRUST AND IDENTRUST'S AGENTS.

IN NO EVENT SHALL IDENTRUST BE LIABLE FOR ITS ACTS OR THE ACTIONS OF ITS AGENTS FOR ANY CONSEQUENTIAL, INDIRECT, REMOTE, EXEMPLARY, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR BUSINESS INTERRUPTION, LOSS OF PROFITS, REVENUES, SAVINGS, OPPORTUNITIES OR DATA, OR INJURY TO CUSTOMER RELATIONSHIPS, REGARDLESS OF THE FORM OF ACTION AND REGARDLESS OF WHETHER THEY WERE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IDENTRUST SHALL INCUR NO LIABILITY FOR ITS ACTIONS OR THE ACTIONS OF ITS AGENTS IF THEY ARE PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMIT 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 THEM OR ANY ACT OF GOD, EMERGENCY CONDITION OR WAR OR OTHER CIRCUMSTANCE BEYOND THEIR CONTROL.

Section 9.13 of this CPS provides a claims and dispute resolution procedure and limits remedies accordingly.

9.8 Limitations of Liability

9.8.1 Loss Limitation

IdenTrust's entire liability, in law or in equity, for losses due to its operations at variance with its procedures defined in this CPS shall not exceed the following limits:

- One thousand U.S. dollars (USD $1,000) for all recoverable losses sustained by each person, whether natural or legal, as a result of a single transaction involving the reliance upon or use of a Certificate.
- One million U.S. dollars (USD $1,000,000) maximum total liability for all recoverable losses sustained by all persons as a result of a single incident

(i.e. the aggregate of all transactions arising out of the reliance upon or use of a Certificate).

IdenTrust disclaims any liability for loss due to use of Certificates it issues, if the Certificate was issued in accordance with the ECA CP and this CPS.

9.8.2 Other Exclusions

No stipulation.

9.8.3 US Federal Government Liability

As provided in the ECA CP, Subscribers and Relying Parties shall have no claim against the US Federal Government arising from use of the Subscriber's Certificate or a Certificate Management Authority's determination to terminate a Certificate. In no event will the Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any Certificate issued or revoked by a CA approved under the ECA CP.

As an ECA acting pursuant to the ECA CP, IdenTrust has no claim for loss against the EPMA, including but not limited to the revocation of IdenTrust's ECA Certificate issued by the ECA Root CA.

Subscribers and Relying Parties shall have no claim against the US Federal Government arising from erroneous Certificate status information provided by the servers and services operated by IdenTrust as an ECA and by the US Federal Government.

9.9 Indemnities

Neither IdenTrust nor its agents (e.g., RA Operators, Trusted Correspondents, etc.) assume financial responsibility for improperly used Certificates.

9.10 Term and Termination

9.10.1 Term

This CPS shall remain in effect until a new CPS is approved by the EPMA or the conditions and effect resulting from a termination of this document are communicated via IdenTrust's Repository.

9.10.2 Termination

The requirements of this CPS remain in effect through the end of the archive period for the last Certificate issued. The conditions and effect resulting from any termination of this document will be communicated via IdenTrust's Repository.

9.10.3 Effect of Termination and Survival

The responsibilities for protecting business confidential and personal information, and for protecting the respective participants' intellectual property rights shall survive termination of this CPS.

9.11 Individual Notices and Communications with Participants

All parties shall use commercially reasonable methods to communicate with each other.

9.12 Amendments

9.12.1 Procedure for Amendment

This CPS will be reviewed by IdenTrust from time to time. Errors, updates, or suggested changes to this document should be communicated to helpdesk@IdenTrust.com. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change. The EPMA shall review this CPS from time to time.

9.12.2 Notification Mechanism and Period

Any changes to this CPS will be submitted to the EPMA for approval. Notice of changes to this CPS will be provided by publication of a revised CPS at: https://secure.identrust.com/Certificates/policy/eca/.

9.12.3 Circumstances Under Which OID Must be Changed

A policy OID for Certificates issued pursuant to this CPS should change only if the change in the ECA CP results in a material change to the trust by the relying parties.

9.13 Dispute Resolution Provisions

As provided in the ECA CP, the EPMA shall be the sole arbiter of disputes over the interpretation or applicability of the ECA CP. Other disputes arising from the operation of the IdenTrust ECA shall be resolved as provided in this section.

If a Subscriber, Relying Party or Subscribing Organization of a Certificate issued under this CPS is an individual employed by or acting on behalf of the United States Government, a dispute arising in connection with such a Certificate shall be resolved under applicable Federal law. If the United States Government has purchased a service or a Certificate provided under this CPS, a dispute arising in connection with such service or Certificate, and asserted on behalf of any such entity shall be resolved under the Contract Disputes Act of 1978, as amended (41 U.S.C. § 601 et. seq.).

Where the Subscriber, Relying Party or Subscribing Organization is not the United States Government or a Government employee, the dispute resolution procedures specified in

this section shall provide the sole remedy for any claim against IdenTrust for any loss sustained by such party, whether that loss is claimed to arise from reliance on a Certificate, from breach of a contract, from a failure to perform according to the ECA CP and/or this CPS, or from any other act or omission. No such Relying Party, Subscriber, or Subscribing Organization shall require IdenTrust to respond to any attempt to seek recourse through any other means.

9.13.1 Claims and Claim Determinations

Before making a claim to recover a loss for which IdenTrust may be responsible, a Subscriber, Relying Party, or Subscribing Organization that is not the United States Government or a Government employee (the "Claimant") shall make a thorough investigation. IdenTrust will cooperate reasonably in that investigation. The Claimant will then present to IdenTrust Appeal Officer reasonable documented proof:

- That the Claimant has suffered a recoverable loss as a result of a transaction;
- Of the amount and extent of the recoverable loss claimed; and
- Of the causal linkage between the alleged transaction and the recoverable loss claimed, itemized as necessary.

Upon the occurrence of any loss arising out of a transaction, the Claimant shall file notice and all required proof of the claim using a procedure accessed through IdenTrust's web site not later than one year after the date of discovery of the facts out of which the claim arose. Notice of the claim must be given on a form downloadable from https://secure.identrust.com/federal/eca/claim-form-loss.html. Instructions for completion and submission of the claim form also appear on that web page.

On receipt of a claim form, IdenTrust may determine to pay the claim or deny it. IdenTrust may also pay the claim in an amount less than the amount claimed if IdenTrust determines that the loss calculations exceed the amount that IdenTrust is obligated to pay. IdenTrust will notify the Claimant of its determination within 30 days of receipt of the claim form.

If the Claimant is not satisfied with IdenTrust's determination of the claim, the Claimant may seek judicial relief as provided in the next section.

9.13.2 Judicial Review

A Relying Party, Subscriber, or Subscribing Organization who is not the U.S. Government may contest the determination of the claim by IdenTrust under section 9.13.1 by filing suit as provided herein within one year after IdenTrust's determination of the claim.

The courts of the State of Utah have exclusive subject matter jurisdiction over all suits and any other disputes arising out of or based on this CPS, including suits for judicial review of claims decided according to section 9.13.1.

9.14 Governing Law

The laws of the United States of America will govern the enforceability, construction, interpretation, and validity of this CPS relative to the ECA CP and the Memorandum of Agreement between the EPMA and IdenTrust. With respect to US Government Subscribers or US Government Relying Parties, this CPS and its interpretation shall be governed by the Contracts Disputes Act of 1978, as amended (41 US.C. § 601 et seq.). In all other cases, the law of the State of Utah shall govern the enforceability, construction, interpretation, and validity of this CPS, without reference to its rules regarding conflicts of laws.

In the event of any conflict between the ECA CP and this CPS, the ECA CPS shall control. Except to the extent prohibited by law, in the event of any conflict between this CPS or the ECA CP, on the one hand, and any Subscriber Agreement, Subscribing Organization Agreement, or other document issued or agreement entered into by IdenTrust in connection with the performance of services under this CPS, on the other hand, the ECA CP, or this CPS, respectively, shall control. The provisions of this CPS cannot be overridden, bypassed or changed by any document issued or agreement entered into by IdenTrust in connection with the performance of services under this CPS.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS shall constitute the entire understanding and agreement between the parties with respect to the transactions contemplated, and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement or communication concerning the subject matter hereof. No party is relying upon any warranty, representation, assurance or inducement not expressly set forth herein and none shall have any liability in relation to any representation or other assurance not expressly set forth herein, unless it was made fraudulently. Without prejudice to any liability for fraudulent misrepresentation, no party shall be under any liability or shall have any remedy in respect of misrepresentation or untrue statement unless and to the extent that a claim lies for breach of a duty set forth in this CPS.

9.16.2 Assignment

Parties may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of IdenTrust.

9.16.3 Severability

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

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

No stipulation.

9.16.5 Force Majeure

IDENTRUST SHALL INCUR NO LIABILITY IF IT 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; CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT ITS OWN FAULT OR NEGLIGENCE.

9.17 Other Provisions

No stipulation.

10. Certificate and CRL Formats

Fields defined for Certificates in standards such as [ITU X.509] are not used in End-Entity ECA Certificates issued by IdenTrust, if those fields do not appear in the tables below.

10.1 ECA Root CA Self-Signed Certificate

The profile for the ECA Root Certificate is as specified in Section 10.1 of the ECA CP.

10.2 Subordinate CA Certificates

The profile for the Subordinate CA Certificates is as specified in Section 10.2 of the ECA CP with the exception of the Subject DN which is defined by IdenTrust. See section 7.1.4.2 for interpretation of the other elements of this distinguished name.

10.3 Signing Certificate (Identity Certificate)

Two profiles tables are provided for a signing Certificate. The first profile table supports an implementation using SHA-1 as the signing algorithm. The second profile table supports SHA-256 as the signing algorithm. The second table is not comprehensive; instead it shows the fields and extensions that should be modified in the first table.

Signing Certificate Profile for SHA-1 Implementation

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
Version	n/a	v3 only (indicated by the integer "2")	Indicates the version of [ITU-T X.509] to which the Certificate conforms.
serialNumber	n/a	An integer unique to the Certificate among the range of all serial numbers in ECA Certificates issued by the IdenTrust ECA.	The serial number of the Certificate in question.
Issuer's Signature	n/a	The subfield *algorithmIdentifier: algorithm* must contain the object identifier (specified in ECA CP and [IETF RFC 5280]) for SHA-1. {1.2.840.113549.1.1.5}	Indicates the algorithm used by IdenTrust to sign the Certificate, which is SHA-1 with RSA Encryption.
Issuer	n/a	cn=IdenTrust ECA[X], ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US	Identifies the certificationauthority which signed this Certificate; see section 7.1.4.2 [X] = Iteration of IdenTrust ECA CA (e.g., ECA 1, ECA 2, etc.)
Validity	n/a	The subfields notBefore and notAfter contain dates in the form	NotBefore indicates the date on which the Certificate begins to be valid and notAfter indicates when it ceases to be

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
		specified for UTC Time in [IETF RFC 5280].	valid. Years are listed as specified in [IETF RFC 5280]. The time interval listed may be 1, 2, 3 years, or less, but shall not exceed 3 years.
Subject	n/a	cn=[FirstName MI Last Name:UID], ou=[OrganizationUnitName], ou=IdenTrust, ou=ECA, o=U.S. Government, c=US	As explained in section 3.1.5, IdenTrust appends a disambiguating number after the colon character in the subject:CommonName field, and as specified in section 7.1.4.1, OrganizationUnitName is the name of the Subscribing Organization.
subjectPublicKey-Info	n/a	The subfield *algorithmIdentifier: algorithm* contains the object identifier for RSA Encryption. The length of the public key in *subjectPublicKey* is 1024 bits for Certificates issued off the IdenTrust ECA 1 subordinate CA and 2048 bits for all Certificates issued off subsequent subordinate CAs.	*SubjectPublicKey* is the Subscriber's public key, and *algorithmIdentifier* indicates the algorithm to use with it.
Extension	***Critical***	***Data Content Requirements***	***Significance***
authorityKeyIdenti-fier	No	The subfield *keyIdentifier* contains the 20-byte SHA-1 hash of the DER-encoded public key by which the issuer's signature on the Certificate can be verified. The other subfields of *authorityKeyIdentifier* are not used.	Indicates which public key to use in verifying the authenticity of the Certificate.
subjectKeyIdenti-fier	No	The subfield *keyIdentifier* contains the 20-byte SHA-1 hash of the DER-encoded public key listed in *subjectPublic-KeyInfo:subjectPublicKey*.	The subfield *keyIdentifier* labels the public key of this Certificate for convenient reference and to help prevent confusion with other key pairs that the same Subscriber may have.
keyUsage	Yes	Bit 0 and bit 1 of the bitstring are set to true; all others are set to false.[24] digitalSignature, nonRepudation.	Indicates to software applications using the key what the key is to be used for (see [ITU X.509] and [IETF 5280]). This field is to signal to applications how to use the Certificate and the corresponding private key.
ExtendedkeyUsag e	No	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; id-kp-emailProtection {1.3.6.1.5.5.7.3.4};	Indicates to software applications for what purposes the key can be used .

[24] A value of true for Bit 1 indicates that the Certificate may be used for a "nonrepudiation service", which is defined in [IETF RFC 5280] section 4.2.1.3 as "protect[ing] against the signing entity falsely denying some action", such as a digital signature verifiable by reference to the Certificate. Whether this *technical* "nonrepudiation" *legally* prevents a digital signer from denying a signature depends on more than simply setting this bit to "true". This bit is a signal to digital verification software on how to use the Certificate rather than a basis for legal inferences, which would have to be grounded in additional facts and circumstances as well as in the applicable law.

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
		smartCardLogon[25] {1.3.6.1.4.1.311.20.2.2};MSFT Document Signing[26] {1.3.6.1.4.1.311.10.3.12}; Adobe Certified Document Signing[27] {1.2.840.113583.1.1.5}	
certificatePolicies	No	*The PolicyInformation:policyIdentifier* subfield contains an OID specified below as appropriate for the type of Certificate. OIDs are: {2.16.840.1.101.3.2.1.12.1} for Medium Assurance Certificate Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html **or** {2.16.840.1.101.3.2.1.12.2} for Medium Hardware Assurance Certificate Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html **or** {2.16.840.1.101.3.2.1.12.3} for Medium Token Assurance Certificate Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html	The ECA CP applies in relation to this Certificate, and that the Certificate is of the type indicated in section 1.2. See also section 1.4 on Certificate Usage.
subjectAltName	No	A subfield as specified in section 7.1.4.1.	As stated in section 7.1.4.1.
authorityInforma-tionAccess	No	The subfield AccessDescription contains either one or two paired subfields. Each pair contains an accessLocation and accessMethod. OIDs for indicating access methods are as defined in IETF RFC 5280. One accessLocation lists the URI of the Certificate issued to	Access Method 1.3.6.1.5.5.7.48.2 is cAIssuers, which provides a pointer

[25] The smartCardLogon purpose is optional. When this purpose is included in the EKU extension, the User Principal Name in the Subject Alternative Extension is also included in accordance with naming guidelines in Section 7.1.4.1.

[26] The MSFT Document Signing purpose is optional.

[27] The Adobe Certified Document Signing purpose is optional.

Field Name	Critical?	Data Content Requirements	Significance
		IdenTrust by the ECA Root CA and the method for accessing that URL: [1] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = ldap://ldap[eca].identrust.com/cn%3DIdenTrust%20ECA%20[X]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?cACertificate;binary} [2] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = http://apps.identrust.com/roots/identrusteca[X].cer}	reference to the current Certificate issued to IdenTrust by the ECA Root CA. [X] = Iteration of IdenTrust ECA CA (e.g., ECA 1, ECA 2, etc.) Information related to ECA 1 will be published to and continue to be available at ldap.identrust.com until expiration of all Certificates issued by ECA 1. This information will also be published to ldapeca.identrust.com.
		An additional accessLocation will be present if and when an OCSP Responder is available for the Certificate. The responder's URL appears with OCSP as the appropriate access method, as prescribed in [IETF RFC 2560]. accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation ::= { URL = http://eca.ocspts.identrust.com} for the 1,024 bit length subordinate CAs or accessLocation ::= { URL = http://eca.ocsp.identrust.com} for all subsequent subordinate CAs	Access Method 1.3.6.1.5.5.7.48.1 is OCSP, which provides a pointer to the OCSP Responder for the Certificate. The content and format of OCSP requests and responses is specified in sections 10.11 and 10.12.
CRLDistribution-Points	No	The subfield *DistributionPointName* contains LDAP and HTTP URLs pointing to the appropriate CRL. [1] URL = ldap://ldap[eca].identrust.com/cn%3DIdenTrust%20ECA%20[X]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?certificateRevocationList;binary [2] URL = http://crl.identrust.com/eca/identrusteca[X].crl	Points to URLs where more information about the post-issuance validity or reliability of a Certificate may be available. [X] = Iteration of IdenTrust ECA CA (e.g., ECA 1, ECA 2, etc.) Information related to ECA 1 will be published to and continue to be available at ldap.identrust.com until expiration of all Certificates issued by ECA 1. This information will also be published to ldapeca.identrust.com.
SubjectDirectoryAttributes	No	This subfield CountryOfCitizenship contains a two-character PrintableString listing an ISO 3166 Country Code.	The citizenship of the Subscriber. . Multiple citizenships may be asserted in multiple instances of the attribute.

Signing Certificate Profile for SHA-256 Implementation

The following fields are different for SHA-256 implementation.

Field Name	***Critical?***	***Data Content Requirements***	***Significance***
Issuer's Signature	n/a	The subfield *algorithmIdentifier: algorithm* must contain the object identifier (specified in ECA CP and [IETF RFC 5280]) for SHA-256 {1.2.840.113549.1.1.11}	Indicates the algorithm used by IdenTrust to sign the Certificate, which is SHA-256 with RSA Encryption
Issuer	n/a	cn=IdenTrust ECA S2[Y], ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US	Identifies the Certification Authority which signed this Certificate; see section 7.1.4.2 [Y] = Iteration of IdenTrust ECA CA S2, starting with zero (0) (e.g., ECA S20, ECA S21, etc.)
Extension	***Critical***	***Data Content Requirements***	***Significance***
certificatePolicies	No	*The PolicyInformation:policyIdentifier* subfield contains an OID specified below as appropriate for the type of Certificate. OIDs are: {2.16.840.1.101.3.2.1.12.4} for Medium Assurance SHA-256 Certificate Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html **or** {2.16.840.1.101.3.2.1.12.5} for Medium Token SHA-256 Assurance Certificate Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html	The ECA CP applies in relation to this Certificate, and that the Certificate is of the type indicated in section 1.2. See also section 1.4 on Certificate Usage.
authorityInforma-tionAccess	No	The subfield AccessDescription contains either one or two paired subfields. Each pair contains an accessLocation and accessMethod. OIDs for indicating access methods are as defined in IETF RFC 5280. One accessLocation lists the URI of the Certificate issued to IdenTrust by the ECA Root CA for SHA-256 and the method for accessing that URL: [1] accessMethod ::={1.3.6.1.5.5.7.48.2}	Access Method 1.3.6.1.5.5.7.48.2 is caIssuers, which provides a pointer reference to the current Certificate issued to IdenTrust by the ECA root for SHA-256 CA. [Y] = Iteration of IdenTrust ECA CA S2, starting with zero (0) (e.g., ECA S20, ECA S21, etc.)

Field Name	Critical?	Data Content Requirements	Significance
		accessLocation ::= {URL = ldap://ldapeca.identrust.com/cn%3DIdenTrust%20ECA%20S2[Y]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?cACertificate;binary} [2] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = http://apps.identrust.com/roots/identrustecas2[Y].cer} An additional accessLocation will be present if and when an OCSP Responder is available for the Certificate. The responder's URL appears with OCSP as the appropriate access method, as prescribed in [IETF RFC 2560]. accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation ::= { URL = http://eca2.ocsp.identrust.com} for all subsequent subordinate CAs	Access Method 1.3.6.1.5.5.7.48.1 is OCSP, which provides a pointer to the OCSP Responder for the Certificate. The content and format of OCSP requests and responses is specified in sections 10.11 and 10.12.
CRLDistribution-Points	No	The subfield *DistributionPointName* contains LDAP and HTTP URLs pointing to the appropriate CRL. [1] URL = ldap://ldapeca.identrust.com/cn%3DIdenTrust%20ECA%20S2[Y]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?certificateRevocationList;binary [2] URL = http://crl.identrust.com/eca/identrustecas2[Y].crl	Points to URLs where more information about the post-issuance validity or reliability of a Certificate may be available. [Y] = Iteration of IdenTrust ECA CA S2, starting with zero (0) (e.g., ECA S21, ECA S22, etc.)

10.4 Encryption Certificate

End-entity Encryption Certificates have the same content as specified in the preceding section, except that the third bit (numbered 2) of the keyUsage field is set to true. All other bits of that field are set to false.

Two profile tables are provided for an encryption Certificate. The first profile table supports an implementation using SHA-1 as the signing algorithm. The second profile table supports SHA-256 as the signing algorithm. The second table is not comprehensive; instead it shows the fields and extensions that should be modified in the first table.

Encryption Certificate Profile for SHA-1 Implementation

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
Version	n/a	v3 only (indicated by the integer "2")	Indicates the version of [ITU-T X.509] to which the Certificate conforms.
serialNumber	n/a	An integer unique to the Certificate among the range of all serial numbers in ECA Certificates issued by the IdenTrust ECA.	The serial number of the Certificate in question.
Issuer's Signature	n/a	The subfield *algorithmIdentifier: algorithm* must contain the object identifier (specified in ECA CP and [IETF RFC 5280]) for SHA-1 {1.2.840.113549.1.1.5}	Indicates the algorithm used by IdenTrust to sign the Certificate, which is SHA-1 with RSA Encryption.
Issuer	n/a	cn=IdenTrust ECA[X], ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US	Identifies the Certification Authority which signed this Certificate; see section 7.1.4.2 [X] = Iteration of IdenTrust ECA CA (e.g., ECA 1, ECA 2, etc.)
Validity	n/a	The subfields notBefore and notAfter contain dates in the form specified for UTC Time in [IETF RFC 5280].	NotBefore indicates the date on which the Certificate begins to be valid and notAfter indicates when it ceases to be valid. Years are listed as specified in [IETF RFC 5280]. The time interval listed may be 1, 2, 3 years, or less, but shall not exceed 3 years.
Subject	n/a	cn=[FirstName MI Last Name:UID], ou=[OrganizationUnitName], ou=IdenTrust, ou=ECA, o=U.S. Government, c=US	As explained in section 3.1.5, IdenTrust appends a disambiguating number after the colon character in the subject:CommonName field, and as specified in section 7.1.4.1, OrganizationUnitName is the name of the Subscribing Organization.
subjectPublicKey-Info	n/a	The subfield *algorithmIdentifier: algorithm* contains the object identifier for RSA Encryption. The length of the public key in *subjectPublicKey* is 2048 bits for all	*SubjectPublicKey* is the Subscriber's public key, and *algorithmIdentifier* indicates the algorithm to use with it.

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
		Certificates issued off subordinate CAs.	
Extension	***Critical***	***Data Content Requirements***	***Significance***
authorityKeyIdenti-fier	No	The subfield *keyIdentifier* contains the 20-byte SHA-1 hash of the DER-encoded public key by which the issuer's signature on the Certificate can be verified. The other subfields of *authorityKeyIdentifier* are not used.	Indicates which public key to use in verifying the authenticity of the Certificate.
subjectKeyIdenti-fier	No	The subfield *keyIdentifier* contains the 20-byte SHA-1 hash of the DER-encoded public key listed in *subjectPublic-KeyInfo:subjectPublicKey*.	The subfield *keyIdentifier* labels the public key of this Certificate for convenient reference and to help prevent confusion with other key pairs that the same Subscriber may have.
keyUsage	Yes	The third bit (bit 2) of the bitstring is set to true; all others are set to false. keyEncipherment.	Indicates to software applications using the key what the key is to be used for (see [ITU X.509] and [IETF 5280]). This field is to signal to applications how to use the Certificate and the corresponding private key.
ExtendedkeyUsag e	No	id-kp-emailProtection {1.3.6.1.5.5.7.3.4}; Encrypting File System[28] {1.3.6.1.4.1.311.10.3.4}	Indicates to software applications using the key for what purposes the key can be used.
certificatePolicies	No	*The PolicyInformation:policyIdentifier* subfield contains an OID specified below as appropriate for the type of Certificate. OIDs are: {2.16.840.1.101.3.2.1.12.1} for Medium Assurance Certificate Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html **or** {2.16.840.1.101.3.2.1.12.2} for Medium Hardware Assurance Certificate Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html **or** {2.16.840.1.101.3.2.1.12.3} for Medium Token Assurance Certificate Policy Qualifier Id=CPS	The ECA CP applies in relation to this Certificate, and that the Certificate is of the type indicated in section 1.2. See also section 1.4 on Certificate Usage.

[28] The Encrypting File System purpose is optional.

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
		Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html	
subjectAltName	No	A subfield as specified in section 7.1.4.1.	As stated in section 7.1.4.1.
authorityInformationAccess	No	The subfield AccessDescription contains either one or two paired subfields. Each pair contains an accessLocation and accessMethod. OIDs for indicating access methods are as defined in IETF RFC 5280. One accessLocation lists the URL of the Certificate issued to IdenTrust by the ECA Root CA and the method for accessing that URL: [1] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = ldap://ldap[eca].identrust.com/cn%3DIdenTrust%20ECA%20[X]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?cACertificate;binary} [2] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = http://apps.identrust.com/roots/identrusteca[X].cer} An additional accessLocation will be present if and when an OCSP Responder is available for the Certificate. The responder's URL appears with OCSP as the appropriate access method, as prescribed in [IETF RFC 2560]. accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation ::= { URL = http://eca.ocspts.identrust.com} for the 1,024 bit length subordinate CAs or accessLocation ::= { URL = http://eca.ocsp.identrust.com} for all subsequent subordinate CAs	Access Method 1.3.6.1.5.5.7.48.2 is caIssuers, which provides a pointer reference to the current Certificate issued to IdenTrust by the ECA Root CA. [X] = Iteration of IdenTrust ECA CA (e.g., ECA 1, ECA 2, etc.) Information related to ECA 1 will be published to and continue to be available at ldap.identrust.com until expiration of all Certificates issued by ECA 1. This information will also be published to ldapeca.identrust.com. Access Method 1.3.6.1.5.5.7.48.1 is OCSP, which provides a pointer to the OCSP Responder for the Certificate. The content and format of OCSP requests and responses is specified in sections 10.11 and 10.12.
CRLDistribution-Points	No	The subfield *DistributionPointName* contains LDAP and HTTP URLs pointing to the appropriate CRL. [1] URL = ldap://ldap[eca].identrust.com/cn%3DIdenTrust%20ECA%20[X]%2Cou%3DCertification%20Authorities%	Points to URLs where more information about the post-issuance validity or reliability of a Certificate may be available. [X] = Iteration of IdenTrust ECA CA (e.g., ECA 1, ECA 2, etc.)

Field Name	Critical?	Data Content Requirements	Significance
		2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?certificateRevocationList;binary [2] URL = http://crl.identrust.com/eca/identrusteca[X].crl	Information related to ECA 1 will be published to and continue to be available at ldap.identrust.com until expiration of all Certificates issued by ECA 1. This information will also be published to ldapeca.identrust.com.
SubjectDirectoryAttributes	No	This subfield CountryOfCitizenship contains a two-character PrintableString listing an ISO 3166 Country Code.	The citizenship of the Subscriber. Multiple citizenships may be asserted in multiple instances of the attribute.

Signing Certificate Profile for SHA-256 Implementation

The following fields are different for SHA-256 implementation.

Field Name	Critical?	Data Content Requirements	Significance
Issuer's Signature	n/a	The subfield *algorithmIdentifier: algorithm* must contain the object identifier (specified in ECA CP and [IETF RFC 5280]) for SHA-256 {1.2.840.113549.1.1.11}	Indicates the algorithm used by IdenTrust to sign the Certificate, which is SHA-256 with RSA Encryption
Issuer	n/a	cn=IdenTrust ECA S2[Y], ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US	Identifies the Certification Authority which signed this Certificate; see section 7.1.4.2 [Y] = Iteration of IdenTrust ECA CA S2, starting with zero (0) (e.g., ECA S20, ECA S21, etc.)
Extension	***Critical***	***Data Content Requirements***	***Significance***
certificatePolicies	No	*The PolicyInformation:policyIdentifier* subfield contains an OID specified below as appropriate for the type of Certificate. OIDs are: {2.16.840.1.101.3.2.1.12.4} for Medium Assurance SHA-256 Certificate Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html **or** {2.16.840.1.101.3.2.1.12.5} for Medium Token SHA-256 Assurance Certificate Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html	The ECA CP applies in relation to this Certificate, and that the Certificate is of the type indicated in section 1.2. See also section 1.4 on Certificate Usage.

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
authorityInforma-tionAccess	No	The subfield AccessDescription contains either one or two paired subfields. Each pair contains an accessLocation and accessMethod. OIDs for indicating access methods are as defined in IETF RFC 5280. One accessLocation lists the URI of the Certificate issued to IdenTrust by the ECA Root CA for SHA-256 and the method for accessing that URL: [1] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = ldap://ldapeca.identrust.com/cn%3DIdenTrust%20ECA%20S2[Y]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?cACertificate;binary} [2] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = http://apps.identrust.com/roots/identrustecas2[Y].cer} An additional accessLocation will be present if and when an OCSP Responder is available for the Certificate. The responder's URL appears with OCSP as the appropriate access method, as prescribed in [IETF RFC 2560]. accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation ::= { URL = http://eca2.ocsp.identrust.com} for all subsequent subordinate CAs	Access Method 1.3.6.1.5.5.7.48.2 is caIssuers, which provides a pointer reference to the current Certificate issued to IdenTrust by the ECA root for SHA-256 CA. [Y] = Iteration of IdenTrust ECA CA S2, starting with zero (0) (e.g., ECA S20, ECA S21, etc.) Access Method 1.3.6.1.5.5.7.48.1 is OCSP, which provides a pointer to the OCSP Responder for the Certificate. The content and format of OCSP requests and responses is specified in sections 10.11 and 10.12.
CRLDistribution-Points	No	The subfield *DistributionPointName* contains LDAP and HTTP URLs pointing to the appropriate CRL. [1] URL = ldap://ldapeca.identrust.com/cn%3DIdenTrust%20ECA%20S2[Y]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?certificateRevocationList;binary	Points to URLs where more information about the post-issuance validity or reliability of a Certificate may be available. [Y] = Iteration of IdenTrust ECA CA S2, starting with zero (0) (e.g., ECA S21, ECA S22, etc.)

Field Name	Critical?	Data Content Requirements	Significance
		[2] URL = http://crl.identrust.com/eca/identrustecas2[Y].crl	

10.5 Component Certificate

Component Certificates have similar content as specified in section 10.3, except for the SubjectDistinguishedName, keyUsage and SubjectDirectoryAttributes fields. For the SubjectDistinguishedName the Common Name may indicate different name for a CA dedicated to the issuance of component certificates. For the KeyUsage field, the first and third bits of that field, numbered 0 and 2 and indicating digital signature and key encipherment, respectively, are set to true. All other bits of that field are set to false. Also, in accordance with section 7.1.4.1, the subjectAltName may contain the URL, IP Address, e-mail address, or fully qualified domain name of the Component. The SubjectDirectoryAttributes is omitted.

10.5.1 SSL Certificate

SSL Certificate Profile for SHA-1 Implementation

Field Name	Critical?	Data Content Requirements	Significance
Version	n/a	v3 only (indicated by the integer "2")	Indicates the version of [ITU-T X.509] to which the Certificate conforms.
serialNumber	n/a	An integer unique to the Certificate among the range of all serial numbers in ECA Certificates issued by the IdenTrust ECA.	The serial number of the Certificate in question.
Issuer's Signature	n/a	The subfield *algorithmIdentifier: algorithm* must contain the object identifier (specified in ECA CP and [IETF RFC 5280]) for SHA-1 {1.2.840.113549.1.1.5}	Indicates the algorithm used by IdenTrust to sign the Certificate, which is SHA-1 with RSA Encryption.
Issuer	n/a	cn=IdenTrust ECA[X], ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US or cn=IdenTrust ECA Component [X], ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US	Identifies the Certification Authority which signed this Certificate; see section 7.1.4.2 [X] = Iteration of IdenTrust ECA CA (e.g., ECA 1, ECA 2, etc. Or for a dedicated subordinate CA, ECA Component 1, ECA Component 2, etc
Validity	n/a	The subfields notBefore and notAfter contain dates in the form specified for UTC Time in [IETF RFC 5280].	NotBefore indicates the date on which the Certificate begins to be valid and notAfter indicates when it ceases to be valid. Years are listed as specified in [IETF RFC 5280]. The time interval listed may be 1, 2, 3 years, or less, but shall not exceed 3 years.

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
Subject	n/a	cn=[Fully Qualified Domain Name] ou=[OrganizationUnitName], ou=IdenTrust, ou=ECA, o=U.S. Government, c=US	As specified in section 3.1.5, in the case of a Component Certificate, the CommonName is the fully qualified domain name of the component or device being certified. If the component is a web server, the FQDN is always listed in subjectAltName. The OrganizationUnitName is the name of the Subscribing Organization.
subjectPublicKey-Info	n/a	The subfield *algorithmIdentifier: algorithm* contains the object identifier for RSA Encryption. The length of the public key in *subjectPublicKey* is 2048 bits for all Certificates issued off subordinate CAs.	*SubjectPublicKey* is the Subscriber's public key, and *algorithmIdentifier* indicates the algorithm to use with it.
Extension	***Critical***	***Data Content Requirements***	***Significance***
authorityKeyIdenti-fier	No	The subfield *keyIdentifier* contains the 20-byte SHA-1 hash of the DER-encoded public key by which the issuer's signature on the Certificate can be verified. The other subfields of *authorityKeyIdentifier* are not used.	Indicates which public key to use in verifying the authenticity of the Certificate.
subjectKeyIdenti-fier	No	The subfield *keyIdentifier* contains the 20-byte SHA-1 hash of the DER-encoded public key listed in *subjectPublic-KeyInfo:subjectPublicKey*.	The subfield *keyIdentifier* labels the public key of this Certificate for convenient reference and to help prevent confusion with other key pairs that the same Subscriber may have.
keyUsage	Yes	Bit 0 and bit 2 of the bitstring are set to true; all others are set to false. digitalSignature, keyEncipherment.	Indicates to software applications using the key what the key is to be used for (see [ITU X.509] and [IETF 3280]). This field is to signal to applications how to use the Certificate and the corresponding private key.
ExtendedkeyUsag e	No	id-kp-serverAuth {1 3 6 1 5 5 7 3 1}; id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	Indicates to software applications using the key what the key can be used for. This field is to signal to specific applications how to use the Certificate and the corresponding private key.
certificatePolicies	No	*The PolicyInformation:policyIdentifier* subfield contains an OID specified below as appropriate for the type of Certificate. OIDs are: {2.16.840.1.101.3.2.1.12.1} for Medium Assurance Certificate Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html	The ECA CP applies in relation to this Certificate, and that the Certificate is of the type indicated in section 1.2. See also section 1.4 on Certificate Usage.

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
subjectAltName	No	A Fully Qualified Domain in the dNSName name form in accordance with Section 7.4.1	FQDN Identified in the Certificate
authorityInforma-tionAccess	No	The subfield AccessDescription contains either one or two paired subfields. Each pair contains an accessLocation and accessMethod. OIDs for indicating access methods are as defined in IETF RFC 3280.	
		One accessLocation lists the URI of the Certificate issued to IdenTrust by the ECA Root CA and the method for accessing that URI: [1] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URI = ldap://ldap[eca].identrust.com/ cn%3DIdenTrust%20ECA%20[X]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3CUS?cACertificate;binary} [2] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = http://apps.identrust.com/roots/identrusteca[X].cer}	Access Method 1.3.6.1.5.5.7.48.2 is caIssuers, which provides a pointer reference to the current Certificate issued to IdenTrust by the ECA Root CA. [X] = Iteration of IdenTrust ECA CA (e.g., ECA1, ECA2, etc.) Information related to ECA 1 will be published to and continue to be available at ldap.identrust.com until expiration of all Certificates issued by ECA 1. This information will also be published to ldapeca.identrust.com.
		An additional accessLocation will be present if and when an OCSP Responder is available for the Certificate. The responder's URI appears with OCSP as the appropriate access method, as prescribed in [IETF RFC 2560]. accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation ::= { URL = http://eca.ocspts.identrust.com} for the 1,024 bit length subordinate CAs or accessLocation ::= { URL = http://eca.ocsp.identrust.com} for all subsequent subordinate CAs	Access Method 1.3.6.1.5.5.7.48.1 is OCSP, which provides a pointer to the OCSP Responder for the Certificate. The content and format of OCSP requests and responses is specified in sections 10.11 and 10.12.

Field Name	Critical?	Data Content Requirements	Significance
CRLDistribution-Points	No	The subfield *DistributionPointName* contains LDAP and HTTP URLs pointing to the appropriate CRL. [1] URL = ldap://ldap[eca].identrust.com/cn%3DIdenTrust%20ECA%20[X]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?certificateRevocationList;binary [2] URL = http://crl.identrust.com/eca/identrusteca[X].crl	Points to URLs where more information about the post-issuance validity or reliability of a Certificate may be available. [X] = Iteration of IdenTrust ECA CA (e.g., ECA 1, ECA 2, etc.) Information related to ECA 1 will be published to and continue to be available at ldap.identrust.com until expiration of all Certificates issued by ECA 1. This information will also be published to ldapeca.identrust.com.

SSL Certificate Profile for SHA-256 Implementation

The following fields are different for SHA-256 implementation.

Field Name	Critical?	Data Content Requirements	Significance
Issuer's Signature	n/a	The subfield *algorithmIdentifier: algorithm* must contain the object identifier (specified in ECA CP and [IETF RFC 5280]) for SHA-256 {1.2.840.113549.1.1.11}	Indicates the algorithm used by IdenTrust to sign the Certificate, which is SHA-256 with RSA Encryption
Issuer	n/a	cn=IdenTrust ECA Component S2[Y], ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US	Identifies the Certification Authority which signed this Certificate; see section 7.1.4.2 [Y] = Iteration of IdenTrust ECA Component CA S2, starting with zero (0) (e.g., ECA Component S20, ECA Component S21, etc.)
Extension	***Critical***	***Data Content Requirements***	***Significance***
certificatePolicies	No	*The PolicyInformation:policyIdentifier* subfield contains an OID specified below as appropriate for the type of Certificate. OIDs are: {2.16.840.1.101.3.2.1.12.9} for Medium Assurance Device SHA-256 Certificate Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html	The ECA CP applies in relation to this Certificate, and that the Certificate is of the type indicated in section 1.2. See also section 1.4 on Certificate Usage.
authorityInforma-tionAccess	No	The subfield AccessDescription contains either one or two paired subfields. Each pair contains an accessLocation and	

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
		accessMethod. OIDs for indicating access methods are as defined in IETF RFC 5280. One accessLocation lists the URI of the Certificate issued to IdenTrust by the ECA Root CA for SHA-256 and the method for accessing that URL: [1] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = ldap://ldapeca.identrust.com/cn%3DIdenTrust%20ECA%20S2[Y]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?cACertificate;binary} [2] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = http://apps.identrust.com/roots/identrustecas2[Y].cer} An additional accessLocation will be present if and when an OCSP Responder is available for the Certificate. The responder's URL appears with OCSP as the appropriate access method, as prescribed in [IETF RFC 2560]. accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation ::= { URL = http://eca2.ocsp.identrust.com} for all subsequent subordinate CAs	Access Method 1.3.6.1.5.5.7.48.2 is caIssuers, which provides a pointer reference to the current Certificate issued to IdenTrust by the ECA root for SHA-256 CA. [Y] = Iteration of IdenTrust ECA CA S2, starting with zero (0) (e.g., ECA S20, ECA S21, etc.) Access Method 1.3.6.1.5.5.7.48.1 is OCSP, which provides a pointer to the OCSP Responder for the Certificate. The content and format of OCSP requests and responses is specified in sections 10.11 and 10.12.
CRLDistribution-Points	No	The subfield *DistributionPointName* contains LDAP and HTTP URLs pointing to the appropriate CRL. [1] URL = ldap://ldapeca.identrust.com/cn%3DIdenTrust%20ECA%20S2[Y]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?certificateRevocationList;binary [2] URL = http://crl.identrust.com/eca/identrustecas2[Y].crl	Points to URLs where more information about the post-issuance validity or reliability of a Certificate may be available. [Y] = Iteration of IdenTrust ECA CA S2, starting with zero (0) (e.g., ECA S21, ECA S22, etc.)

10.6 Code Signing Certificate

Not applicable as IdenTrust does not issue ECA Certificates for purposes of code signing, i.e. with an extendedKeyUsage field having a value "codeSigning" as specified in [IETF RFC 5280].

10.7 OCSP Responder Self-Signed Certificate

As specified in Section 10.8 of the ECA CP.

10.8 ECA Root CA CRL

As specified in Section 10.9 of the ECA CP.

10.9 OCSP Responder Certificate

An OCSP Responder Certificate that is not self-signed has the same content as specified in section 7.1.4.2, except as otherwise indicated below.

Two profile tables are provided for an OCSP Responder Certificate. The first profile table supports an implementation using SHA-1 as the signing algorithm. The second profile table supports SHA-256 as the signing algorithm. The second table is not comprehensive; instead it shows the fields and extensions that should be modified in the first table.

OCSP Responder Certificate Profile for SHA-1 Implementation

Field Name	***Critical?*** [29]	***Data Content Requirements***	***Significance***
Version	n/a	v3 only (indicated by the integer "2")	Indicates the version of [ITU-T X.509] to which the Certificate conforms.
SerialNumber	n/a	An integer unique to the Certificate among the range of all serial numbers in ECA Certificates issued by IdenTrust.	The serial number of the Certificate in question.
Issuer's Signature	n/a	The subfield *algorithmIdentifier: algorithm* must contain the object identifier (specified in ECA CP and [IETF RFC 5280]) for SHA-1 or SHA-256 with RSA encryption. {1.2.840.113549.1.1.5}	Indicates the algorithm used by IdenTrust to sign the Certificate, which is SHA-1 with RSA Encryption.
Issuer	n/a	cn=IdenTrust ECA[X], ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US	Identifies the Certification Authority which signed this Certificate; see section 7.1.4.2.

[29] "Critical" indicates for an extension whether an application is required to be able to process the content of the field. It is not applicable ("n/a") for fields that are not extensions.

			[X] = Iteration of IdenTrust ECA CA (e.g., ECA1, ECA 2, etc.)
Validity	n/a	The subfields notBefore and notAfter contain dates in the form specified for UTC Time in [IETF RFC 5280].	NotBefore indicates the date on which the Certificate begins to be valid and notAfter indicates when it ceases to be valid. Years are listed as specified in [IETF RFC 5280]. The Certificate validity time interval may be up to, but not greater than, one month.
Subject	n/a	cn=IdenTrust OCSP Responder ou=IdenTrust ou=IdenTrust[30] ou= ECA o=U.S. Government c=US	As specified in section 7.1.4.1.
subjectPublicKey-Info	n/a	The subfield *algorithmIdentifier: algorithm* contains the object identifier for RSA Encryption. The length of the public key in *subjectPublicKey* is 2048 bits for all Certificates issued off subordinate CAs.	*SubjectPublicKey* is the Subscriber's public key, and *algorithmIdentifier* indicates the algorithm to use with it.
Extension	***Critical***	***Data Content Requirements***	***Significance***
authorityKeyIdenti-fier	No	The subfield *keyIdentifier* contains the 20-byte SHA-1 hash of the DER-encoded public key by which the issuer's signature on the Certificate can be verified. The other subfields of *authorityKeyIdentifier* are not used.	Indicates which public key to use in verifying the authenticity of the Certificate.
subjectKeyIdenti-fier	No	The subfield *keyIdentifier* contains the 20-byte SHA-1 hash of the DER-encoded public key listed in *subjectPublic-KeyInfo:subjectPublicKey*.	The subfield *keyIdentifier* labels the public key of this Certificate for convenient reference and to help prevent confusion with other key pairs that the same Subscriber may have.
KeyUsage	Yes	Bits 0 and 1 of the bitstring are set to true; all others are set to false. digitalSignature, nonRepudation.	Indicates to software applications using the key what the key is to be used for (see [ITU X.509] and [IETF 5280]). This field is to signal to applications how to use the Certificate and the corresponding private key.
extendedKeyUsag e	Yes	It indicates OCSPSigning as specified in the ECA CP section10.8 id-kp-OCSPSigning {1.3.6.1.5.5.7.3.9}	The Issuer CA designates authority to sign responses to this Certificate.

[30] Two separate OrganizationalUnitName subfields each contain "IdenTrust". The duplicate fields are because one "ou" represents IdenTrust as the ECA in the directory tree and the other "ou" is for IdenTrust as the organizational unit operating the OCSP Responder.

certificatePolicies	No	*The PolicyInformation:policyIdentifier* subfield contains the following OIDs: {2.16.840.1.101.3.2.1.12.1} for Medium Assurance Certificate {2.16.840.1.101.3.2.1.12.2} for Medium Hardware Assurance Certificate {2.16.840.1.101.3.2.1.12.3} for Medium Token Assurance Certificate (All OIDs are asserted.) [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html	The ECA CP applies in relation to this Certificate, and that the Certificate is of the type indicated in section 1.2. See also section 1.4 on Certificate Usage.
SubjectAltName	No	A subfield as specified in section 7.1.4.1. e.g. http://eca.ocspts.identrust.com for the 1,024 bit length subordinate CAs or http://eca.ocsp.identrust.com for all subsequent subordinate CAs	As stated in section 7.1.4.1.
NoCheck Id-pkix-ocsp-nocheck {1.3.6.1.5.5.7.48.1.5}	No	It indicates no check as specified in the ECA CP section10.8 NULL	The CA specifies that an OCSP client can trust this responder for the lifetime of the responder's Certificate.
AuthorityInformationAccess	No	The subfield AccessDescription contains either one or two paired subfields. Each pair contains an accessLocation and accessMethod. OIDs for indicating access methods are as defined in IETF RFC 3280. One accessLocation lists the URL of the Certificate issued to IdenTrust by the ECA Root CA. [1] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= { URL = ldap://ldap.identrust.com/cn%3DIdenTrust%20ECA%20[X]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?cACertificate;binary}	A pointer reference to the current Certificate issued to IdenTrust by the ECA Root CA. [X] = Iteration of IdenTrust ECA CA (e.g., ECA 1, ECA 2, etc.) Information related to ECA 1 will be published to and continue to be available at ldap.identrust.com until expiration of all Certificates issued by ECA 1. This information will also be published to ldapeca.identrust.com

		[2] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= { URL = http://apps.identrust.com/roots/identrusteca[X].cer}	

OCSP Responder Certificate Profile for SHA-256 Implementation

The following fields are different for SHA-256 implementation.

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
Issuer's Signature	n/a	The subfield *algorithmIdentifier: algorithm* must contain the object identifier (specified in ECA CP and [IETF RFC 5280]) for SHA-256 {1.2.840.113549.1.1.11}	Indicates the algorithm used by IdenTrust to sign the Certificate, which is SHA-256 with RSA Encryption
Issuer	n/a	cn=IdenTrust ECA S2[Y], ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US	Identifies the Certification Authority which signed this Certificate; see section 7.1.4.2 [Y] = Iteration of IdenTrust ECA CA S2, starting with zero (0) (e.g., ECA S20, ECA S21, etc.)
Subject	n/a	cn=IdenTrust S2 OCSP Responder ou=IdenTrust ou=IdenTrust[31] ou= ECA o=U.S. Government c=US	As specified in section 7.1.4.1.
Extension	***Critical***	***Data Content Requirements***	***Significance***
certificatePolicies	No	*The PolicyInformation:policyIdentifier* subfield contains an OID specified below as appropriate for the type of Certificate. OIDs are: {2.16.840.1.101.3.2.1.12.4} for Medium Assurance SHA-256 Certificate {2.16.840.1.101.3.2.1.12.5} for Medium Token SHA-256 Assurance Certificate {2.16.840.1.101.3.2.1.12.9} for Medium Assurance Device SHA-256 Assurance Certificate Policy Qualifier Id=CPS	The ECA CP applies in relation to this Certificate, and that the Certificate is of the type indicated in section 1.2. See also section 1.4 on Certificate Usage.

[31] Two separate OrganizationalUnitName subfields each contain "IdenTrust". The duplicate fields are because one "ou" represents IdenTrust as the ECA in the directory tree and the other "ou" is for IdenTrust as the organizational unit operating the OCSP Responder.

Field Name	Critical?	Data Content Requirements	Significance
		Qualifier: https://secure.identrust.com/certificates/policy/eca/index.html	
authorityInformationAccess	No	The subfield AccessDescription contains either one or two paired subfields. Each pair contains an accessLocation and accessMethod. OIDs for indicating access methods are as defined in IETF RFC 5280. One accessLocation lists the URI of the Certificate issued to IdenTrust by the ECA Root CA for SHA-256 and the method for accessing that URL: [1] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = ldap://ldapeca.identrust.com/cn%3DIdenTrust%20ECA%20S2[Y]%2Cou%3DCertification%20Authorities%2Cou%3DECA%2Co%3DU.S.%20Government%2Cc%3DUS?cACertificate;binary} [2] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = http://apps.identrust.com/roots/identrustecas2[Y].cer} An additional accessLocation will be present if and when an OCSP Responder is available for the Certificate. The responder's URL appears with OCSP as the appropriate access method, as prescribed in [IETF RFC 2560]. accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation ::= { URL = http://eca2.ocsp.identrust.com} for all subsequent subordinate CAs	Access Method 1.3.6.1.5.5.7.48.2 is caIssuers, which provides a pointer reference to the current Certificate issued to IdenTrust by the ECA root for SHA-256 CA. [Y] = Iteration of IdenTrust ECA CA S2, starting with zero (0) (e.g., ECA S20, ECA S21, etc.) Access Method 1.3.6.1.5.5.7.48.1 is OCSP, which provides a pointer to the OCSP Responder for the Certificate. The content and format of OCSP requests and responses is specified in sections 10.11 and 10.12.

10.10 Subordinate CA CRL

CRLs have the content specified in the ECA CP. This section clarifies how IdenTrust implements those specifications and how they are to be understood by Relying Parties and others.

Field Name	*Critical?*	*Data Content Requirements*	*Significance*
Version	n/a	V2 only (indicated by the integer "1")	Indicates the version of [ITU-T X.509] to which the Certificate revocation list (CRL) conforms.
Signature	n/a	Same as specified for Certificates (i.e. the IdenTrust ECA's signature algorithm for SHA-1 or SHA-256 with RSA Encryption. {1.2.840.113549.1.1.5} for SHA-1 {2.16.840.1.101.3.4.2.1} for SHA-256	
Issuer	n/a	The distinguished name of the issuer of the revoked Certificate specified according to section 7.1.4.2.	Identifies IdenTrust as issuer of the CRL; see section 7.1.4.2.
ThisUpdate	n/a	A date and time specified according to section 5.1.2.4 of [IETF RFC 5280] (*i.e.* in UTCtime).	The date and time when the Certificate revocation list was issued.
NextUpdate	n/a	A date and time specified according to section 5.1.2.5 of [IETF RFC 5280] (*i.e.* in UTCtime). The time indicated is 24 hours from the time listed in ThisUpdate.	The date and time when IdenTrust anticipates issuing an update to the CRL.
RevokedCertifi-cates	n/a	If present, this field contains the following subfields: userCertificate contains a subfield containing an integer revocationDate contains a date and time specified as UTCtime Reason Code is an enumerated integer between zero and five. The invalidityDate extension is not used.	If this field is present: userCertificate indicates the serial number of the revoked Certificate. Indicates the date and time when IdenTrust revoked the Certificate. The reason provided by the Subscriber for revocation of the Certificate.
CRL Extension	***Critical***	***Data Content Requirements***	***Significance***
authorityKeyIdenti-fier	No	The subfield keyIdentifier contains the SHA-1 hash of the public key by which the issuer's signature on the Certificate revocation list can be verified.	Indicates which public key to use in verifying the authenticity of the CRL.
CRLnumber	No	An integer.	The serial number of this CRL in an incrementally increasing sequence of CRLs.

10.11 OCSP Request Format

Field Name	*Data Content Requirements*	*Significance*
Version	An integer with the value of 0.	Indicates version 1 of OCSP, *i.e.* the version specified in [IETF RFC 2560].
requestorName (omissible)	A GeneralName	IdenTrust ignores this field *i.e*. treats it as insignificant.
requestList	One or more request subfields, each identifying a Certificate by its CertID as defined in [IETF RFC 2560].	Indicates the Certificate(s) for which notification of validity is requested.
optionalSignature (omissible)	A digital signature in the form prescribed by [IETF RFC 2560].	IdenTrust ignores this field and does not verify the signature if any is present.
requestExtensions (omissible)	May be empty, if present at all. If populated, content must be as prescribed in [IETF RFC 2560] and [IETF RFC 5280].	IdenTrust will process a nonce when provided in the request.

10.12 OCSP Response Format

IdenTrust supports only the responseType specified as BasicOCSPResponse in [IETF RFC 2560]. To be succinct, some ASN.1 layers present in the response and required by [IETF RFC 2560] do not appear in the table below.

Field Name	*Data Content Requirements*	*Significance*
responseStatus	One of the following values: successful, malformedRequest, internalError, or tryLater. The standardized values sigRequired and unauthorized are not supported for OCSP responses in relation to ECA Certificates.	Successful: The OCSP request has been fulfilled.[32] If the responseStatus is other than successful, the response contains no reliable information about the Certificate's validity. malformedRequest: The form or content of the OCSP request was erroneous as received by the OCSP Responder. internalError: The OCSP Responder appears to have erred in processing the OCSP request. tryLater: The OCSP Responder cannot respond at this time.
Response Type	Id-pkix-ocsp-basic{1.3.6.1.55.7.48.1.1}	BasicOCSPResponse as defined in IETF RFC 2560
Version	An integer with a value of 0.	Indicates version 1 of OCSP, *i.e.* the version specified in [IETF RFC 2560].

[32] A value of "successful" does not indicate that the Certificate in question is valid but rather indicates that the OCSP request has been successful. Whether the Certificate is valid is indicated in the responseBytes:response field.

Field Name	*Data Content Requirements*	*Significance*
ResponderID	The subfield byKey, which contains a hash value.	The hash value of the OCSP Responder's public key as listed in the current Certificate for the OCSP Responder.
ProducedAt	A GeneralizedTime value specified as Greenwich Mean Time and otherwise as required in RFC 5280.	The date and time when IdenTrust issued the OCSP response. Validity information in the response is **not**, however, current as of this time but rather as of the time listed in thisUpdate.
Extensions	Blank or unused (no value specified)	IdenTrust does not support extensions in OCSP responses.[33]
Signature	Subfields containing a digital signature, the algorithm to be used in verifying it, and Certificates necessary for its verification.	IdenTrust's digital signature verifiable by a Certificate in the form prescribed for an OCSP Responder. Signature algorithm is consistent with guidance in Section 6.1.5.
List of Responses		
certID	A sequence of subfields as specified in RFC 2560.	Indicates the Certificate to which the related[34] certStatus pertains.
certStatus	One of the following values: good, revoked, or unknown.	Good indicates that the Certificate indicated by the related certStatus is not revoked as of the time listed in thisUpdate. Revoked indicates that the Certificate is revoked as of the time listed in thisUpdate. Unknown indicates that the OCSP has no information available for the Certificate as of the time listed in thisUpdate, perhaps because it was not issued by IdenTrust or because the OCSP Responder has not yet been updated, or for some other reason.
thisUpdate	A GeneralizedTime value specified as Greenwich Mean Time and otherwise as required in RFC 5280.	The date and time when the OCSP database used in generating responses was last updated.
nextUpdate	A GeneralizedTime value specified as Greenwich Mean Time and otherwise as required in RFC 5280.	The date and time when IdenTrust next expects to update the OCSP database used in generating responses.

[33] With the exception of a request containing a nonce request. Value in nonce field of request will be returned if specified in the original request and omitted if not included in request.

[34] Instances of the certID, certStatus, thisUpdate, and nextUpdate are grouped together within a SingleResponse field for each Certificate to which the response pertains.

11. Identity Proofing Outside of the U.S.

This Section addresses identity proofing for U.S. citizens and non-U.S. citizens located outside the U.S. All other identity proofing performed by IdenTrust is performed in accordance with section 3.2.3.

11.1 Identity Proofing by U.S. Consular Officers and Judge Advocate General (JAG) Officers

For the issuance of Medium Assurance Certificates and Medium Token Assurance Certificates, IdenTrust will make use of notarial services provided by U.S. consular offices and embassies and Judge Advocate General (JAG) Officers for identity proofing for U.S. citizens located outside the U.S.

Citizens of:

- Australia,
- Canada,
- New Zealand,
- or the United Kingdom (U.K.)

located in:

- Australia,
- Canada,
- New Zealand, or
- the U.K.

may use the notarial services provided by U.S. consular offices and embassies and JAG officers in those countries. (For example, a citizen of Australia may have in-person identity proofing performed at a U.S. consulate in Canada and vice versa.) All other non-U.S. citizens located outside the U.S. (including citizens of Australia, Canada, New Zealand, or the U.K. not located in Australia, Canada, New Zealand, the U.K. or the U.S.) must be enrolled by Authorized DOD Employees in accordance with section 11.2 below.

11.1.1 Procedures for Identity Proofing for U.S and non-U.S. citizens in Participant Countries

IdenTrust uses the steps outlined in section 4.1.2 of this CPS to process applications of U.S. citizens abroad and non-U.S. citizens residing in Participant countries. Applicants are informed that consular and JAG officers can perform the function of a notary public if not applying within the U.S. This notification occurs both during the online registration process as well as in the In-Person Identification Form (section 15.5) downloaded during the process.

The In-Person Identification Form contains instructions to consular and JAG officers regarding the steps and forms of ID that are valid for identity proofing including the mandatory use of a valid passport from each country that the applicant is asserting citizenship.

The step outlined in section 4.1.2.5 (iv) is augmented by having IdenTrust RA Operators verify that the documentation submitted by the applicant is stamped with a seal from a U.S. consular or a JAG officer located in one of the Participant Countries listed in 11.1.

11.2 Identity Proofing by Authorized DoD Employees

All applicants, other than U.S. Citizens, residing outside of the United States may use the in-person identity verification services provided by Authorized DOD Employees. IdenTrust provides processes to support the DOD efforts to issue Certificates to individuals who do not reside in or who are not citizens of the Participant Countries identified in section 11.1.3 of the ECA CP. The following sections outline the processes between IdenTrust and the DoD PKI ECA Liaison Officer and between IdenTrust and authorized DoD employees.

11.2.1 Process for Authorizing Issuance of ECA Certificates When Identity Proofing Is Performed by Authorized DoD Employees Outside the U.S.

DoD components that participate in this process should follow the procedure outlined in section 11.2 of the ECA CP. IdenTrust complements that procedure with the processes explained in the following sections.

11.2.1.1 Maintenance of Contact Information

IdenTrust will use the following procedures to accept information from: (1) the DoD PKI ECA Liaison Officer, and (2) authorized DOD employees.

DOD PKI ECA Liaison Officer

The initial DoD PKI ECA Liaison Officer will be provided to IdenTrust in a secure communication. DoD will also provide the name, title, phone number and e-mail address of the Liaison Officer's supervisor.

The Liaison Officer can be replaced only by the then-current Liaison Officer or by the Liaison Officer's supervisor. Any change will be communicated to the IdenTrust Registration Desk using an email signed using the valid CAC of the Liaison Officer or the supervisor previously identified.

Authorized DoD Employees

Whenever necessary, based on changes or updates to the current list of authorized DoD employees for each DoD Component, the Liaison Officer may submit an updated list of Authorized DoD Employees to the IdenTrust Registration Desk via digitally signed e-mail, along with the Certificate information and mailing address of each Authorized DoD Employee. The new list will supersede any prior list once IdenTrust has validated the signature on the email as coming from the current Liaison Officer.

11.2.2 Identity Proofing Procedures to Be Used by Authorized DoD Employees for ECA Certificates

Authorized DoD employees will follow the procedure in the ECA CP section 11.2.2 to proof identities. This process is a step in the larger process explained in the following section.

11.2.3 IdenTrust's Process for DoD Approved Certificates

This section outlines steps that will be taken when issuing Certificates based on identity proofing performed by Authorized DOD Employees which steps are in addition to those otherwise required to meet other relevant requirements of the CP and are explained in the main body of the CPS. If there are any inconsistencies between these steps and those stated above in the main body of the CPS, the steps specified in this section shall apply.

The applicant will provide registration information on a Server-authenticated SSL/TLS secured web site hosted by IdenTrust. The applicant must provide the following information:

- applicant Name,
- applicant Address (if necessary for sending Cryptographic Module to applicant or billing purposes)
- applicant's Email Address,
- applicant's Citizenship(s),
- applicant's Organization Name,
- An account password and password hint, and
- A payment form (e.g, Voucher, order number[35] or credit card)

During this session, the applicant will be provided with an Account Number/Application ID that is at least 8 characters long and a link to the Subscriber Agreement and Subscribing Organization Authorization Agreement ("Subscriber Agreements"). The applicant is instructed to: (a) make a record of the Account Number/Application ID, (b) print out the Subscriber Agreements, (c) take the Account Number/Application ID and Subscriber Agreement with them to the identity proofing session with the authorized

[35] When the payment mechanism is a voucher or an order number, arrangements to provide this information to the applicant must occur prior to initial enrollment.

DoD employee, accompanied by the applicant's country representative, to continue the identity proofing process.

When the applicant, the country representative, and the authorized DOD employee meet, the authorized DOD employee will follow the process outlined in the ECA CP section 11.2.2 to perform identity proofing. As part of completing the steps in section 11.2.2, the applicant will provide physical proof (to include passport) supporting the identifying information provided during the online registration (except the account password and hint, which are to be kept secure by the applicant).

After successful identity proofing, the authorized DoD employee must send an email to the IdenTrust's Registration Desk (to an e-mail address provided out-of-band by IdenTrust to the Liaison Officer for that purpose) that is digitally signed with the authorized DOD employee's CAC signature Certificate, containing:

- The applicant's name, address (if necessary for sending Cryptographic Module to applicant), email, organization's name, Account Number/Application ID, identification types, serial numbers and expiration dates, and the citizenship(s) verified by the authorized DOD employee during the identity proofing process,
- And, a statement that the authorized DoD employee has performed identity proofing for this applicant in accordance with the ECA CP,

An IdenTrust RA Operator from the Registration Desk, will:

- Verify the signature on the email to Confirm it matches the name of the sender in the full Certificate path validation,
- Confirm that the signer is listed among those authorized DoD employees described above in 11.2.1,
- Use the Account Number/Application ID to find the applicant record and compare all the information,
- Verify that the Subscriber is a qualified national of a country other than those restricted in accordance to the practices defined in Section 11.2.4, and
- If no discrepancy is found, approve the account, generate the Activation Code and send it either (1) via digitally signed e-mail to the applicant's e-mail address or (2) in a retrieval kit with a Cryptographic Module as described in sections 4.1.2.6, 6.1.2, and 6.2.6 along with directions on retrieving the Certificate(s) at a specified, secure URL (Server-authenticated SSL/TLS session).

The applicant will use the Activation Code and account password to authenticate and provide the public key for the signature Certificate request, receive the encryption key, and to retrieve the encryption key and Certificate(s) from the retrieval URL, as further described in Section 4.3.1 of this CPS.

11.2.4 Participating Countries

IdenTrust may issue Certificates to all qualified local nationals except for nationals of countries proscribed by law and regulation at the time of approval of the Certificate application as defined in Section 11.2.3.

IdenTrust maintains and reviews monthly a list of proscribed countries used to verify applications. The list is amended according to any changes occurred in the prior month. The list is generated based on the applicable regulations defined in the ECA CP Section 11.2.4 including:

- Department of Commerce Export Administration Regulations (EAR), 15 C.F.R. Section 730 et seq., including specifically, but not limited to, Parts 736, 738, 740, 744 Spir, and 746. See http://www.access.gpo.gov/bis/ear/ear_data.html
- Department of the Treasury regulations issued pursuant to the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. Ch.35, Sec. 1701 et seq. or other laws identifying prohibited countries or people or entities, including the Office of Foreign Assets Control ("OFAC") Listing of Specially Designated Nationals and Blocked Persons (SDN List) and OFAC Country Sanctions Programs. For more information, see specifically:

  http://www.treas.gov/offices/enforcement/ofac/index.shtml and
  http://www.treas.gov/offices/enforcement/lists/

11.2.3.1 Export License Practices

In order to meet the requirements of the Department of Commerce Bureau of Industry and Security export license, IdenTrust will:

- Retain copies of all records pertaining to each ECA Certificate exported to an individual under Export License D528777. For every Certificate, a record is created in the tools provided by the Department of Commerce. At the time of writing this document, the tool available is the Automated Export System ("AES"). In case of absence of any tool, IdenTrust will use its own customer database.
  IdenTrust records: i) export commodity control number, and ii) validated license number.
- Provide the records upon written request within the timeframe specified in the requesting document, to DISA, DoD and/or to the Department of Commerce's Bureau of Industry and Security. A list will be generated upon request using the information available in the tool provided by the Department of Commerce. In case that the records are unavailable through the a Department of Commerce tool (e.g., AES), IdenTrust may generate the list of exported commodity types (i.e., ECA Certificate, ECA Certificate on Smart Card, or ECA Certificate on USB Tokens) including: the Subscriber's name, email, country of citizenship, and, commodity type.

11.3 IDENTITY PROOFING BY TRUSTED CORRESPONDENTS

IdenTrust uses Trusted Correspondents who follow the steps outlined in sections 4.1.2 or 4.1.3 of this CPS to perform in-person identification of: (a) U.S. citizens located outside the U.S.; and (b) citizens of Participant Countries who are located in one of the

Participant Countries. All CP requirements applicable to Trusted Correspondents shall apply to these Trusted Correspondents. Additionally, the Trusted Correspondent must be a U.S. citizen unless the identity proofing is carried out in one of the Participant Countries, in which case, the Trusted Correspondent must either be a U.S. citizen or a citizen of the country where the identity proofing is performed.

The Trusted Correspondent performs the steps specified in Section 3.2.3.1.2 of this CPS for in-person authentication of Subscribers. Applicants must present, and Trusted Correspondents verify, the Applicant's current valid passport for proof of citizenship and as one of the documents proving identity. Upon issuance of the Certificate, IdenTrust includes the country of citizenship in the SubjectDirectoryAttributes extension of the Certificate.

12. References

[AICPA Code of Professional Conduct]: American Institute of Certified Public Accountants, *Code of Professional Conduct*. Available online.

[AICPA CA WebTrust Criteria]: American Institute of Certified Public Accountants, *WebTrust Principles and Criteria for Certification Authorities* version 2 (2011). Available online.

[ANSI X9.79]: American National Standards Institute, PKI Practices and Policy Framework, revision 1 (2001).

[ECA CP]: United States Department of Defense External Certification Authority, X.509 Certificate Policy, Version 4.4 (dated 10/1/2015).

[IETF RFC 1630]: T. Berners-Lee, *Universal Resource Identifiers in WWW: A Unifying Syntax for the Expression of Names and Addresses of Objects on the Network as used in the World-Wide Web* (1994).

[IETF RFC 2253]: M. Wahl et al., *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names* (1997). Available online.

[IETF RFC 2560]: M. Myers, et al., *X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP* (1999). Available online.

[IETF RFC 2822]: P. Rosnick, ed., *Internet Message Format* (2001). Available online.

[IETF RFC 2616]: R. Fielding, et al., *Hypertext Transfer Protocol -- HTTP/1.1* (1999). Available online.

[IETF RFC 3647]: S. Chokhani, et al., Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework (2003). Available online.

[IETF RFC 5280]: D. Cooper, et al., Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile (2008). Available online.

[ISO/IEC 27001:2013]: International Standards Organization, Information technology—Security Techniques—Information security management systems—Requirements.

[ITU-T X.500]: International Telecommunication Union, *Recommendation X.500: The Directory* version 02/01 (2001). Available online.

[ITU-T X.509]: International Telecommunication Union, *The Directory: Authentication Framework* version 03/00. Also published by ISO as [ISO 9594-8]. Available online.

[NIST FIPS 140-2]: National Institute of Standards and Technology, *Security Requirements For Cryptographic Modules* (2001)

[RSA PKCS #10]: RSA Laboratories, *Certification Request Syntax Standard* version 1.7 (2000). Available online.

[RSA PKCS #12]: RSA Laboratories, *Personal Information Exchange Syntax* version 1.0 (1999). Available online.

13. Acronyms and Abbreviations

IdenTrust incorporates Section 14 of the ECA CP and includes other acronyms in the CPS as follows:

(1) **CIO**: Chief Information Officer.

(2) **COO**: Chief Operating Offiicer.

(3) **TC**: Trusted Correspondent.

14. Glossary

The definitions in the ECA CP are incorporated into this CPS unless the CPS provides a different definition.

(4) **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 validity period, and (5) is digitally signed by the Certification Authority issuing it. This CPS applies only in relation to ECA Certificates and generally not to Certificates generally unless the context indicates otherwise.

(5) **Claimant**: A Relying Party, Subscriber, or Subscribing Organization (who is not the U.S. Government or a Government employee) pursuing a claim against IdenTrust; see section 9.13 of this CPS.

(6) **Client-authenticated SSL/TLS**: Transport Layer Security v.1.0 and higher are cryptographic protocols that use PKI to secure communications transmitted over the Internet. For Client-authenticated SSL/TLS sessions discussed in this CPS, the IdenTrust secure server sends its Certificate to the user's SSL/TLS-enabled client software and requests the client's Certificate. The SSL/TLS client responds by sending its Certificate to the server. The SSL/TLS client confirms the identity of the IdenTrust secure server by reference to the Certificate, which has been issued by a CA that is listed in the SSL/TLS client's list of trusted root Certificates. Both server and client check the date to see if the Certificate has expired and whether the public key of the CA will validate the CA's Digital Signature on the other party's Certificate. The SSL/TLS client determines whether the domain name in the server's Certificate matches the actual domain name being used. The IdenTrust secure server verifies the digital signature on data signed with the SSL/TLS client's private key. The server also checks for the client's Certificate in its database and determines whether the subject of the Certificate has any permissions to access resources on an access control list. Using public key cryptography, the client and server negotiate a session key for use during the Client-authenticated SSL/TLS session.

(7) **Confirm**: To ascertain the accuracy of information represented (1) in conformity with the applicable contractual obligations, the ECA CP, and this CPS, and (2) in any case, through inquiry and investigation appropriate and reasonable under the circumstances as IdenTrust determines in its discretion. This concept is sometimes termed "verification" but this CPS reserves that term for digital signature verification. Identification and authentication, identity proofing, and similar processes are aspects of confirmation.

(8) **CRL (Certificate Revocation List)**: A list of Certificates that became invalid before they expired.

(9) **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. [NIST FIPS 140-2]

(10) **IdenTrust**: IdenTrust Services, LLC, a Delaware limited liability company.

(11) **ECA Certificate**: A Certificate which can be validated for one or more of the ECA policy OIDs when starting with the ECA Root as the trust anchor and using certification path validation rules described in [IETF RFC 5280].

(12) **Individual Subscriber**: See section 1.3.3. This term means essentially the same as "Subscriber" that term is defined in the ECA CP. It is sometimes used in this CPS to distinguish clearly between the Individual Subscriber and the Subscribing Organization with which the Individual Subscriber is affiliated.

(13) **Public Key Infrastructure ("PKI")**: A Framework established to issue, maintain, and revoke public key Certificates.

(14) **PKI Sponsor**: An individual who functions in the role of a Subscriber for a non-human system component.

(15) **Registration Authority**: See section 1.3.1.3.

(16) **Registrar**: The individual before whom a prospective Individual Subscriber appears for confirmation of the Individual Subscriber's identification preparatory to issuance of a Certificate. A Registrar may be a Trusted Correspondent, an employee of IdenTrust, or a notary in some circumstances; see section 3.2.3.1.1 of this CPS.

(17) **Repository**: A system for storing and retrieving Certificates or other information relevant to Certificates.

(18) **Requestor**: An individual who is authorized, under the Key Recovery Policy, to request recovery of Subscriber's escrowed key. Subscribers can always request recovery of their own keys. Other employees within the Subscribing Organization may be authorized by the Organization, based on their internal policies, to request key recovery of any Subscriber. Law enforcement may request key recovery by service of a subpoena upon a Subscribing Organization or IdenTrust.

(19) **Server-authenticated SSL/TLS**: Transport Layer Security v.1.0 and higher are cryptographic protocols that use PKI to secure communications transmitted over the Internet. In the Server-authenticated SSL/TLS sessions discussed in this CPS, the client or user is directed to a specified, secure URL (https://). The SSL/TLS-enabled client software confirms the identity of the IdenTrust secure server by reference to a Certificate issued by a CA that is listed in the client software's list of trusted, high assurance IdenTrust Root Certificates (e.g., IdenTrust Commercial Root CA), which are embedded in the most widely distributed commercial browsers. The client software checks the date to see if the server's Certificate has expired, whether the public key of the CA will validate the Root CA's Digital Signature on the Certificate, and whether the domain name in the IdenTrust secure server's Certificate matches the actual domain name being used. Then, using the server's public key obtained from the server's Certificate for encryption, the client software sends the secure server a Master Key used to create a session key for use during the Server-authenticated SSL/TLS session. Both the secure server and the client

create a session key based on the Master Key and then begin encrypted communication.

(20) **Subscriber**: See section 1.3.3.

(21) **Subscriber Database**: A database maintained by IdenTrust that contains account information about applicants for Certificates (i.e. the Registration System / Certificate Information System) and Subscribers.

(22) **Subscribing Organization**: See section 1.3.3.

(23) **Trusted Correspondent**: See section 1.3.2.1.

(24) **Trusted Role**: See section 5.2.1

(25) **Valid Certificate**: A Certificate which (a) has been issued and accepted, (b) has not been revoked, and (c) has not expired. Expiration occurs when the time specified in the Certificate's validity:notAfter field passes. Validity is ordinarily relevant in relation to a point in time when reliance on a Certificate occurs.

15. Agreements and Forms

15.1 Subscriber Agreement

Print page

COMPLETE TERMS OF IDENTRUST SERVICES ECA CERTIFICATE SUBSCRIBER AGREEMENT:

IMPORTANT NOTICE: This ECA Certificate Subscriber Agreement is a legal agreement between IdenTrust Services, LLC ("IdenTrust") and the Applicant or Subscriber of the ECA Certificates ("Applicant"/"Subscriber"). "Subscribing Organization" shall mean the Organization identified in the application for ECA Certificates and for whom Subscriber will act under the terms of this Agreement and the Subscribing Organization Authorization Agreement in using the Private Key corresponding to the public key listed in each ECA Certificate.

Capitalized terms used herein shall have the meaning given to them in the public version of IdenTrust's ECA Certification Practices Statement (https://secure.identrust.com/certificates/policy/eca/) ("the CPS") and the current ECA Certificate Policy (http://iase.disa.mil/pki/eca/Pages/documents.aspx) ("the CP"). The public version of the CPS, the CP, the In-Person Identification Form (https://secure.identrust.com/certificates/policy/eca/) ("ID Form") and the Subscribing Organization Authorization Agreement, are incorporated by reference herein and comprise "this Agreement," as that term is used herein. IdenTrust reserves, and Applicant acknowledges and accepts IdenTrust's right to modify the CPS, which modifications shall become a part of this Agreement.

By signing the ID Form or by clicking the checkbox next to "I accept the complete terms and conditions of the Subscriber Agreement" during the online certificate application process, Applicant agrees that the information provided during the application process is accurate, current, complete, and not misleading and that Applicant will be bound by the terms and conditions of this Agreement. Applicant is also requesting that IdenTrust issue ECA Certificates that will contain Applicant's name and the name of the Subscribing Organization.

If Applicant does not accept this Agreement, then Applicant must choose "Cancel" during the online application process, and the application will be terminated.

1. Acceptance and Payment. IdenTrust will begin processing the application as soon as it has received: (a) preauthorization to charge the credit card, purchase order or voucher number provided; (b) fully completed paper forms, i.e. the Subscribing Organization Authorization Form and the In-Person Identification Form. By proceeding with the application process, Applicant authorizes IdenTrust to bill the Subscribing Organization or the credit card for the applicable certificate issuance fee. Credit card information is transmitted securely to IdenTrust in an encrypted format and is securely stored by IdenTrust. Upon certificate approval, IdenTrust will process the credit card charge or purchase order. IdenTrust will revoke any ECA Certificates not paid for within 60 days of certificate issuance.

2. Identification Procedure. After Applicant has completed the electronic portion of the application process, IdenTrust provides Applicant with a Subscribing Organization Authorization Agreement and an In-Person Identification Form (the "ID Form"). The Applicant must sign the ID Form in the presence of a Registrar, i.e. a person authorized to perform the in-person confirmation of identity. As part of the ECA Certificate issuance process, the Applicant must present the Registrar with a valid, government-issued photo ID and another government-issued ID. At least one of the documents must establish country of citizenship. For non-U.S. citizens, a passport is required. The documents presented to the Registrar must be the same as those reported to IdenTrust during the electronic application process. Sign the ID Form in the presence of the Registrar, the Registrar must review the Applicant's credentials and also sign the ID Form. The ID Form contains instructions to follow in submitting confirmation of identity to IdenTrust. If IdenTrust accepts an application for ECA Certificates and confirms the information submitted during the application process, IdenTrust will issue ECA Certificates to Applicant for use by Applicant on behalf of the Subscribing Organization.

3. ECA Key Generation, Certificate Issuance and Term. Certificates will be valid for the Validity Period specified therein. The term of this Agreement shall correspond to the term of the ECA Certificates' validity. Sections 5 through 11 of this Agreement will survive the termination, expiration or revocation of this Agreement or the Certificate. IdenTrust will keep a copy of the Private Key corresponding to the Encryption Certificate in a secure, encrypted database for Key Recovery purposes. HOWEVER, IN NO EVENT SHALL IDENTRUST EVER HAVE ACCESS TO, OR STORE, THE SUBSCRIBER'S DIGITAL SIGNATURE PRIVATE KEY. IdenTrust will provide Key Recovery services for the Private Key corresponding to the

Encryption Certificate in the event that it becomes unavailable or is subject to disclosure by an authorized party, e.g., by the Subscribing Organization. IdenTrust charges additional key recovery fees for such services in accordance with its published fee schedule or by separate agreement with IdenTrust.

4. IdenTrust Verification of Identity. IdenTrust may seek to verify the identity of the Applicant and that of the Subscribing Organization by any reasonable means. IdenTrust may make inquiry with public or private databases or other sources, for the purpose of verifying the information that Applicant and Subscribing Organization provide in order to determine whether to issue an ECA Certificate to the Applicant. IdenTrust is hereby also authorized to store and keep any information generated during the application, identification, authentication, certificate issuance and certificate management processes, which shall become the property of IdenTrust. IdenTrust, in its sole discretion and without incurring liability for any loss arising out of such denial or refusal, may deny an application for, or otherwise refuse to issue, an ECA Certificate. IdenTrust shall have no liability for any delay experienced during the Certificate issuance process, including but not limited to Applicant's inability to retrieve a certificate because more than thirty (30) days have passed since the Applicant appeared before the registrar for in-person identity proofing.

5. Privacy. IdenTrust agrees to take reasonable care to ensure that private information submitted or obtained during the application, identification and authentication, and certificate issuance processes will be kept private. Except as necessary to carry out the provisions of this Agreement, or for auditing purposes, or as otherwise required by law or court order, IdenTrust will protect the confidentiality of such private information and will not sell, rent, lease, or disclose such information in any manner to any person without prior permission. IdenTrust also agrees to protect such information in a manner designed to ensure its integrity and to make it available to the Subscriber or the Subscribing Organization, following an appropriate request. However, information contained in ECA Certificates and related status information are not private. (That would defeat the purpose of an ECA Certificate, which is to establish a person's identity.) Accordingly, IdenTrust may disclose the Subscriber's name, public key, email address, citizenship, Subscribing Organization's name, the certificate serial number, and the certificate expiration date to any person and for any purpose.

6. Subscriber Obligations

6.1. Submit Correct Information. Applicant warrants and represents that he or she is obtaining the ECA Certificate for use in compliance with one of the reasons stated in Section 1.3.4 of the CP (e.g. an employee of a business or governmental entity conducting business with a US government agency at the local, state or Federal level); that all of the information provided during the application process is accurate, current, complete, and not misleading; and that Applicant has provided IdenTrust with all facts material to IdenTrust's ability to confirm Applicant's identity and material to the reliability of the ECA Certificates to be issued. Applicant represents that he or she will immediately inform IdenTrust if any information submitted in any application form or during the application process changes or becomes false or misleading.

6.2. Key Protection and Certificate Use. IdenTrust issues an ECA Certificate based on a public key that the Applicant sends to IdenTrust. In public key Cryptography, a Key Pair of two mathematically related keys is generated by computer software whereby a public key has a corresponding Private Key. The Key Pair is stored on a computer, smart card, or some other cryptographic hardware device. To obtain an ECA Certificate, Applicant will need to submit an ECA Certificate request to IdenTrust containing the Applicant's public key. When IdenTrust creates the ECA Certificate, the public key is included in the ECA Certificate.

By requesting ECA Certificates from IdenTrust, Applicant:

a) Agrees to protect each Private Key corresponding to each public key submitted to IdenTrust;

b) Warrants and represents that he or she has kept and will keep the Private Keys private and will safeguard and maintain the Private Keys (and any user IDs, account passwords, passwords or PINs used to activate the Private Keys) in strict secrecy and take reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, the Private Keys and the computer system or media on which the Private Keys are stored;

c) Agrees to use ECA Certificates only in accordance with this Agreement and in conjunction with the uses permitted by the CP;

d) Agrees not to use the ECA Certificate(s) issued by IdenTrust for purposes of fraud, any other illegal scheme, or any use requiring fail-safe performance where failure could lead directly to death, personal injury, or severe environmental damage;

e) Agrees during initial registration and subsequent key recovery requests to provide accurate identification and authentication information;

f) Agrees that when notified that the escrowed Private Key corresponding to his or her Encryption Certificate has been recovered, to determine whether revocation of such Certificate is necessary and request revocation, if necessary; and

g) Agrees that whenever the Subscriber's Private Key has been compromised, or is suspected of compromise, the Subscriber will immediately contact IdenTrust and request that the ECA Certificate be revoked. A revocation request may be sent in a signed email (containing the reason for revocation and using the key for which revocation is requested) to ecaservices@identrust.com, by calling the IdenTrust Help Desk at 1-888-882-1104 (U.S.) or 1-801-924-8141 (International) or by facsimile at 801-924-8138.

h) Agrees that the ECA Certificate(s) issued by IdenTrust may only be used for one of the following purposes:

1. Employees of businesses acting in the capacity of an employee and conducting business with a US government agency at local, state, or Federal level;
2. Employees of state and local governments conducting business with a US government agency at local, state, or Federal level;
3. Employees of foreign governments or organizations conducting business with a US government agency at a local, state, or Federal level.
4. Individuals communicating securely with a US government agency at local, state, or Federal level; and
5. Workstations, guards and firewalls, routers, trusted servers (e.g., database, FTP, and WWW), and other infrastructure components communicating securely with or for a US government agency at local, state, or Federal level. These components must be under the cognizance of humans, who accept the Certificate and are responsible for the correct protection and use of the associated private key.

NOTICE IS HEREBY GIVEN THAT THE THEFT, COMPROMISE, OR MISUSE OF THE PRIVATE KEY MAY CAUSE THE SUBSCRIBER OR THE SUBSCRIBING ORGANIZATION SERIOUS ADVERSE LEGAL CONSEQUENCES.

IF SECURITY OF THE PRIVATE KEY HAS BEEN OR IS IN DANGER OF BEING COMPROMISED IN ANY WAY, SUBSCRIBER AND/OR THE SUBSCRIBING ORGANIZATION MUST IMMEDIATELY NOTIFY IDENTRUST AND REQUEST THAT IDENTRUST REVOKE THE ECA CERTIFICATE.

6.3. Review the ECA Certificate; ECA Certificate Acceptance. The contents of the ECA Certificates issued to the Subscriber will be based on information provided by the Subscriber and the Subscribing Organization. After downloading the ECA Certificates from the Web site designated by IdenTrust, the Subscriber shall examine the contents of his or her ECA Certificates. The Subscriber shall promptly review and verify the accuracy of the information contained in the ECA Certificates. Subscriber acknowledges that downloading or using the ECA Certificate constitutes acceptance of the Certificate and its contents. If the Subscriber fails to notify IdenTrust of any errors, defects, or problems with an ECA Certificate within 24 hours after downloading it, it will be considered to have been accepted. By accepting the ECA Certificate, the Subscriber further acknowledges that all information in the ECA Certificate is accurate, current, complete, and not misleading and that he or she is not aware of any fact material to the reliability of that information that has not been previously communicated to IdenTrust. Upon acceptance, and upon each occasion thereafter when the Subscriber uses the ECA Certificate or the Private Key corresponding to the ECA Certificate, the responsibilities identified herein, as well as those in the public version of the CPS and in the ECA CP, are reaffirmed.

6.4. Revoke the ECA Certificate If Necessary.

(a) Permissive Revocation

1. The Subscriber may request revocation of the Certificate at any time for any reason. The Subscribing Organization may request revocation of a Certificate issued to its Individual Subscriber at any time for any reason.
2. IdenTrust may also revoke the Certificates:
   i. Upon the Subscriber's failure, (or that of the Subscribing Organization, where applicable) to meet its obligations under the ECA CP, the public version of the CPS, or an applicable agreement, regulation, or law; or
   ii. For any of the other reasons for Certificate revocation set forth in the CP, public version of the CPS, or any other reasonable grounds for revocation.

(b) Required Revocation

1. The Subscriber and Subscribing Organization are responsible for promptly requesting revocation of a Certificate as soon as any of the following events occurs:
   i. The Subscriber's name or any other information in the Certificate becomes inaccurate or is discovered to be inaccurate;

ii. The private key corresponding to the public key in the ECA Certificate, or the media holding that private key has been compromised or such a compromise is suspected; or

iii. The Subscriber's employment with the Subscribing Organization ends.

2. The Subscriber and Subscribing Organization assume the risk of any failure to request a revocation required above.
3. IdenTrust will revoke the Certificates:
   i. If IdenTrust learns, or reasonably suspects, that the private key corresponding to the public key listed in a Certificate has been compromised;
   ii. If IdenTrust determines that the Certificates were not issued in accordance with the ECA CP and/or IdenTrust's ECA CPS;
   iii. Upon determining that the Certificates have become unreliable or that material information in the application for the Certificates or in the Certificates themselves have changed or have become false or misleading (e.g., the Subscriber changes his or her name);
   iv. A governmental authority has lawfully ordered IdenTrust to revoke the Certificates; or
   v. If other circumstances transpire that cause the Certificates to be misleading to a relying party or in violation of the ECA CP, the public version of the CPS, or other ECA requirements.

6.5. Cease Using the ECA Certificate. Except for sending a signed e-mail requesting revocation of the Certificate, the Subscriber agrees to immediately cease using his or her ECA Certificate in the following circumstances: (i) when the Private Key corresponding to the ECA Certificate has been or may be compromised or subjected to unauthorized use in any way; (ii) when any information in the ECA Certificate is no longer accurate, current, or complete or becomes misleading, (iii) upon the revocation or expiration of the ECA Certificate, or (iv) upon termination of this Agreement or employment with the Subscribing Organization.

6.6. Indemnification. If the Subscribing Organization is not a State government, the U.S. Government, or one of their political subdivisions, the Subscriber and Subscribing Organization shall indemnify and hold IdenTrust and its officers, directors, employees, Trusted Correspondents, and affiliates harmless from any and all liabilities, costs, and expenses, including reasonable attorneys' fees, related to: any intentional misrepresentation or omission of material fact made by the Subscriber; any compromise or misuse of the Private Key or ECA Certificate caused directly or indirectly by the Subscriber's negligent or intentional conduct, unless prior to that compromise or misuse the Subscriber or Subscribing Organization appropriately requested revocation of the Certificates; or any violation of this Agreement by the Subscriber or the Subscribing Organization.

7. IdenTrust Warranties. IdenTrust warrants that the procedures it uses to issue and manage ECA Certificates are in accordance with the CP and the CPS.

8. DISCLAIMER OF WARRANTIES. IDENTRUST DISCLAIMS ANY AND ALL WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, THAT ARE NOT SPECIFICALLY PROVIDED HEREIN, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO IDENTRUST SERVICES OR ANY ECA CERTIFICATE ISSUED HEREUNDER.

9. Limitation of Liability. IdenTrust shall not be liable for any consequential, indirect, special, remote, exemplary, punitive or incidental damages, including, without limitation, damages arising from loss of profits, revenues, savings, opportunities or data, injuries to customer relationships or business interruption, regardless of the cause of action, even if IdenTrust has been advised of the possibility of such loss. IDENTRUST SHALL HAVE NO LIABILITY FOR LOSS DUE TO USE OF AN IDENTRUST-ISSUED ECA CERTIFICATE, UNLESS THE LOSS IS PROVEN TO BE A DIRECT RESULT OF A BREACH BY IDENTRUST OF THE CP OR THE CPS OR A PROXIMATE RESULT OF THE NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT OF IDENTRUST.

IdenTrust's entire liability, in law or in equity, for losses due to its operations at variance with its procedures defined in the ECA CP or the CPS shall not exceed either of the following limits:

- One thousand U.S. dollars (USD $1,000) for all recoverable losses sustained by each person, whether natural or legal, as a result of a single transaction involving the reliance upon or use of a certificate.
- One million U.S. dollars (USD $1,000,000) maximum aggregate total liability for all recoverable losses sustained by all persons as a result of a single incident (i.e. the aggregate of all transactions) arising out of the reliance upon or use of a certificate.

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.

10. Dispute Resolution Provisions. This Agreement, the Subscribing Organization Authorization Agreement, the ID Form, the public version of the CPS, and the CP constitute the entire agreement between Subscriber, Subscribing Organization and IdenTrust. With respect to US Government Subscribers or US Government Relying Parties, this Agreement, the Subscribing Organization Authorization Agreement, the ID Form, and the CPS and their interpretation shall be governed by the Contracts Disputes Act of 1978, as amended (41 US.C. § 601 et seq.). With respect to State governments, this Agreement and its attached Terms and Conditions shall be construed, interpreted, and enforced in accordance with the substantive laws of that State, without regard to its conflicts of law rules. In all other cases, they shall be governed by, and interpreted and construed under, the laws of the State of Utah without regard to its conflicts of law principles. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

If any provision of this Agreement, the Subscribing Organization Authorization Agreement, the ID Form, or the CPS is found to be invalid or unenforceable, then such document shall be deemed amended by modifying such provision to the extent necessary to make it valid and enforceable while preserving its intent or, if that is not possible, by striking the provision and enforcing the remainder of this Agreement.

The dispute resolution procedures specified in this Agreement shall provide the sole remedy for any claim against IdenTrust for any loss sustained by any Relying Party, Subscriber, or Subscribing Organization, whether that loss is claimed to arise from reliance on a Certificate, from breach of a contract, from a failure to perform according to the ECA CP and/or the CPS, or from any other act or omission. No Relying Party, Subscriber, or Subscribing Organization shall require IdenTrust to respond to any attempt to seek recourse through any other means.

10.1 Claims and Claim Determinations. Before making a claim to recover a loss for which IdenTrust may be responsible, a Subscriber, Relying Party, or Subscribing Organization who is not the U.S. Government, a State Government, or a Government employee (the "Claimant") shall make a thorough investigation. IdenTrust will cooperate reasonably in that investigation. The Claimant will then present to IdenTrust reasonable documented proof:

a) That the Claimant has suffered a recoverable loss as a result of a transaction;
b) Of the amount and extent of the recoverable loss claimed; and
c) Of the causal linkage between the alleged transaction and the recoverable loss claimed, itemized as necessary.

Upon the occurrence of any loss arising out of a transaction, the Claimant shall file notice and all required proof of the claim (using a procedure accessed through IdenTrust's web site) not later than one year after the date of discovery of the facts out of which the claim arose. Notice of the claim must be given on an IdenTrust Claim-Loss Form downloadable from https://secure.identrust.com/certificates/policy/eca. Instructions for completion and submission of the claim form also appear in the Claim-Loss Form downloadable from that web page.

On receipt of a claim form, IdenTrust may determine to pay the claim or deny it. IdenTrust may also pay the claim in an amount less than the amount claimed if IdenTrust determines that the loss calculations exceed the amount that IdenTrust is obligated to pay. IdenTrust will notify the Claimant of its determination within 30 days of receipt of the claim form.

If the claimant is not satisfied with IdenTrust's determination of the claim, the Claimant may seek judicial relief as provided in the next section.

10.2 Judicial Review. A Relying Party, Subscriber, or Subscribing Organization who is not the U.S. Government, a State Government or a Government Subscriber may contest the determination of the claim by IdenTrust under the preceding section by filing suit as provided herein within one year after IdenTrust's determination of the claim.

The courts of the State of Utah have exclusive subject matter jurisdiction over all suits and any other disputes arising out of or based on this Agreement, the ECA CP, or the public version of the CPS, including suits for judicial review of claims decided according to the preceding section. The parties hereby waive any right to trial by jury of any claim or suit arising out of the CP, the public version of the CPS, or this Agreement.

11. Survival. Sections 5-11 of this Agreement and the provisions of the ID Form shall survive any termination or expiration of this Agreement or expiration or revocation of the ECA Certificates.

15.2 PKI Sponsor Agreement

Print page

COMPLETE TERMS OF IDENTRUST SERVICES ECA SSL CERTIFICATE AGREEMENT:

IMPORTANT NOTICE: This ECA SSL Certificate Agreement is a legal agreement between IdenTrust Services, LLC ("IdenTrust") and the Applicant or PKI Sponsor of the ECA SSL Certificates ("Applicant"/"Subscriber"). "Subscribing Organization" shall mean the Organization identified in the application for ECA SSL Certificates and for whom PKI Sponsor will act under the terms of this Agreement and the SSL Subscribing Organization Authorization Agreement in using the Private Key corresponding to the public key listed in each ECA SSL Certificate. "Component" shall mean a non-human system that is identified in the subject of an ECA SSL Certificate, is owned by the Subscribing Organization, and is administered by the PKI Sponsor.

Capitalized terms used herein shall have the meaning given to them in the public version of IdenTrust's ECA Certification Practices Statement (https://secure.identrust.com/certificates/policy/eca/) ("the CPS") and the current ECA SSL Certificate Policy (http://iase.disa.mil/pki/eca/documents.html) ("the CP"). The public version of the CPS, the CP, the In-Person Identification Form (https://secure.identrust.com/certificates/policy/eca/) ("ID Form") and the Subscribing Organization Authorization Agreement, are incorporated by reference herein and comprise "this Agreement," as that term is used herein. IdenTrust reserves, and Applicant acknowledges and accepts IdenTrust's right to modify the CPS, which modifications shall become a part of this Agreement.

By signing the ID Form or by clicking the checkbox next to "I accept the complete terms and conditions of the ECA SSL Agreement" during the online certificate application process, Applicant agrees that the information provided during the application process is accurate, current, complete, and not misleading and that Applicant will be bound by the terms and conditions of this Agreement. Applicant is also requesting that IdenTrust issue ECA SSL Certificates that will contain Component's name and the name of the Subscribing Organization.

If Applicant does not accept this Agreement, then Applicant must choose "Cancel" during the online application process, and the application will be terminated.

1. Acceptance and Payment. IdenTrust will begin processing the application as soon as it has received: (a) preauthorization to charge the credit card, purchase order or voucher number provided; (b) fully completed paper forms, i.e. the SSL Subscribing Organization Authorization Form and the In-Person Identification Form. By proceeding with the application process, Applicant authorizes IdenTrust to bill the Subscribing Organization or the credit card for the applicable certificate issuance fee. Credit card information is transmitted securely to IdenTrust in an encrypted format and is securely stored by IdenTrust. Upon certificate approval, IdenTrust will process the credit card charge or purchase order. IdenTrust will revoke any ECA SSL Certificates not paid for within 60 days of certificate issuance.

2. Identification Procedure. After Applicant has completed the electronic portion of the application process, IdenTrust provides Applicant with a Subscribing Organization Authorization Agreement and an In-Person Identification Form (the "ID Form"). The Applicant must sign the ID Form in the presence of a Registrar, i.e. a person authorized to perform the in-person confirmation of identity. As part of the ECA SSL Certificate issuance process, the Applicant must present the Registrar with a valid, government-issued photo ID and another government-issued ID. At least one of the documents must establish country of citizenship. For non-U.S. citizens, a passport is required. The documents presented to the Registrar must be the same as those reported to IdenTrust during the electronic application process. Sign the ID Form in the presence of the Registrar, the Registrar must review the Applicant's credentials and also sign the ID Form. The ID Form contains instructions to follow in submitting confirmation of identity to IdenTrust. If IdenTrust accepts an application for ECA SSL Certificates and confirms the information submitted during the application process, IdenTrust will issue ECA SSL Certificates to Component for use by Applicant on behalf of the Subscribing Organization.

3. ECA Key Generation, Certificate Issuance and Term. Certificates will be valid for the Validity Period specified therein. The term of this Agreement shall correspond to the term of the ECA SSL Certificates' validity. Sections 5 through 11 of this Agreement will survive the termination, expiration or revocation of this Agreement or the Certificate. IN NO EVENT SHALL IDENTRUST EVER HAVE ACCESS TO, OR STORE, THE COMPONENT'S DIGITAL SIGNATURE PRIVATE KEY.

4. IdenTrust Verification of Identity. IdenTrust may seek to verify the identity of the Applicant, Component, and that of the Subscribing Organization by any reasonable means. IdenTrust may make inquiry with public or private databases or other sources, for the purpose of verifying the information that

Applicant and Subscribing Organization provide in order to determine whether to issue an ECA SSL Certificate to the Component. IdenTrust is hereby also authorized to store and keep any information generated during the application, identification, authentication, certificate issuance and certificate management processes, which shall become the property of IdenTrust. IdenTrust, in its sole discretion and without incurring liability for any loss arising out of such denial or refusal, may deny an application for, or otherwise refuse to issue, an ECA SSL Certificate. IdenTrust shall have no liability for any delay experienced during the certificate issuance process, including but not limited to Applicant's inability to retrieve a Certificate because more than thirty (30) days have passed since the Applicant appeared before the registrar for in-person identity proofing.

5. Privacy. IdenTrust agrees to take reasonable care to ensure that private information submitted or obtained during the application, identification and authentication, and certificate issuance processes will be kept private. Except as necessary to carry out the provisions of this Agreement, or for auditing purposes, or as otherwise required by law or court order, IdenTrust will protect the confidentiality of such private information and will not sell, rent, lease, or disclose such information in any manner to any person without prior permission. IdenTrust also agrees to protect such information in a manner designed to ensure its integrity and to make it available to the Subscriber or the Subscribing Organization, following an appropriate request. However, information contained in ECA SSL Certificates and related status information are not private. (That would defeat the purpose of an ECA SSL Certificate, which is to establish a Component's identity.) Accordingly, IdenTrust may disclose the Component's identifier, public key, email address, Subscribing Organization's name, the certificate serial number, and the certificate expiration date to any person and for any purpose.

6. PKI Sponsor Obligations

6.1. Submit Correct Information. Applicant warrants and represents that he or she is obtaining the ECA SSL Certificate for use in compliance with one of the reasons stated in Section 1.3.4 of the CP (e.g. an employee of a business or governmental entity administering a Component used in conducting business with a US government agency at the local, state or Federal level); that all of the information provided during the application process is accurate, current, complete, and not misleading; and that Applicant has provided IdenTrust with all facts material to IdenTrust's ability to confirm Applicant's and Component's identity and material to the reliability of the ECA SSL Certificates to be issued. Applicant represents that he or she will immediately inform IdenTrust if any information submitted in any application form or during the application process changes or becomes false or misleading.

6.2. Key Protection and Certificate Use. IdenTrust issues an ECA SSL Certificate based on a public key that the Applicant sends to IdenTrust. In public key Cryptography, a Key Pair of two mathematically related keys is generated by computer software whereby a public key has a corresponding Private Key. The Key Pair is stored on a computer, smart card, or some other cryptographic hardware device. To obtain an ECA SSL Certificate, Applicant will need to submit an ECA SSL Certificate request to IdenTrust containing theComponent's public key. When IdenTrust creates the ECA SSL Certificate, the public key is included in the ECA SSL Certificate.

By requesting ECA SSL Certificates from IdenTrust, Applicant:

a) Agrees to protect each Private Key corresponding to each public key submitted to IdenTrust;

b) Warrants and represents that he or she has kept and will keep the Private Keys private and will safeguard and maintain the Private Keys (and any user IDs, account passwords, passwords or PINs used to activate the Private Keys) in strict secrecy and take reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, the Private Keys and the computer system or media on which the Private Keys are stored;

c) Agrees to use ECA SSL Certificates only in accordance with this Agreement and in conjunction with the uses permitted by the CP;

d) Agrees not to use the ECA SSL Certificate(s) issued by IdenTrust for purposes of fraud, any other illegal scheme, or any use requiring fail-safe performance where failure could lead directly to death, personal injury, or severe environmental damage;

e) Agrees that whenever the Component's Private Key has been compromised, or is suspected of compromise, the Applicant will immediately contact IdenTrust and request that the ECA SSL Certificate be revoked. A revocation request may be sent in a signed email (containing the reason for revocation and using the key for which revocation is requested) to ecaservices@identrust.com, by calling the IdenTrust Help Desk at 1-888-882-1104 (U.S.) or 1-801-924-8141 (International) or by facsimile at 801-924-8138.

NOTICE IS HEREBY GIVEN THAT THE THEFT, COMPROMISE, OR MISUSE OF THE PRIVATE KEY MAY CAUSE THE PKI SPONSOR OR THE SUBSCRIBING ORGANIZATION SERIOUS ADVERSE LEGAL CONSEQUENCES.

IF SECURITY OF THE PRIVATE KEY HAS BEEN OR IS IN DANGER OF BEING COMPROMISED IN ANY WAY, PKI SPONSOR AND/OR THE SUBSCRIBING ORGANIZATION MUST IMMEDIATELY NOTIFY IDENTRUST AND REQUEST THAT IDENTRUST REVOKE THE ECA SSL CERTIFICATE.

6.3. Review the ECA SSL Certificate Acceptance. The contents of the ECA SSL Certificates issued to the Component will be based on information provided by the PKI Sponsor and the Subscribing Organization. After downloading the ECA SSL Certificates from the Web site designated by IdenTrust, the PKI Sponsor shall examine the contents of his or her ECA SSL Certificates. The PKI Sponsor shall promptly review and verify the accuracy of the information contained in the ECA SSL Certificates. PKI Sponsor acknowledges that downloading or using the ECA SSL Certificate constitutes acceptance of the Certificate and its contents. If the PKI Sponsor fails to notify IdenTrust of any errors, defects, or problems with an ECA SSL Certificate within 24 hours after downloading it, it will be considered to have been accepted. By accepting the ECA SSL Certificate, the PKI Sponsor further acknowledges that all information in the ECA SSL Certificate is accurate, current, complete, and not misleading and that he or she is not aware of any fact material to the reliability of that information that has not been previously communicated to IdenTrust. Upon acceptance, and upon each occasion thereafter when the Component uses the ECA SSL Certificate or the Private Key corresponding to the ECA SSL Certificate, the responsibilities identified herein, as well as those in the public version of the CPS and in the ECA CP, are reaffirmed.

6.4. Revoke the ECA SSL Certificate If Necessary.

(a) Permissive Revocation

1. The PKI Sponsor may request revocation of the Certificate at any time for any reason. The Subscribing Organization may request revocation of a Certificate issued to its Component at any time for any reason.
2. IdenTrust may also revoke the Certificates:
   i. Upon the PKI Sponsor's failure, (or that of the Subscribing Organization, where applicable) to meet its obligations under the ECA CP, the public version of the CPS, or an applicable agreement, regulation, or law; or
   ii. For any of the other reasons for Certificate revocation set forth in the CP, public version of the CPS, or any other reasonable grounds for revocation.

(b) Required Revocation

4. The PKI Sponsor and Subscribing Organization are responsible for promptly requesting revocation of a Certificate as soon as any of the following events occurs:
   i. The Component's name or any other information in the Certificate becomes inaccurate or is discovered to be inaccurate;
   ii. The private key corresponding to the public key in the ECA SSL Certificate, or the crypto-module holding that private key has been compromised or such a compromise is suspected; or
   iii. The PKI Sponsor's employment with the Subscribing Organization ends.
5. The PKI Sponsor and Subscribing Organization assume the risk of any failure to request a revocation required above.
6. IdenTrust will revoke the Certificates:
   i. If IdenTrust learns, or reasonably suspects, that the private key corresponding to the public key listed in a Certificate has been compromised;
   ii. If IdenTrust determines that the Certificates were not issued in accordance with the ECA CP and/or IdenTrust's ECA CPS;
   iii. Upon determining that the Certificates have become unreliable or that material information in the application for the Certificates or in the Certificates themselves have changed or have become false or misleading (e.g., the Subscriber changes his or her name);
   iv. A governmental authority has lawfully ordered IdenTrust to revoke the Certificates; or
   v. If other circumstances transpire that cause the Certificates to be misleading to a relying party or in violation of the ECA CP, the public version of the CPS, or other ECA requirements.

6.5. Cease Using the ECA SSL Certificate. Except for sending a signed e-mail requesting revocation of the Certificate, the PKI Sponsor agrees to immediately cease using Component's ECA SSL Certificate in the following circumstances: (i) when the Private Key corresponding to the ECA SSL Certificate has been or may be compromised or subjected to unauthorized use in any way; (ii) when any information in the ECA SSL Certificate is no longer accurate, current, or complete or becomes misleading, (iii) upon the revocation or expiration of the ECA SSL Certificate, or (iv) upon termination of this Agreement or lack of ownership of component by the Subscribing Organization.

6.6. Indemnification. If the Subscribing Organization is not a State government, the U.S. Government, or one of their political subdivisions, the PKI Sponsor and Subscribing Organization shall indemnify and hold IdenTrust and its officers, directors, employees, Trusted Correspondents, and affiliates harmless from any and all liabilities, costs, and expenses, including reasonable attorneys' fees, related to: any intentional misrepresentation or omission of material fact made by the Subscriber; any compromise or misuse of the Private Key or ECA SSL Certificate caused directly or indirectly by the PKI Sponsor's negligent or intentional conduct, unless prior to that compromise or misuse the PKI Sponsor or Subscribing Organization appropriately requested revocation of the Certificates; or any violation of this Agreement by the PKI Sponsor or the Subscribing Organization.

7. IdenTrust Warranties. IdenTrust warrants that the procedures it uses to issue and manage ECA SSL Certificates are in accordance with the CP and the CPS.

8. DISCLAIMER OF WARRANTIES. IDENTRUST DISCLAIMS ANY AND ALL WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, THAT ARE NOT SPECIFICALLY PROVIDED HEREIN, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO IDENTRUST SERVICES OR ANY ECA SSL CERTIFICATE ISSUED HEREUNDER.

9. Limitation of Liability. IdenTrust shall not be liable for any consequential, indirect, special, remote, exemplary, punitive or incidental damages, including, without limitation, damages arising from loss of profits, revenues, savings, opportunities or data, injuries to customer relationships or business interruption, regardless of the cause of action, even if IdenTrust has been advised of the possibility of such loss. IDENTRUST SHALL HAVE NO LIABILITY FOR LOSS DUE TO USE OF AN IDENTRUST-ISSUED ECA SSL CERTIFICATE, UNLESS THE LOSS IS PROVEN TO BE A DIRECT RESULT OF A BREACH BY IDENTRUST OF THE CP OR THE CPS OR A PROXIMATE RESULT OF THE NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT OF IDENTRUST.

IdenTrust's entire liability, in law or in equity, for losses due to its operations at variance with its procedures defined in the ECA CP or the CPS shall not exceed either of the following limits:

- One thousand U.S. dollars (USD $1,000) for all recoverable losses sustained by each person, whether natural or legal, as a result of a single transaction involving the reliance upon or use of a certificate.
- One million U.S. dollars (USD $1,000,000) maximum aggregate total liability for all recoverable losses sustained by all persons as a result of a single incident (i.e. the aggregate of all transactions) arising out of the reliance upon or use of a certificate.

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.

10. Dispute Resolution Provisions. This Agreement, the Subscribing Organization Authorization Agreement, the ID Form, the public version of the CPS, and the CP constitute the entire agreement between PKI Sponsor, Subscribing Organization and IdenTrust. With respect to US Government PKI Sponsor or US Government Relying Parties, this Agreement, the Subscribing Organization Authorization Agreement, the ID Form, and the CPS and their interpretation shall be governed by the Contracts Disputes Act of 1978, as amended (41 US.C. § 601 et seq.). With respect to State governments, this Agreement and its attached Terms and Conditions shall be construed, interpreted, and enforced in accordance with the substantive laws of that State, without regard to its conflicts of law rules. In all other cases, they shall be governed by, and interpreted and construed under, the laws of the State of Utah without regard to its conflicts of law principles. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

If any provision of this Agreement, the Subscribing Organization Authorization Agreement, the ID Form, or the CPS is found to be invalid or unenforceable, then such document shall be deemed amended by modifying such provision to the extent necessary to make it valid and enforceable while preserving its intent or, if that is not possible, by striking the provision and enforcing the remainder of this Agreement.

The dispute resolution procedures specified in this Agreement shall provide the sole remedy for any claim against IdenTrust for any loss sustained by any Relying Party, PKI Sponsor, or Subscribing Organization, whether that loss is claimed to arise from reliance on a Certificate, from breach of a contract, from a failure to perform according to the ECA CP and/or the CPS, or from any other act or omission. No Relying Party, PKI Sponsor, or Subscribing Organization shall require IdenTrust to respond to any attempt to seek recourse through any other means.

10.1 Claims and Claim Determinations. Before making a claim to recover a loss for which IdenTrust may be responsible, a PKI Sponsor, Relying Party, or Subscribing Organization who is not the U.S. Government, a State Government, or a Government employee (the "Claimant") shall make a thorough

investigation. IdenTrust will cooperate reasonably in that investigation. The Claimant will then present to IdenTrust reasonable documented proof:

a) That the Claimant has suffered a recoverable loss as a result of a transaction;
b) Of the amount and extent of the recoverable loss claimed; and
c) Of the causal linkage between the alleged transaction and the recoverable loss claimed, itemized as necessary.

Upon the occurrence of any loss arising out of a transaction, the Claimant shall file notice and all required proof of the claim (using a procedure accessed through IdenTrust's web site) not later than one year after the date of discovery of the facts out of which the claim arose. Notice of the claim must be given on an IdenTrust Claim-Loss Form downloadable from https://secure.identrust.com/certificates/policy/eca. Instructions for completion and submission of the claim form also appear in the Claim-Loss Form downloadable from that web page.

On receipt of a claim form, IdenTrust may determine to pay the claim or deny it. IdenTrust may also pay the claim in an amount less than the amount claimed if IdenTrust determines that the loss calculations exceed the amount that IdenTrust is obligated to pay. IdenTrust will notify the Claimant of its determination within 30 days of receipt of the claim form.

If the claimant is not satisfied with IdenTrust's determination of the claim, the Claimant may seek judicial relief as provided in the next section.

10.2 Judicial Review. A Relying Party, PKI Sponsor, or Subscribing Organization who is not the U.S. Government, a State Government or a Government Subscriber may contest the determination of the claim by IdenTrust under the preceding section by filing suit as provided herein within one year after IdenTrust's determination of the claim.

The courts of the State of Utah have exclusive subject matter jurisdiction over all suits and any other disputes arising out of or based on this Agreement, the ECA CP, or the public version of the CPS, including suits for judicial review of claims decided according to the preceding section. The parties hereby waive any right to trial by jury of any claim or suit arising out of the CP, the public version of the CPS, or this Agreement.

11. Survival. Sections 5-11 of this Agreement and the provisions of the ID Form shall survive any termination or expiration of this Agreement or expiration or revocation of the ECA SSL Certificates.

15.3 In-Person Identification Form (Medium Hardware Assurance)

INSTRUCTIONS FOR APPLICANT

(Medium Hardware Assurance Certificates)

Instructions for Applicant

You will be working with a Trusted Correspondent from your organization or a person specifically appointed by IdenTrust to get your DOD ECA certificate. As a part of the Certificate application process, you will be asked to complete and sign an **In-Person Identification** form in the presence of the IdenTrust Registrar or Trusted Correspondent.

YOU ONLY HAVE 30 DAYS AFTER YOU SIGN THESE FORMS TO COMPLETE THE APPLICATION PROCESS AND RETRIEVE YOUR CERTIFICATE.

STEP 1: Online Application

Begin the application process online at http://www.identrust.com/certificates/eca/buy_eca.html. By completing the online application process and by signing the **In-Person Identification Form** you agree to the terms of the ECA Certificate Subscriber Agreement and IdenTrust's ECA Certificate Practices Statement (CPS), located here: http://www.identrust.com/certificates/eca/eca_downloads.html.. You also agree to the terms of the current ECA Certificate Policy (CP) located at http://iase.disa.mil/pki/eca/documents.html.

STEP 2: Subscribing Organization Authorization Form

Complete **Part I - Subscribing Organization Authorization Form**. Take Part I - Subscribing Organization Authorization Form to an officer in your Organization who can sign on behalf of your Organization and bind your Organization to the terms and conditions of the document. Have the officer sign Part I - Subscribing Organization Authorization Form and return it to you for submission to IdenTrust. In the event Subscribing Organization does not have an "officer", this form should then be signed by an authorized representative of the Subscribing Organization with sufficient authority to bind the Subscribing Organization to the terms hereof.

STEP 3: In-Person Identification Form

Complete and Sign **Part II - In-person Identification Form.** You must present two forms of identification to an IdenTrust Registrar or a Trusted Correspondent.

Option 1: One from List A and one from either List B or C

Option 2: One from List B and one from List C

Non-US Citizens: Valid passport and one from List B.)

***If you have more than one citizenship asserted in your certificate, you must provide proof of citizenship (i.e. passport) for each.

LIST A - Photo ID Documents that Establish Identity and Citizenship	LIST B – Photo ID Documents that Establish Identity	LIST C – Other Documents that Establish U.S. Citizenship but not Identity

1. Passport from Country of Citizenship 2. Certificate of U.S. Citizenship issued by U.S. Citizenship and Immigration Service -USCIS (formerly INS) 3. Certificate of Naturalization issued by a court of competent jurisdiction prior to October 1, 1991, or the USCIS (INS), since that date	1. Driver's license or government-issued ID card (containing a photograph) 2. Military ID (with photograph) 3. Permanent or Unexpired Temporary Resident Card issued by the USCIS (with photograph) 4. Other Official Photo ID	1. Original or certified copy of a birth certificate issued by a state, county, municipal authority, or outlying possession of the United States bearing an official seal 2. Consular Report of Birth from a U.S. Consulate (Form FS-240) 3. Certification of Birth Abroad issued by the Department of State (Form DS-1350)

STEP 4: Send forms to IdenTrust

Mailing Address: **DOD / ECA Registration**
IdenTrust Services
255 North Admiral Byrd Road
Suite 200
Salt Lake City, UT, 84116-4915

If you should have any questions during the process and would like to speak with a customer service representative, please call (888) 882-1104 or by email at helpdesk@identrust.com

Part 2: In-Person Identification Form

Terms and Conditions

The undersigned applicant attests that all facts and information provided are accurate, current, complete, and not misleading and that he or she: a) is authorized to receive, and has applied for, a digital certificate to be issued by IdenTrust; b) has read and verified the personal identifying information to be contained in the certificate; c) is who he or she represents himself or herself to be; and d) has read, understood, and agrees to the responsibilities associated with being a certificate subscriber, including the terms and conditions found in the IdenTrust Services ECA Certificate Subscriber Agreement, the public version of IdenTrust's ECA Certification Practices Statement ("CPS"), and the ECA Certificate Policy ("the ECA CP"). The applicant agrees to: 1) accurately represent him or herself in all communications; 2) protect his or her private keys at all times; 3) immediately notify IdenTrust if he or she suspects his or her private keys to have been compromised, stolen or lost; and 4) use his or her private key(s) in accordance with the above-mentioned documents.

Signed By(Applicant): _____ Date: _____

(Sign Only In The Presence of the Trusted Correspondent)

Printed Name: _____ E-mail Address: _____

You must present **two** forms of identification to the **Trusted Correspondent**, according to the following instructions:

- **Option 1:** One from List A **and** one from either List B or C
- **Option 2:** One from List B **and** one from List C
- **Non-US Citizens:** Valid passport **and** one from List B.

LIST A - Photo ID Document Establishing Identity & Citizenship (Passport / Naturalization)	**LIST B – Gov't-issued Photo ID Card (Driver's Lic., Military ID or Res. Alien)**	**LIST C – Certified Birth Certificate (U.S. Citizens Only)**
Doc. Type / Title: _____	**Doc. Type/ Title** _____	**Doc. Type/ Title** _____
Issuer: _____	**Issuer:**_____	**Issuer:**_____
Serial No.: _____	**Serial No.:**_____	**Serial No.:**_____
Exact Name Listed: _____	**Exact Name Listed:** _____	**Exact Name Listed:** _____
/Issue Date: _____	**Issue Date:** _____	**Issue Date:** _____
Expir. Date: _____	**Expir. Date**	***See Note below**

***Note**: If the name on your Birth Certificate is different from the name on your Driver's License or other form of ID, please send a **notarized** copy of a document showing the name change (Eg. A **notarized** copy of your marriage license or **notarized** certificate of marriage).

On this _____ day of _____, 20___, the Applicant listed above personally appeared before me and signed this ID Form in my presence, at which time I reviewed the above-referenced identification documents, including those containing photographs, and confirmed that: (a) the identification documents do not appear to have been altered, forged or modified; (b) the picture(s) and name on the Photo ID(s) matched the appearance and name of the individual identified as the Applicant; and (c) the Applicant is the holder of the identification documents presented.

Name of IdenTrust Registrar or Trusted Correspondent

Signature of IdenTrust Registrar or Trusted Correspondent

Additional Citizenship Addendum
(ECA In-Person Identification Form)

THIS SECTION TO BE VERIFIED BY TRUSTED CORRESPONDENT - *(ONLY NECESSARY IF MORE THAN ONE CITIZENSHIP IS ASSERTED)*

If applicant has more than one citizenship, it must be asserted in the Certificate, and the applicant must present one valid passport for each citizenship.

Second Citizenship (Passport)

Issuing Authority: _____

Doc. / ID No.: _____

Exact Name Listed on ID: _____

Issue Date: _____

Expir. Date: _____

Third Citizenship (Passport)

Issuing Authority: _____

Doc. / ID No.: _____

Exact Name Listed on ID: _____

Issue Date: _____

Expir. Date: _____

The undersigned applicant swears under penalty of perjury that all facts and information provided above are accurate and that he or she is the subject and holder of the above-referenced passports and is who he or she represents himself or herself to be.

On this _____ day of _____, 20___, the Applicant listed above personally appeared before me and signed this ID Form in my presence, at which time I reviewed the above-referenced identification documents, including those containing photographs, and confirmed that: (a) the identification documents do not appear to have been altered, forged or modified; (b) the picture(s) and name on the Photo ID(s) matched the appearance and name of the individual identified as the Applicant; and (c) the Applicant is the holder of the identification documents presented.

Name of IdenTrust Registrar or Trusted Correspondent Name	Signature of IdenTrust Registrar or Trusted Correspondent

15.4 In-Person Identification Form (Notary or Consular Officer)

INSTRUCTIONS FOR APPLICANT

As a part of the certificate application process, you will be asked to complete and sign the attached In-Person Identification Form in the presence of a Notary (or an IdenTrust Trusted Correspondent). This form may be used by all applicants for ECA Medium Assurance and Medium Token Assurance Certificates who are located in the United States, by any U.S. citizen, or by citizens of Australia, Canada, New Zealand, or the U.K. at a U.S. consulate or embassy located in one of those countries at a U.S. consulate or embassy located in one of those countries. Otherwise, you may not use this form. **If you are located outside of the United States and you are not a citizen of Australia, Canada, New Zealand, the U.K. or the U.S., you may not use this form. ALSO NOTE: YOU ONLY HAVE *30 DAYS* AFTER YOU SIGN THESE FORMS TO COMPLETE THE APPLICATION PROCESS AND RETRIEVE YOUR CERTIFICATE.**

STEP 1: Online Application

Begin the application process online at http://www.identrust.com/certificates/eca/buy_eca.html. By completing the online application process and by signing the **In-Person Identification Form** you agree to the terms of the ECA Certificate Subscriber Agreement and

IdenTrust's ECA Certification Practices Statement, (CPS) also located here:

http://www.identrust.com/certificates/eca/eca_downloads.html.

You also agree to the terms of the current ECA Certificate Policy, (CP), located here:

http://iase.disa.mil/pki/eca/documents.html.

STEP 2: Subscribing Organization Authorization Form:

Complete and Sign Part I - Sponsoring Organization Authorization Form. Take it to an officer in your Organization who can sign on behalf of your Organization and represent to IdenTrust that you are a duly-authorized representative of the Organization and that it agrees to be bound by the terms described therein (Section 2). Have the officer sign Part I - Sponsoring Organization Authorization Form and return it to you for submission to IdenTrust. Complete and Sign Part II - In-person Identification Form. This form must be filled in completely (see example page). You must

STEP 3: In-person Identification Form

Complete and Sign Part II – In-person identification Form. This form must be filled in completely (see example page). You must present two forms of identification to a Notary, Consular Officer or Trusted Correspondent, according to the following instructions:

Option 1: One from List A **and** one from either List B or C

Option 2: One from List B **and** one from List C

Non-US Citizens: Valid passport **and** one from List B.)

***If you have more than one citizenship asserted in your certificate, you must provide proof of citizenship (i.e. passport) for each.

.

LIST A - Photo ID Documents that Establish Identity and Citizenship	LIST B – Photo ID Documents that Establish Identity	LIST C – Other Documents that Establish U.S. Citizenship but not Identity
1. Passport from Country of Citizenship 2. Certificate of U.S. Citizenship issued by U.S. Citizenship and Immigration Service -USCIS (formerly INS) 3. Certificate of Naturalization issued by a court of competent jurisdiction prior to October 1, 1991, or the USCIS (INS), since that date	1. Driver's license or government-issued ID card (containing a photograph) 2. Military ID (with photograph) 3. Permanent or Unexpired Temporary Resident Card issued by the USCIS (with photograph) 4. Other Official Photo ID	1. Original or certified copy of a birth certificate issued by a state, county, municipal authority, or outlying possession of the United States bearing an official seal 2. Consular Report of Birth from a U.S. Consulate (Form FS-240) 3. Certification of Birth Abroad issued by the Department of State (Form DS-1350)

STEP 4: Send Forms to IdenTrust

STEP 4: Send Forms to IdenTrust

Record the name and place where you had the form notarized. For your records, make a copy of your Part 1 and Part 2, then send the signed (ink-on-paper) originals to IdenTrust.

Mailing Address: **ECA Registration**
IdenTrust Services
255 North Admiral Byrd Road
Suite 200
Salt Lake City, UT, 84116-4915

If you should have any questions during the process and would like to speak with a customer service representative, please call (888) 882-1104 or by email at helpdesk@identrust.com

Part 2: In-Person Identification Form

INSTRUCTIONS FOR NOTARY, CONSULAR OFFICER OR TRUSTED CORRESPONDENT:

Terms and Conditions

The undersigned applicant attests that all facts and information provided are accurate, current, complete, and not misleading and that he or she: a) is authorized to receive, and has applied for, a digital Certificate to be issued by IdenTrust; b) has read and verified the personal identifying information to be contained in the Certificate; c) is who he or she represents himself or herself to be; and d) has read, understood, and agrees to the responsibilities associated with being a Certificate Subscriber, including the terms and conditions found in the IdenTrust Services ECA Certificate Subscriber Agreement, the public version of IdenTrust's ECA Certification Practices Statement ("CPS"), and the ECA Certificate Policy ("the ECA CP"). The applicant agrees to: 1) accurately represent him or herself in all communications; 2) protect his or her private key(s) at all times; 3) immediately notify IdenTrust if he or she suspects his or her private key(s) to have been compromised, stolen or lost; and 4) use his or her private keys in accordance with the above-mentioned documents.

Signed By: _____ (Applicant)
(Sign Only In The Presence of the Notary/Consular Officer)

Date: _____

Printed Name: _____ Business Name: _____

You must present **two** forms of identification to a Notary, Consular Officer or Trusted Correspondent, according to the following instructions:

- **Option 1:** One from List A **and** one from either List B or C
- **Option 2:** One from List B **and** one from List C
- **Non-US Citizens:** Valid passport **and** one from List B.)

LIST A - Photo ID Document for Identity & Citizenship (Passport / Naturalization)	**LIST B – Gov't-issued Photo ID Card (Driver's Lic., Military ID or Res. Alien)**	**LIST C – Certified Birth Certificate (U.S. Citizens Only)**
Doc. Type / Title: _____	**Doc. Type/ Title:** _____	**Doc. Type/ Title:** _____
Issuer: _____	**Issuer:** _____	**Issuer:** _____
Serial No.: _____	**Serial No.:** _____	**Serial No.:** _____
Exact Name Listed: _____	**Exact Name Listed:** _____	**Exact Name Listed:** _____
Issue Date: _____	**Issue Date:** _____	**Issue Date:** _____
Expir. Date: _____	**Expir. Date:** _____	***See Note below**

***Note**: If the name on your Birth Certificate is different from the name on your Driver's License or other form of ID, please send a **notarized** copy of a document showing the name change (Eg. A **notarized** copy of a marriage license or **notarized** certificate of marriage).

NOTARIAL ACKNOWLEDGEMENT

I _____ (name of Notary/Officer), registered in the state of _____, county of do hereby certify under PENALTY OF PERJURY under the laws of the State of _____ that the following information is true and correct:

1. On _____ (date), before me personally appeared _____ (name of signer), who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by his/her signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.

(name of signer), who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by his/her signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.

2. I have seen and verified the forms of identification for which information is written above and hereby assert that said forms of ID do not appear to be altered, forged or modified in any way.

WITNESS my hand and official seal.

Signature _____ (seal)

ECA Registration / IdenTrust Services 255 Admiral Byrd Road Suite 200 Salt Lake City, UT 84116-4915

Additional Citizenship Addendum
(ECA In-Person Identification Form)

THIS SECTION TO BE VERIFIED BY THE NOTARY OR CONSULAR OFFICER - ***(ONLY NECESSARY IF MORE THAN ONE CITIZENSHIP IS ASSERTED)***

If applicant has more than one citizenship, it must be asserted in the Certificate, and the applicant must present one valid passport for each citizenship.

Second Citizenship (Passport)	**Third Citizenship (Passport)**
Issuer: _____	**Issuer:** _____
ID No.: _____	**ID No.:** _____
Exact Name Listed: _____	**Exact Name Listed:** _____
/Issue Date: _____	**/Issue Date:** _____
Expir. Date: _____	**Expir. Date:** _____

The undersigned applicant swears under penalty of perjury that all facts and information provided above are accurate and that he or she is the subject and holder of the above-referenced passports and is who he or she represents himself or herself to be.

Notiral Acknowledgement

State of: _____

County of: _____

Signed By: _____ (Applicant) Date: _____

(Sign Only In Presence of the Notary/Consular Officer)

Printed Name: _____

On _____ before me, _____, (name and title of the notary/officer),
(date)

personally appeared _____ (name of signer), who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by

his/her signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of _____that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature _____ (seal)

15.5 In-Person Identification Form (Authorized DoD Employee)

INSTRUCTIONS FOR APPLICANT

As a part of the Certificate application process, you will be asked to complete and sign the attached Subscribing Organization Authorization Agreement (Part 1) and the In-Person Identification Form (Part 2). The In-person Identification Form must be signed in the presence of an Authorized DoD Employee (ADE). These forms and instructions apply to all applicants for ***ECA Medium Assurance and Medium Token Assurance Certificates*** who are non-U.S. citizens and are located outside of the United States. **PLEASE NOTE: YOU ONLY HAVE *30 DAYS* AFTER YOU SIGN THESE FORMS TO COMPLETE THE APPLICATION PROCESS AND RETRIEVE YOUR CERTIFICATE.**

STEP 1: Online Application

Begin the application process online at http://www.identrust.com/certificates/eca/buy_eca.html. By completing the online application process and by signing the In-Person Identification Form you are agreeing to the terms of the ECA Certificate Subscriber Agreement ECA Certificate Practices Statement (CPS), located here: http://www.identrust.com/certificates/eca/eca_downloads.html. You also agree to the terms of the current ECA Certificate Policy (CP) located at: http://iase.disa.mil/pki/eca/documents.html.

STEP 2: Subscribing Organization Authorization Form

Complete **Part I - Subscribing Organization Authorization Form**. Take Part I - Subscribing Organization Authorization Form to an officer in your Organization who can sign on behalf of your Organization and bind your Organization to the terms and conditions of the document. Have the officer sign Part I - Subscribing Organization Authorization Form and return it to you for submission to IdenTrust. In the event Subscribing Organization does not have an "officer", this form should then be signed by an authorized representative of the Subscribing Organization with sufficient authority to bind the Subscribing Organization to the terms hereof.

STEP 3: In-person Identification Form

Complete and sign Part II – In-person Identification Form. You will need to present certain identification to the Authorized DoD Employee (ADE). All non-U.S. Citizens must present a valid passport **and** one form of identification from the list below:

1. Valid Passport

-AND-

2. Official Photo ID, such as,
    a. Driver's license with photograph
    b. Government-issued ID card containing a photograph
    c. Employee identification card from your current employer with photograph
    d. Military ID with photograph
    e. Other official photo ID

For ECA Medium Hardware Assurance applicants; your forms of identification will need to be verified by an IdenTrust Registrar or by a Trusted Correspondent and further confirmed by the Authorized DoD employee. Your In-person Identification Form needs to be signed by both parties; IdenTrust Registrar or Trusted Corresponded **-AND-** the Authorized DoD employee.

STEP 4: Send Forms to IdenTrust

Send an original Part 1: Authorization Agreement and Part 2: In-person ID Form to IdenTrust at the address below. Please keep copies for your records. Failure to submit your forms in a timely manner may result in revocation of your Certificate.

Mailing Address:

DoD / ECA Registration
IdenTrust Services
255 Admiral Byrd Road
Suite 200
Salt Lake City, UT 84116-4915
United States

If you should have any questions during the process and would like to speak with a customer service representative, please call (888) 882-1104 or by email at helpdesk@identrust.com

ECA DIGITAL CERTIFICATE PROGRAM
Foreign Subscribers
Part 2: In-Person Identification Form

The undersigned applicant attests that all facts and information provided are accurate, current, complete, and not misleading and that he/she: a) is authorized to receive, and has applied for, a digital Certificate to be issued by IdenTrust; b) has read and verified the personal identifying information to be contained in the Certificate; c) is who he/she represents himself/herself to be; and d) has read, understood, and agrees to the responsibilities associated with being a Certificate Subscriber, including the terms and conditions found in the IdenTrust Services ECA Certificate Subscriber Agreement (Part 3), the public version of IdenTrust's ECA Certification Practices Statement ("CPS"), and the ECA Certificate Policy ("the ECA CP"). The applicant agrees to: 1) accurately represent him/herself in all communications; 2) protect his/her private key(s) at all times; 3) immediately notify IdenTrust if he/she suspects his/her private keys to have been compromised, stolen or lost; and 4) use his/her private keys in accordance with the above-mentioned documents.

THIS SECTION TO BE USED BY THE APPLICANT

Signed By (Applicant): _____ Date: _____
(Sign Only In Presence of the Authorized DoD Employee)

Printed Name: _____ E-mail Address: : _____

Your application ID number is: _____

You must present **two** forms of identification to an Authorized DoD Employee (ADE). **All Non-US Citizens** must present a valid passport from their country of citizenship **and** an official photo ID as described in the instructions above.

Passport	**Official Photo ID, such as Driver's license, Military photo ID, or Government-issued photo ID card.**
Doc. Type/ Title:	Doc. Type/ Title:
Issuer:	Issuer:
Serial No.:	Serial No.:
Exact Name :	Exact Name :
Issue Date:	Issue Date:
Expir Date:	Expir Date:

ACKNOWLEDGEMENT BY AUTHORIZED DoD EMPLOYEE

Country: _____

On _____ before me, _____ (name of the ADE)
(Date)

personally appeared _____ (name of signer), who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within

instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by his/her signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.

I certify under PENALTY OF PERJURY under federal laws of the United States of America that the foregoing paragraph is true and correct.

Signature _____

Additional Citizenship Addendum
(ECA In-Person Identification Form)

THIS SECTION TO BE VERIFIED BY THE AUTHORIZED DoD EMPLOYEE - *(ONLY NECESSARY IF MORE THAN ONE CITIZENSHIP IS ASSERTED)*

If applicant has more than one citizenship, it must be asserted in the Certificate, and the applicant must present one valid passport for each citizenship.

Second Citizenship (Passport)	**Third Citizenship (Passport)**
Issuing Authority:	Issuing Authority:
Serial No.:	Serial No..:
Exact Name :	Exact Name:
Issue Date:	Issue Date:
Expir Date:	Expir Date:

The undersigned applicant swears under penalty of perjury that all facts and information provided above are accurate and that he or she is the subject and holder of the above-referenced passports and is who he or she represents himself or herself to be.

Signed By: _____ (Applicant) Date: _____

(Sign Only In Presence of the Authorized DoD Employee)

Printed Name: _____

ACKNOWLEDGEMENT BY AUTHORIZED DoD EMPLOYEE

Country: _____

On _____ before me, _____ (name of the ADE)
(Date)

personally appeared _____ (name of signer), who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by his/her signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.

I certify under PENALTY OF PERJURY under federal laws of the United States of America that the foregoing paragraph is true and correct.

Signature _____

15.6 In-Person Identification Form (for Component Certificates)

INSTRUCTIONS FOR PKI SPONSOR

As a part of the certificate application process, you will be asked to complete and sign the attached In-Person Identification Form in the presence of a Notary (or an IdenTrust Trusted Correspondent). This form may be used by all PKI Sponsors ("applicants") for ECA Secure Socket Layer (SSL) Certificates who are located in the United States, by any U.S. citizen at a U.S. consulate or embassy, or by citizens of Australia, Canada, New Zealand, or the U.K. located in one of those countries at a U.S. consulate or embassy located in one of those countries. Otherwise, you may not use this form. **If you are located outside of the United States and you are not a citizen of Australia, Canada, New Zealand, the U.K. or the U.S., you may not use this form. ALSO NOTE: YOU ONLY HAVE *30 DAYS* AFTER YOU SIGN THESE FORMS TO COMPLETE THE APPLICATION PROCESS AND RETRIEVE YOUR CERTIFICATE.**

STEP 1: Online Application

Begin the application process online at http://www.identrust.com/certificates/eca/buy_eca.html. By completing the online application process and by signing the In-Person Identification Form you agree to the terms of the ECA Certificate Subscriber Agreement and IdenTrust's ECA Certificate Practices Statement (CPS), located here: http://www.identrust.com/certificates/eca/eca_downloads.html. You also agree to the terms of the current ECA Certificate Policy (CP) located at: http://iase.disa.mil/pki/eca/documents.html.

STEP 2: Subscribing Organization Authorization Form

Complete **Part I - Subscribing Organization Authorization Form**. Take Part I - Subscribing Organization Authorization Form to an officer in your Organization who can sign on behalf of your Organization and bind your Organization to the terms and conditions of the document. Have the officer sign Part I - Subscribing Organization Authorization Form and return it to you for submission to IdenTrust. In the event Subscribing Organization does not have an "officer", this form should then be signed by an authorized representative of the Subscribing Organization with sufficient authority to bind the Subscribing Organization to the terms hereof.

STEP 3: In-person Identification Form

Complete and Sign **Part II - In-person Identification Form**. You must present **two** forms of identification to a Notary, Consular Officer or Trusted Correspondent, according to the following instructions:

Option 1: One from List A **and** one from either List B or C

Option 2: One from List B **and** one from List C

Non-US Citizens: Valid passport **and** one from List B.)

***If you have more than one citizenship asserted in your certificate, you must provide proof of citizenship (i.e. passport) for each.

LIST A - Photo ID Documents that Establish Identity and Citizenship	LIST B – Photo ID Documents that Establish Identity	LIST C – Other Documents that Establish U.S. Citizenship but not Identity
1. Passport from Country of Citizenship 2. Certificate of U.S. Citizenship issued by U.S. Citizenship and Immigration Service -USCIS (formerly INS) 3. Certificate of Naturalization issued by a court of competent jurisdiction prior to October 1, 1991, or the USCIS (INS), since that date	1. Driver's license or government-issued ID card (containing a photograph) 2. Military ID (with photograph) 3. Permanent or Unexpired Temporary Resident Card issued by the USCIS (with photograph) 4. Other Official Photo ID	1. Original or certified copy of a birth certificate issued by a state, county, municipal authority, or outlying possession of the United States bearing an official seal 2. Consular Report of Birth from a U.S. Consulate (Form FS-240) 3. Certification of Birth Abroad issued by the Department of State (Form DS-1350)

STEP 4: Send Forms to IdenTrust

Record the name and place where you had the form notarized. For your records, make a copy of your Part 1 and Part 2 forms, then send the signed (ink-on-paper) originals to IdenTrust.

Mailing Address:
DOD / ECA Registration
IdenTrust Services
255 North Admiral Byrd Road
Suite 200
Salt Lake City, UT, 84116-4915

If you should have any questions during the process and would like to speak with a customer service representative, please call (888) 882-1104 or by email at helpdesk@identrust.com

Part 2: In-Person Identification Form

The undersigned applicant attests that all facts and information provided are accurate, current, complete, and not misleading and that he or she: a) is authorized to receive, and has applied for, a digital Certificate to be issued by IdenTrust; b) has read and verified the personal identifying information to be contained in the Certificate; c) is who he or she represents himself or herself to be; and d) has read, understood, and agrees to the responsibilities associated with being a Certificate Subscriber, including the terms and conditions found in the IdenTrust Services ECA SSL PKI Sponsor agreement, the public version of IdenTrust's ECA Certification Practices Statement ("CPS"), and the ECA Certificate Policy ("the ECA CP"). The applicant agrees to: 1) accurately represent him or herself in all communications; 2) protect component private key(s) at all times; 3) immediately notify IdenTrust if he or she suspects component private key(s) to have been compromised, stolen or lost; and 4) use component private keys in accordance with the above-mentioned documents.

THIS SECTION TO BE USED BY THE APPLICANT

Signed By: _____ Date: _____

(Sign Only In The Presence of the Notary/Consular Officer)

Printed Name: _____ E-mail Address: _____

You must present **two** forms of identification to a Notary, Consular Officer or Trusted Correspondent, according to the following instructions:

- **Option 1:** One from List A **and** one from either List B or C
- **Option 2:** One from List B **and** one from List C
- **Non-US Citizens:** Valid passport **and** one from List B.)

LIST A - Photo ID Document for Identity & Citizenship (Non-expired Passport / Naturalization)	**LIST B – Gov't-issued Photo ID Card (Driver's Lic., Military ID or Res. Alien)**	**LIST C – Certified Birth Certificate (U.S. Citizens Only)**
Doc. Type / Title: _____	**Doc. Type/ Title:** _____	**Doc. Type/ Title:** _____
Issuer: _____	**Issuer:** _____	**Issuer:** _____
Serial No.: _____	**Serial No.:** _____	**Serial No.:** _____
Exact Name: _____	**Exact Name:** _____	**Exact Name:** _____
		Issue Date: _____
Issue Date: _____	**Issue Date:** _____	***See Note below**
Expir. Date: _____	**Expir. Date:** _____	

***Note**: If the name on your Birth Certificate is different from the name on your Driver's License or other form of ID, please send a **notarized** copy of a document showing the name change (Eg. A **notarized** copy of a marriage license or **notarized** certificate of marriage).

NOTARIAL ACKNOWLEDGEMENT

I _____ (name of Notary/Officer), registered in the state of _____, county of _____ do hereby certify under PENALTY OF PERJURY under the laws of the State of _____ that the following information is true and correct:

1. On _____ before me, _____ (name and title of the notary/officer)
(date)

personally appeared _____ (name of signer), who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by his/her signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.

2. I have seen and verified the forms of identification for which information is written above and hereby assert that said forms of ID do not appear to be altered, forged or modified in any way.

WITNESS my hand and official seal.

Signature _____ (Seal)

15.7 Part 1: Subscribing Organization Authorization Agreement

Subscribing Organization ("Organization"), identified below, acknowledges that IdenTrust Services, LLC ("IdenTrust") (www.IdenTrust.com), an External Certification Authority ("ECA") for the Department of Defense, will issue Digital Certificates ("Certificates") to employees of Organization. The Certificate will identify the Applicant or Subscriber, identified below, or Applicants/Subscribers identified in a Bulk Load Template, as being employed by Organization.

Capitalized terms used herein shall have the meaning given to them in the public version of IdenTrust's DOD ECA Certification Practices Statement (https://secure.identrust.com/certificates/policy/eca) ("the CPS") and the ECA Certificate Policy (http://iase.disa.mil/pki/eca/Documents) ("the CP"). The public version of the CPS, the CP, the Terms and Conditions attached as Part II hereof and the In-Person Identification Form (https://secure.identrust.com/certificates/policy/eca) ("ID Form"), are incorporated by reference herein and comprise this Agreement, as that term is used herein. IdenTrust reserves, and Organization acknowledges and accepts, IdenTrust's right to modify the CPS, which modifications shall become a part of this Agreement.

Organization and IdenTrust acknowledge that:

(a) IdenTrust or Organization, in its sole discretion, may revoke the Certificate issued hereunder at any time and for any reason;

(b) IdenTrust will revoke the Certificate promptly upon confirming that the person making the revocation request is authorized to do so or upon otherwise determining that the Certificate should be revoked; and

(c) With respect to US Government Subscribers or US Government Relying Parties, this Agreement and its attached Terms and Conditions shall be governed by the Contracts Disputes Act of 1978, as amended (41 US.C. § 601 et seq.). In all other cases, irrespective of the place of performance, this Agreement and its attached Terms and Conditions shall be construed, interpreted, and enforced in accordance with the substantive laws of the State of Utah, without regard to its conflicts of law rules.

Organization warrants and represents that:

(a) Organization agrees to be bound by the Terms and Conditions set forth in Appendix A to this Part 1;

(b) It is duly-organized and validly-existing under the laws of its jurisdiction of organization and has full right and authority to use the Organization's name, given below, to grant this authorization, and to perform all obligations required of it hereunder;

(c) Subscriber is a duly-authorized employee of the Organization and IdenTrust is hereby authorized to issue a Certificate to Subscriber that identifies Subscriber as being employed by Organization;

(d) Federal agencies, and other authorized recipients of messages signed with Subscriber's Private Key, may rely on such messages to the same extent as though they were manually signed by the Subscriber listed in a valid, unrevoked and unexpired Certificate issued by IdenTrust; and

(e) All information provided to IdenTrust by Organization is and will be accurate, current, complete, and not misleading and Organization will immediately notify IdenTrust and request that the Certificate be revoked if: (1) any information or fact material to the reliability of the Certificate is no longer accurate, current, complete or becomes misleading, (2) Organization suspects any loss, disclosure, or other compromise of the Subscriber's Private Key, or (3) Subscriber is no longer employed by, associated with, authorized by or affiliated with Organization.

The undersigned personally warrants and represents that he or she is an officer of the Organization and has authority to make the representations and warranties in this Agreement on behalf of the Organization and to bind the Organization to the Terms and Conditions attached hereto by his or her signature.

_____	By: _____ Date: _____
Print Applicant/ Subscriber's Name	Organization Officer Signs Here
_____	_____
Print Subscribing Organization's Name	Print Organization Officer's Name Here
_____	Title: _____
Organizational Headquarters' Full Address	Print Officer's Title Here

Appendix to Part 1
Terms and Conditions

1. Certification Services from IdenTrust

a. Issuance and Revocation of Certificates. On request by the Subscribing Organization and one or more individual Subscribers employed by the Subscribing Organization, IdenTrust agrees to issue ECA Certificates as specified in the ECA CPS. IdenTrust also agrees to revoke an ECA Certificate that it has issued on receipt of a request by either the Subscribing Organization or the Subscriber listed in that Certificate. With respect to the issuance and revocation of ECA Certificates, IdenTrust and the Subscribing Organization agree to perform as required of each in the ECA CP and the public version of IdenTrust's ECA CPS. Moreover, IdenTrust in providing ECA public key Certificate issuance and revocation services, and the Subscribing Organization in accepting them, is subject to the ongoing oversight of the EPMA as provided in the ECA CP.

b. Individual Subscriber Agreements. In connection with registration of each Subscriber employed by the Subscribing Organization, Subscriber enters into a separate agreement, which is legally binding on each Individual Subscriber. The current form of Subscriber Agreement and IdenTrust's public version of the CPS are publicly available on IdenTrust's web site.

c. IdenTrust Verification of Identity. Section 4 of the Subscriber Agreement is hereby incorporated by reference.

2. Obligations of the Subscribing Organization

a. Supervision of Subscribers. Organization agrees that it will require each of its Subscribers to carefully and fully comply with each of the provisions of the Subscriber Agreement.

b. Duties. Subscribers and Subscribing Organizations are each required under the terms of the CP and the public version of the CPS to do the following, among other things:

(1) Accurately represent themselves in all communications relevant to the ECA system.

(2) Protect their private keys at all times as specified in the ECA CP and as required by IdenTrust's instructions given at the time of Certificate acceptance or otherwise.

(3) Notify IdenTrust in a timely manner of any grounds for revocation of a Certificate issued by IdenTrust to a Subscriber employed by the Organization. Such grounds include termination of the employee or if ever a private key held by the Subscriber is suspected to have been compromised or lost. Such notification will be made through the means specified in the public version of the CPS.

(4) Notify IdenTrust whenever any information in a Certificate ceases to be accurate or should be changed.

3. Fees. Fees for Certificate issuance are published on the IdenTrust website. There is no fee for Certificate revocation. When a Subscriber applies for a Certificate, the initial fee is charged with respect to its initial term, and renewal fees are charged upon renewal. If Certificates are to be issued via a Bulk Load procedure, an aggregate fee will be charged to the Subscribing Organization.

4. Use of Information.

a. Confidential Information and Disclosure. IdenTrust obtains certain sensitive information from Subscribers in providing public key Certificate issuance and revocation services. That information includes contact information, billing and payment details, and sometimes information gained in the course of providing consulting, implementation, sales or other support services to the Subscribing Organization. This agreement restricts IdenTrust's use of that information solely to the purposes for which it was collected, and prohibits its disclosure to third parties, except as may be required by law. Access to sensitive Subscriber-related information within IdenTrust is limited to IdenTrust employees acting in Trusted Roles, other trusted employees within IdenTrust, and IdenTrust's and the EPMA's auditors on a need-to-know basis. Access to that information in IdenTrust customer databases is limited accordingly using the structure and access limits of those databases. However, information contained in ECA Certificates and related status information <u>are not confidential</u>. (That would defeat the purpose of an ECA Certificate, which is to establish a person's identity.) Accordingly, IdenTrust may disclose the Subscriber's name, public key, email address, citizenship, Organization name, Certificate serial number, and Certificate expiration date to any person and for any purpose. Information listed in the Repository provided by IdenTrust is also not confidential.

b. Disclosure of Certificate Revocation/Suspension Information. IdenTrust discloses information concerning the revocation of a Certificate or events leading to such a revocation only to the Subscriber and/or Subscribing Organization of that Certificate, and only on request. However, the information disclosed in a CRL or OCSP

response, such as the fact that a Certificate is revoked and date of revocation, is not confidential. IdenTrust discloses that information on request or, preferably, through online retrieval.

5. **Incorporation by Reference.** Sections 6 through 11 of the Subscriber Agreement are hereby incorporated by reference as though fully set forth herein

15.8 Part 1: SSL Subscribing Organization Authorization Agreement

Subscribing Organization ("Organization"), identified below, acknowledges that IdenTrust Services, LLC ("IdenTrust") (www. IdenTrust.com), an External Certification Authority ("ECA") for the Department of Defense, will issue Digital Certificates ("Certificates") to components owned by the Organization and requested by authorized PKI sponsors (“Applicant”). The Certificate will identify the component, identified herein, (), as being owned by Organization.

Capitalized terms used herein shall have the meaning given to them in the public version of IdenTrust's DOD ECA Certification Practices Statement (http://www.identrust.com/certificates/policy/eca) ("the CPS") and the ECA Certificate Policy (http://iase.disa.mil/pki/eca/Documents) ("the CP"). The public version of the CPS, the CP, the Terms and Conditions attached as Appendix A hereof and the Part 2: In-Person Identification Form (https://secure.identrust.com/certificates/policy/eca) ("ID Form"), are incorporated by reference herein and comprise this Agreement, as that term is used herein. IdenTrust reserves, and Organization acknowledges and accepts, IdenTrust's right to modify the CPS, which modifications shall become a part of this Agreement.

1. IdenTrust and Organization agree that:

(a) IdenTrust or Organization, in its sole discretion, may revoke the Certificate issued hereunder at any time and for any reason;

(b) IdenTrust will revoke the Certificate promptly upon confirming that the person making the revocation request is authorized to do so or upon otherwise determining that the Certificate should be revoked; and

(c) With respect to US Government Subscribers or US Government Relying Parties, this Agreement and its attached Terms and Conditions shall be governed by the Contracts Disputes Act of 1978, as amended (41 US.C. § 601 et seq.). With respect to State governments, this Agreement and its attached Terms and Conditions shall be construed, interpreted, and enforced in accordance with the substantive laws of that State, without regard to its conflicts of law rules. In all other cases, irrespective of the place of performance, this Agreement and its attached Terms and Conditions shall be construed, interpreted, and enforced in accordance with the substantive laws of the State of Utah, without regard to its conflicts of law rules.

2. Organization warrants, represents and agrees that:

(a) Organization agrees to be bound by the Terms and Conditions set forth in Appendix A to this Part 1;

(b) It is duly-organized and validly-existing under the laws of its jurisdiction of organization and has full right and authority to use the Organization's name, given below, to grant this authorization, and to perform all obligations required of it hereunder;

(c) PKI Sponsor is a duly-authorized employee of the Organization and IdenTrust is hereby authorized to issue a Certificate requested by PKI Sponsor for a component owned by Organization;

(d) Federal agencies, and other authorized recipients of messages signed with Component's Private Key, may rely on such messages to the same extent as though they were sent by component listed in a valid, unrevoked and unexpired Certificate issued by IdenTrust; and

(e) All information provided to IdenTrust by Organization is and will be accurate, current, complete, and not misleading and Organization will immediately notify IdenTrust and request that the Certificate be revoked if: (1) any information or fact material to the reliability of the Certificate is no longer accurate, current, complete or becomes misleading, (2) Organization suspects any loss, disclosure, or other compromise of the Component's Private Key, or (3) Component is no longer owned by, associated with, or affiliated with Organization.

The undersigned personally warrants and represents that he or she is an officer of the Organization and has authority to make the representations and warranties in this Agreement on behalf of the Organization and to bind the Organization to the Terms and Conditions attached hereto by his or her signature.

_____	_____
Print Component Identifier (i.e Fully Qualified Domain Name)	Print PKI Sponsor Name
_____	_____
Print Subscribing Organization’s Name	Organizational Headquarters’ Full Address
_____	_____
Print Organization Officer’s name	Print Organization Officer’s Title
_____	_____
Organizational Officer’s E-mail Address	Organization’s Officer’s Telephone Number
_____	_____
Organization Officer’s Signature	Date

15.9 Trusted Correspondent Addendum to Subscribing Organization Authorization Agreement

Trusted Correspondent Addendum to Subscribing Organization Authorization Agreement

Subscribing Organization hereby recommends that the Candidate identified below ("Candidate") be appointed to the role of Trusted Correspondent in the Department of Defense External Certification Authority program conducted by IdenTrust Services, LLC. ("IdenTrust") and, by signing where indicated below, Candidate pledges to fulfill the responsibilities of that role, as summarized below. If approved by IdenTrust, Candidate will assist IdenTrust in performing such identity verification tasks as may be required by the terms of the Certificate Policy for External Certification Authorities ("CP") published by the United States Department of Defense ("DOD") and the public version of IdenTrust's ECA Certification Practices Statement ("CPS"). (These policies are available for review at https://secure.identrust.com/certificates/policy/eca. From time to time, the DOD ECA Policy Management Authority may amend the CP and the IdenTrust Policy Management Authority may amend the CPS. Any such amendments and any required notices will be pursuant to the terms of those documents and shall be binding upon Subscribing Organization and Candidate unless and until Candidate resigns or Subscribing Organization or IdenTrust terminates the status of Candidate as a Trusted Correspondent.

Candidate confirms that he or she has read the relevant provisions of the CP and the public version of the CPS required by IdenTrust and understands, and will fully and faithfully discharge, his or her obligations as described in those documents and summarized below.

As a Trusted Correspondent of IdenTrust under the ECA Program, I, Candidate, will be performing a key role in the identification and authentication of Applicants for ECAcCertificates. In the capacity as a Trusted Correspondent of IdenTrust, I agree to do the following:

1. Conform to the CP and the public version of the CPS in providing services as a Trusted Correspondent and Registrar under the IdenTrust ECA Program. (A Trusted Correspondent is one of the several kinds of Registrars defined in the CPS.)
2. Follow IdenTrust's instructions relative to the services I perform for IdenTrust.
3. Inform myself of my responsibilities as a Trusted Correspondent by reading and following all written instructions and any training materials provided by IdenTrust.
4. Ensure that each Applicant receives a copy of the Instructions for Applicant. This provides information about the In-Person Identification Form and gives the Applicant the responsibility to review and accept the Subscriber Agreement and policies.
5. Ensure that each Applicant completes all required fields on the In-Person Identification Form, presents the required identification credentials to me for inspection, and signs the form in my presence.
6. Sign each In-Person Identification Form as its Registrar, with a declaration attesting that I reviewed the Applicant's identification credentials, confirmed that the Applicant is the holder of the identification credentials and that the picture and name on the Photo ID match the appearance and name of the Applicant.
7. When performing Bulk Load registrations, complete and forward to IdenTrust a Bulk Load template and, for each Subscriber a completed In-Person Identification Form, attested by me.
8. Supply the appropriate Human Resource Department(s) in the Subscribing Organization with the provided Instruction Form to ensure that IdenTrust is notified in the event of certificate revocation events, such as separation of a Subscriber from the Subscribing Organization.
9. Immediately notify IdenTrust in the event that a Subscriber or Subscribing Organization requests the revocation of any ECA Certificate or whenever I believe that circumstances requiring revocation of any Certificate may exist.

10. Immediately notify IdenTrust in the event that I suspect or have reason to believe a Subscriber's Private Key corresponding to an ECA Certificate has been or may be compromised.
11. Receive from Subscribers and authorized representatives of Subscribing Organization certificate revocation requests, authenticate them, and immediately forward them to IdenTrust for processing.
12. If applicable, receive from Subscribers and authorized representatives of Subscribing Organization cryptographic modules or tokens containing an ECA certificates to be revoked, erase or destroy such modules or tokens pursuant to procedures required by IdenTrust, and request revocation of the Certificates they contain.
13. In the case of a cryptographic module or token containing an ECA certificate that is not returned by a Subscriber, request revocation of such Certificate with a reason code of key compromise.
14. Provide support to Subscribers within Subscribing Organization under procedures established by IdenTrust.
15. Contact IdenTrust at ecaservices.@identrust.com or 1-888-882-1104 (U.S.) or 1-801-924-8141 (International) with any questions I may have.

With respect to US Government Subscribers, Trusted Correspondents or Relying Parties, this Addendum shall be governed by, and interpreted and construed under, the Contracts Disputes Act of 1978, as amended (41 US.C. § 601 et seq.). In all other cases, irrespective of the place of performance, this Trusted Correspondent Addendum shall be construed, interpreted, and enforced in accordance with the substantive laws of the State of Utah, without regard to its conflicts of law principles.

Trusted Correspondent Candidate Signature: _____

Print Name: _____

Date: _____

Telephone Number: (_____)_____

E-Mail Address: _____

Agreement by Subscribing Organization

1. Subscribing Organization hereby confirms that Candidate named above is an employee of Subscribing Organization and appoints and authorizes Candidate to fulfill all the responsibilities of a Trusted Correspondent on behalf of Subscribing Organization, as prescribed above and in the CP and public version of the IdenTrust ECA CPS.
2. Subscribing Organization warrants that, in the event it ever concludes that Candidate has breached any term of this Agreement, or any applicable requirement of the CP or the public version of the CPS, Subscribing Organization will immediately revoke Candidate's authorization to act as a Trusted Correspondent.
3. Subscribing Organization undertakes to supervise Candidate in connection with his or her responsibilities in the role of Trusted Correspondent and ensure that there will be no conflict between Candidate's duties as an employee of Subscribing Organization and duties as a Trusted Correspondent. Subscribing Organization agrees that, if requested by IdenTrust at any time, it will immediately revoke the authorization of Candidate to act as a Trusted Correspondent, and promptly appoint a new individual to serve as a Trusted Correspondent.
4. Subscribing Organization agrees to notify IdenTrust in the event that a Trusted Correspondent is no longer authorized to act as a Trusted Correspondent.
5. In the event that IdenTrust may determine, in its reasonable sole discretion, that the Candidate has breached any of the applicable terms of his or her agreement above, the CP, or the public version of the CPS, or that Subscribing Organization has breached any of the applicable terms of this Agreement or the

CP or the public version of the CPS, then IdenTrust may revoke or suspend any or all of the ECA Certificates registered by Candidate or issued to Subscribing Organization.

6. In consideration of IdenTrust's appointment, Subscribing Organization hereby agrees to indemnify and hold IdenTrust, its parent company, and the officers, directors, employees and agents of either of them harmless from and against any loss, cost, damage, liability or expense any of the foregoing may incur or be liable for, including reasonable attorneys' fees and expenses, arising out of this appointment; any act or omission of Candidate in the capacity as a Trusted Correspondent; or any act or omission of Subscribing Organization in connection with the ECA Program or any ECA Certificate issued as a result of Trusted Correspondent's actions. If Subscribing Organization is the U.S. Government, this provision may not apply.

Organization Officer Sign Here: _____

Print Name: _____

Telephone Number: (_____)_____

E-Mail Address: _____

Appointment by IdenTrust

The above nomination by the Subscribing Organization of the individual named above to serve as a Trusted Correspondent in the IdenTrust ECA program must be accepted in writing by IdenTrust within thirty (30) days after the later of the date of signature by the individual or the Subscribing Organization shown above, or such nomination shall be deemed rejected, and the Subscribing Organization must nominate another individual to the role, or may renominate the original individual, *provided* that any circumstance which prevented IdenTrust from accepting the original nomination shall have been remedied to the satisfaction of IdenTrust.

IdenTrust Services, LLC

By: _____

Name: _____

Date: _____

15.10 PKI Point of Contact (POC) Addendum to Subscribing Organization Authorization Agreement

PKI Point of Contact Addendum to Subscribing Organization Authorization Agreement

Subscribing Organization hereby recommends that the Candidate identified below ("Candidate") be appointed to the role of PKI Point of Contact (PKI POC) in the Department of Defense External Certification Authority program conducted by IdenTrust Services, LLC. ("IdenTrust") and, by signing where indicated below, Candidate pledges to fulfill the responsibilities of that role, as summarized below. If approved by IdenTrust, Candidate will assist IdenTrust in performing such revocation tasks as may be required by the terms of the Certificate Policy for External Certification Authorities ("CP") published by the United States Department of Defense ("DoD") and the public version of IdenTrust's ECA Certification Practices Statement ("CPS"). (These policies are available for review at https://secure.identrust.com/certificates/policy/eca. From time to time, the DoD ECA Policy Management Authority may amend the CP and the IdenTrust Policy Management Authority may amend the CPS. Any such amendments and any required notices will be pursuant to the terms of those documents and shall be binding upon Subscribing Organization and Candidate unless and until Candidate resigns or Subscribing Organization or IdenTrust terminates the status of PKI POC.

Candidate confirms that he or she has read the relevant provisions of the CP and the public version of the CPS required by IdenTrust and understands, and will fully and faithfully discharge, his or her obligations as described in those documents and summarized below.

As a PKI POC of IdenTrust under the ECA Program, I, Candidate, will be performing a key role in the revocation of ECA Certificates. In the capacity as a PKI POC of IdenTrust, I agree to do the following:

1. Conform to the CP and the public version of the CPS in providing services as a PKI POC under the IdenTrust ECA Program.
2. Follow IdenTrust's instructions relative to the services I perform for IdenTrust.
3. Inform myself of my responsibilities as a PKI POC by reading and following all written instructions and any training materials provided by IdenTrust.
4. Immediately notify IdenTrust in the event that a Subscriber or Subscribing Organization requests the revocation of any ECA Certificate or whenever I believe that circumstances requiring revocation of any Certificate may exist.
5. Immediately notify IdenTrust in the event that I suspect or have reason to believe a Subscriber's Private Key corresponding to an ECA Certificate has been or may be compromised.
6. Receive from Subscribers and authorized representatives of Subscribing Organization Certificate revocation requests, authenticate them, and immediately forward them to IdenTrust for processing.
7. If applicable, receive from Subscribers and authorized representatives of Subscribing Organization Cryptographic Modules or tokens containing ECA Certificates to be revoked, erase or destroy such modules or tokens pursuant to procedures required by IdenTrust, and request revocation of the Certificates they contain.
8. In the case of a Cryptographic Module or token containing an ECA Certificate that is not returned by a Subscriber, request revocation of such Certificate with a reason code of key compromise.
9. Contact IdenTrust at helpdesk@identrust.com or 1-888-882-1104 (U.S.) or 1-801-924-8141 (International) with any questions I may have.

With respect to US Government Subscribers, PKI POCs or Relying Parties, this Addendum shall be governed by, and interpreted and construed under, the Contracts Disputes Act of 1978, as amended (41 US.C. § 601 et seq.). In all other cases, irrespective of the place of performance, this PKI Point of Contact Addendum shall be construed, interpreted, and enforced in accordance with the substantive laws of the State of Utah, without regard to its conflicts of law principles.

PKI POC Candidate Signature: _____

Print Name: _____

Date: _____

Telephone Number: (_____)_____

E-Mail Address: _____

Agreement by Subscribing Organization

1. Subscribing Organization hereby confirms that Candidate named above is an employee of Subscribing Organization and appoints and authorizes Candidate to fulfill all the responsibilities of a PKI POC on behalf of Subscribing Organization, as prescribed above and in the CP and public version of the IdenTrust ECA CPS. 2. Subscribing Organization warrants that, in the event it ever concludes that Candidate has breached any term of this Agreement, or any applicable requirement of the CP or the public version of the CPS, Subscribing Organization will immediately revoke Candidate's authorization to act as a PKI POC. 3. Subscribing Organization undertakes to supervise Candidate in connection with his or her responsibilities in the role of PKI POC and ensure that there will be no conflict between Candidate's duties as an employee of Subscribing Organization and duties as a PKI POC. Subscribing Organization agrees that, if requested by IdenTrust at any time, it will immediately revoke the authorization of Candidate to act as a PKI POC, and promptly appoint a new individual to serve as a PKI POC.4. Subscribing Organization agrees to notify IdenTrust in the event that a PKI POC is no longer authorized to act as a PKI POC.5. In consideration of IdenTrust's appointment, Subscribing Organization hereby agrees to indemnify and hold IdenTrust, its parent company, and the officers, directors, employees and agents of either of them harmless from and against any loss, cost, damage, liability or expense any of the foregoing may incur or be liable for, including reasonable attorneys' fees and expenses, arising out of this appointment; any act or omission of Candidate in the capacity as a PKI POC; or any act or omission of Subscribing Organization in connection with the ECA Program or any ECA Certificate issued as a result of PKI POC 's actions. If Subscribing Organization is the U.S. Government, this provision may not apply.

Organization Officer Sign Here: _____

Print Name: _____

Telephone Number: (_____)_____

E-Mail Address: _____

Appointment by IdenTrust

The above nomination by the Subscribing Organization of the individual named above to serve as a PKI POC in the IdenTrust ECA program must be accepted in writing by IdenTrust within thirty (30) days after the later of the date of signature by the individual or the Subscribing Organization shown above, or such nomination shall be deemed rejected, and the Subscribing Organization must nominate another individual to the role, or may renominate the original individual, *provided* that any circumstance which prevented IdenTrust from accepting the original nomination shall have been remedied to the satisfaction of IdenTrust.

IdenTrust Services, LLC

By: _____

Name: _____

Date: _____