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

Version 2.4

April 24, 2023

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 the 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 offsite 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.
2.2	November 18, 2020	Bring CPS current with the ECA CP v4.5 dated 20 February 2019. Also, to incorporate changes requested by the ECA Policy Review team. Incorporated updates to support issuance via RA request submission through CMS implementation and through the use of IdenTrust secure online Certificate Lifecycle Management Tool. Refresh entire document to convey policy and practices currently deployed. Cosmetic changes automatically accepted: • Standardizing all references to the Certificate Lifecycle Management Tool and added the term to the Glossary; • Standardizing all references to the Secure IdenTrust Registration Website and added the term to the Glossary; • Standardizing all references to the Secure IdenTrust Retrieval Website and added the term to the Glossary; • Updated all links to correct section numbers; and • Renamed Trusted Correspondents to Trusted Agents.

Revision	Date	Summary of Changes/Comments
2.3	April 14, 2021	Updates to include the new data center onsite and remote monitoring and surveillance procedures, to remain compliant with security measures: • Section 5.1.1.1.1 Primary Facility – updated grammatical error and updated language pertaining to facility monitoring; • Section 5.1.1.1.2 Disaster Recovery Facility – updated grammatical errors; • Section 5.1.2.1.1 Primary Facility – Updated language pertaining to facility monitoring; • Section 5.1.2.1.2 Disaster Recovery Facility – updated grammatical error; • Section 5.1.2.2 Physical Access to RA Operations room – updated grammatical error; • Section 5.1.5.1 Primary Facility – updated spelling error, also updated bullet point four to read "Monitored on a 24.7 basis by operators with fire control console/panel access"; and • Section 5.1.5.2 Disaster Recovery Facility – updated language to bullet point one to read "Monitored on a 24x7 basis by operators with fire control console/panel access".
2.4	April 24, 2023	• Updated references to sections using hyperlinks throughout the document and fixed broken links. • Section 5.1.6.1 and 5.5.2: Removed CD-ROM/DVD-ROM references as Media Storage. • Added Software Engineer and Development Operations roles to Section 5.2.1.3: Other Trusted Roles • Updated sections 5.2.3 and 5.3.3 Roles Requiring Separation of Duties / Training Requirements including the new added roles mentioned above. • Updates on these Sections based on the ECA CP v.4.6 dated March 9, 2022: o 1.2: Added sha-384 OIDs; o 1.3.7.6: Other Authorities -Cleared No stipulation; o 3.2.3.4/3.2.3.3: Aligned numbering with ECA CP; o 5.2.1.3/5.2.1.4: Aligned numbering with ECA CP; o 5.2.3/5.2.4: Aligned numbering with ECA CP; o 6.1.5: Key Sizes: Added sha-384 algorithms OIDs; o 6.1.7/6.1.8: Aligned numbering with ECA CP; o 7.1.3: Added sha-384 algorithms OIDs; o 9.6.5: Added missing section; o 10.1: Added missing section; o 10.2: Added missing section; o 10.3: Added missing section; o 10.4: Added missing section; and o 10.5.1 thru 10.6.4: Aligned numbering with the ECA CP.

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 4.6 dated March 9, 2022, (the ECA CP) as published by the US Department of Defense (DoD) and downloadable from:

https://public.cyber.mil/unclass-eca_cp_v4-6_final_signed/

The outline and content of this CPS are in accordance with the *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 *Glossary* Section. Also, forms of the verb "confirm" and the noun "confirmation" have the meanings given to the word "confirm" in the *Glossary* Section, even when not capitalized.

1.1 OVERVIEW

1.1.1 Certification Practices Statement (CPS)

This CPS has the following purposes:

Compliance checking: It documents how IdenTrust satisfies the requirements of ECA CP and sets the standard for IdenTrust's internal procedures and their documentation, as well as requirements for documentation of procedures performed by External RA Organizations;

System specifications for contractual purposes: The public version of the CPS specifies for IdenTrust customers (Subscribers under contract with IdenTrust) 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:

- **Registration**

  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 an Applicant, 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 Applicant and authentication of component identity.

NOTE: Once an Applicant has retrieved a Certificate, he or she is then referred to as a Subscriber.

- **Issuance of a Certificate**

  The process of creating a Certificate and sending it to the Applicant for acceptance and installation into his or her system.

- **Publication of a Certificate**

  The process of placing a Certificate online to be available to users via a Repository that can be accessed through a standard communications protocol (e.g., Lightweight Directory Attribute Protocol (LDAP), or Secure LDAP (LDAPS).

- **revocation of a Certificate**

  The process of invalidating a Certificate 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. Approval for issuance of a Certificate may be performed by External RA Organizations who have signed an IdenTrust RA Agreement. IdenTrust also performs revocation of a Certificate and makes the latest revocation information available through publication of CRL and through an OCSP Responder

1.1.2 Registration Practices Statement (RPS)

All External RAs operating under agreement with IdenTrust must produce a Registration Practices (RPS) which aligns with this CPS document and the ECA CP.

Essentially, the RPS document is a subset of this CPS and is used to record the practices that an External RA Organization will employ to ensure compliance with the ECA CP and this CPS.

The RPS is created through collaboration between employees of the External RA Organization who are involved in the PKI operation and designated subject matter experts who are involved in the IdenTrust CA operation. An RPS template is used to ensure that all required sections of the CPS pertaining to RA functions are addressed by the External RA. Sections of the CPS that are not relevant to RA operations may be omitted from the RPS document. Sections that may be omitted are identified in the RPS template to ensure that improper omissions are not made.

The primary purpose of the RPS document is to document the requirements under which the External RA must operate to ensure compliance with the ECA CP, this CPS and to establish controls against which the External RA will be audited.

The RPS document must comply with the following requirements:

- Must align with the ECA CP and this CPS;
- Practices detailed in the RPS may not supersede any requirements of the ECA CP or this CPS;
- Must be approved by the IdenTrust Policy Management Authority (PMA) prior to being granted approval to operate as an External RA; and
- Must be kept current with new releases of the ECA CP and/or this CPS as requested by IdenTrust on a quarterly basis.

Subject Matter Experts (SMEs) representing various segments of the IdenTrust CA operation will review the RPS to ensure that proposed controls are compliant with the ECA CP and this CPS. A thorough review is also conducted by a member of the IdenTrust Policy team prior to the formal RPS review that is conducted by the IdenTrust PMA.

If ever an External RA Organization were to petition the IdenTrust PMA to include language in its RPS document that is not compliant with a requirement stated in the ECA CP or this CPS, the IdenTrust PMA must refer the

request to the DoD PMA for review. Under no circumstance is the IdenTrust PMA allowed to approve an RPS document that is knowingly out of compliance with the ECA CP or this CPS.

All External RA Organizations are required to perform an annual audit against the IdenTrust PMA approved RPS document and must provide evidence of the annual audit to IdenTrust for review and comment per the *Frequency and Circumstances of Assessment* Section.

1.2 DOCUMENT NAME AND 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 - *Document Name and Identification,* are included in this list and OIDs indicate that this CPS and the ECA CP apply in relation to the Certificate. 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-sha256	ID::= {id-eca-policies 4}
id-eca-medium-token-sha256	ID::= {id-eca-policies 5}
id-eca-medium-device sha256	ID::= {id-eca-policies 9}
id-eca-medium-hardware-sha256	ID::= {id-eca-policies 10}
id-eca-medium-sha384	ID::= {id-eca-policies 11}
id-eca-medium-token-sha384	ID::= {id-eca-policies 12}
id-eca-medium-device-sha384	ID::= {id-eca-policies 13}
d-eca-medium-hardware-sha384	ID::= {id-eca-policies 14}
id-eca-medium-device-hardware-sha384	ID::= {id-eca-policies 15}

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)}.

The requirements stipulated in this CPS apply to all assurance levels unless otherwise noted. Requirements for Medium SHA-256, Medium SHA-384, Medium Token SHA-256, Medium Token SHA-384, Medium Hardware SHA-256 and Medium Hardware SHA-384 are identical to Medium, Medium Token, and Medium Hardware respectively, except for the key size and hash algorithm used in generating Certificate, CRL, and OCSP response signatures. Requirements for Medium Device SHA-256 and Medium Device SHA-384 are identical to Medium except for the hash algorithm and activation data. Requirements for Medium Device Hardware OIDs are identical to Medium Device except that for private key generation and storage.

End-Entity certificates issued to devices always assert the Medium Device policy. All other policies defined in this document are reserved for human Subscribers when used in End-Entity certificates.

1.3 PKI PARTICIPANTS

1.3.1 ECA Policy Management Authority

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.

1.3.2 Certification Authorities

A Certification Authority is defined in the ECA CP Section 15 -*Glossary* as "An authority trusted by one or more users to create and assign Certificates".[1] Further, the same section explains a Certification Authority as:

> *An entity authorized by the EPMA to create, sign, and issue public key certificates. A CA 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. A CA may also perform key escrow and support key recovery functions for the PKI. CA is an inclusive term and includes all types of CAs. CA, as used in this document, includes component parts which may be on the same hardware/software system or an integrated set of hardware and software within the control of a designated security boundary. Examples of components would be CA web servers/portals, databases, Key Escrow Systems (KES) and internal directories.*

As an ECA, IdenTrust performs its services in accordance with those requirements in the *CA Representations and Warranties* Section.

As an ECA, IdenTrust issues Certificates only to Subscribers who are end entities. 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 IdenTrust ECA Certificate profiles document and the *Certificate and CRL Formats* Section. The keyCertSign and cRLSign bits are never set in 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 the *Certificate Revocation and Suspension* Section.

A CA may also perform key escrow and support key recovery functions for the PKI. CA is an inclusive term and includes all types of CAs. CA, as used in this CPS document, includes component parts, which may be on the same hardware/software system or an integrated set of hardware and software within the control of a designated security boundary. Examples of components would be CA web servers/portals, databases, Key Escrow Systems (KES) and internal directories. All hardware, software and security requirements specified for CAs apply equally to the CA components. Any CA requirement expressed in this CPS applies to all CA types and components unless expressly stated otherwise. For additional details, refer to the IdenTrust *ECA Key Recovery Practice Statement* document available online at the *IdenTrust ECA Library,* under the "Policies – Current" section.

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

1.3.3 Card Management System

The Card Management System (CMS) manages smart card token content. In this context the CMS requirements are associated with issuing certificates ECA Medium Hardware Assurance and ECA Medium Token Assurance policies only. The CMS can also be utilized for issuance of ECA PIV-I certificates; however, IdenTrust does not

[1] ECA CP Section 15 - *Glossary*.

currently authorize issuance of ECA PIV-I certificates. A CMS is only deployed within IdenTrust or for an authorized External RA Organization. IdenTrust, as the CA, is responsible for ensuring that each CMS implementation meets the requirements described in the ECA CP, this CPS and requirements stated in the RPS document maintained by an authorized RA.

For additional details, see the definition of Card Management System (CMS) in the *Glossary* Section.

1.3.4 Registration Authorities (RAs)

The ECA CP Section 15 – *Glossary,* defines a *Registration Authority* as:

> *A Registration Authority (RA) is an entity that enters into an agreement with a CA to collect and verify Subscribers' identity and information that is to be entered into public key certificates. The RA must perform its functions in accordance with a CPS approved by the CA and the EPMA.*
>
> *RAs register subscribers, approve certificate issuance, and perform key recovery operations. Not all RAs are authorized to perform all RA functions. An RA designated to perform key recovery operations may be referred to as a Key Recovery Authority (KRA). KRAs can be RAs from the organization operating the ECA CA or from the subscriber organization. The KRAs from subscriber organizations shall only be able to recover keys of subscribers from their organization. The specific privileges, duties and responsibilities of individual RAs within the PKI are identified in the appointment documentation.*

A Registration Authority (RA) is an entity that is responsible for collecting and confirming an Applicant's identity and other information ultimately included in the Subscriber's Certificate. RA functions include the following:

- Establishing an environment and procedure for Certificate Applicants to submit their Certificate applications (e.g., creating a web-based enrollment page);
- The I&A of Individuals or entities who apply for a Certificate;
- The approval or rejection of Certificate applications;
- Approval of Certificate Revocations, either at the Subscriber's request or upon the entity's own initiative;
- The I&A of Individuals or entities submitting requests to renew Certificates or seeking a new Certificate following a Re-Keying process and processes set forth above for Certificates that are Issued in response to approved renewal or Re-Keying requests;
- Authenticating the subject's identity;
- Verifying the attributes requested by the subject for their Certificate;
- Assigning distinguished (unique) names to subjects; and
- Distributing Cryptomodules and associated software to Subscribers.

The term Local Registration Authority (LRA) is a trusted individual who performs the certificate registration and approval function for IdenTrust and/or for an External RA. Additionally, the term LRA may be used to describe actions performed by an individual employed by IdenTrust, to whom responsibilities associated with certificate registration and approval functions has been assigned.

In this CPS document the term Applicant is used to describe an individual who has applied for a Certificate, but has not yet received the Certificate.

The term Subscriber is used to describe an individual who has retrieved a Certificate following RA approval for issuance.

RAs are Organizations, whereas LRAs are Individuals; and only financially responsible Organizations will be RAs. CAs may delegate their registration functions (but not the responsibility of the CA to IdenTrust) to external Organizations that meet the financial requirements of the *Financial Responsibility* Section. Such RAs are referred to in this CPS as *External RA*s (see *External RAs* below).

Through their LRAs and TAs, RAs will accept Certificate applications, collect, and confirm Applicant identity information, and approve Certificate Issuance. An RA uses a system (RA System) to support services for

Applicants/Subscribers and LRAs. The RA System can be hosted by IdenTrust or by the External RA. An RA System provides Applicant/Subscriber services including Certificate lifecycle support such as Applicant's registration (only with IdenTrust-hosted system), Certificate retrieval and revocation/Suspension requests. LRA services provided by IdenTrust-hosted RA Systems include upload of Applicant information, Certificate application approval, generation of Activation information, support for emails notifications, and Suspension and/or revocation approval.

The RA System may also include a card issuance system that securely interacts with the CA as necessary to personalize cards and Cryptomodules. Communication between the RA System and an Individual (i.e., Applicant, Subscriber or LRA) is protected by securely encrypted sessions (i.e., Server or Client-authenticated SSL/TLS encryption, depending on whether a Certificate is available for mutual authentication). The server uses a Device Certificate Issued under a policy that achieves authentication of a Web\Application Server in-line with industry best practices and chains to a Root CA embedded in major browsers. LRAs always establish Client-authenticated sessions with the system and an Access Control List (ACL) allows only authorized LRAs to use the system's services.

An RA may communicate with a CA system for Certificate Issuance, Suspension, or revocation through either:

1. An LRA who initiates a Client-authenticated SSL/TLS-encrypted secured session with the CA and manages Certificates through a web-based interface; or
2. An RA System installed in a secure area of an RA facility that submits Digitally Signed ASN.1 or XML DSIG structures; see *XML Key Management Specification* via a Server-authenticated SSL/TLS-encrypted secured session.

1.3.4.1 External RAs

External RAs are Organizations that are bound by written agreement with IdenTrust, called an RA Agreement, under which, at a minimum, the External RA agrees to perform all delegated RA functions in a manner satisfying all RA requirements as stated in their IdenTrust PMA approved RPS, this CPS and the ECA CP. The RA Agreement also provides that the External RA is required to gain written authority to operate from IdenTrust prior to commencing production operations, and that IdenTrust shall not grant such authority until the External RA is able to demonstrate its ability to satisfy the aforementioned RA requirements, including finalization of an IdenTrust PMA approved RPS, and have undergone an external compliance audit in accordance with of the *Compliance Audit and Other Assessments* Section. Refer to the *Registration Practices Statement (RPS)* Section for additional information regarding the creation and approval of an RPS document.

Subsequent to production operations, the External RA is required to undergo an annual compliance audit in accordance with the *Compliance Audit and Other Assessments* Section. This is sometimes referred to as a zero-day audit. IdenTrust may initially grant interim approval to operate, allowing the External RA to begin RA activities and to establish historical transactional records that can be further audited to ensure compliance with the External RA's RPS, this CPS and the ECA CP. Following a full audit of RA activities resulting in a successful report, IdenTrust will grant final approval to operate.

External RAs are prohibited from delegation of their RA responsibilities under this CPS with the exception of contracting TAs.

External RAs are prohibited from contracting operation of a CMS for ECA Certificate Issuance to any entity other than IdenTrust.

1.3.4.2 Certificate Management Authority

ECA CP Section 15 – *Glossary*, defines both *Certification Authorities* and *Registration Authorities* to be *Certificate Management Authorities*.

ECA CP Section 15 – *Glossary*, 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 Section 15 - *Glossary*. IdenTrust conforms to the ECA CP requirements applicable to Certificate Management Authorities.

CMA tasks performed by IdenTrust employees or by individuals designated by an External RA are performed by personnel in Trusted Roles as outlined in the *Trusted Roles* Section. This includes appointment of individuals who are designated as LRAs by IdenTrust and/or an External RA and performs registration and certificate approval activities on behalf of the CMA.

1.3.4.3 Additional Authorities

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

1.3.4.3.1 IdenTrust Policy Management Authority

IdenTrust's Policy Management Authority (PMA) oversees the administration and application of this CPS with IdenTrust. The IdenTrust Policy Management Authority also has charge of the future development and amendment of this CPS, as provided in the *Policy Administration* and *Amendments* Sections. Additionally, the IdenTrust PMA is responsible to review and approve all Registration Practices Statements submitted by External RA organizations, before an External RA may be granted approval to operate on an interim and/or final basis.

1.3.4.3.2 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 the *Dispute Resolution Provisions* Section. The IdenTrust ECA Appeal Officer reviews the decision in the exercise of its oversight of IdenTrust's policies and their implementation in practice.

1.3.4.3.3 Security Officer

Members of the Security Office, are considered Security Officers. The Security Office is accountable directly to the Head of IdenTrust Operations, and they do 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.

1.3.4.3.4 Operations Management

IdenTrust's Operations Management includes the Head of IdenTrust Operation, and any designees he or she formally appoints. 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.

1.3.4.3.5 Head of IdenTrust Operations

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

1.3.4.3.6 Registrars

IdenTrust uses the term *Registrar* to mean the person performing the in-person confirmation of the Applicant's identification. Registrars include: LRAs; TAs; Notaries; Embassy/Consular officers; Authorized DoD Employees (ADE); and Judge Advocate General (JAG) Officers that may play a part in Applicant registration.

1.3.4.3.6.1 LRA

Per the *Qualifications, Experience and Clearance Requirements* Section, a LRA must be a U.S. citizen.

The term LRA is used to designate an individual who is employed with and appointed by IdenTrust to perform registration activities and approve certificate applications that are received via the IdenTrust online registration process for issuance.

Alternatively, the term LRA is also used to designate an individual who is affiliated with and appointed by an External RA to perform registration activities for applicants who are associated with that same External RA organization.

In the case where an organization utilizes TAs to conduct identity proofing, the LRA is a Registrar and the Individual who is responsible to collect (or receive process documentation from TAs) and confirms each Applicant's identity information ultimately to be included the Subscriber's Certificate. Depending on the contractual relationship, a TA may submit documentation to an IdenTrust LRA or an LRA affiliated with an external RA.

When IdenTrust enters a contract with an External RA Organization, through execution of an RA Agreement, the RA appoints one or more LRAs who is authorized to process Certificate Applications. LRAs service a limited population as authorized by the RA. The LRA and the RA Administrator are Trusted Roles held by Individuals who are subject to the requirements stated in the *Trusted Roles* Section. LRAs and RA Administrators comply with the External RA RPS document, this CPS and the ECA CP in the performance of their duties.

The External RA Organization provides information and instructions to LRAs with respect to the requirements and obligations associated with performing tasks respective to his or her LRA role.

Except where otherwise indicated, all requirements applicable to RAs apply to LRAs, including but not limited to physical protection of the LRA's workstation, audit logging, implementation of computer security controls and implementation of network security controls.

1.3.4.3.6.2 Trusted Agents (TAs)

ECA CP Section 15 – *Glossary*, defines a *Trusted Agent* as:

> *A person authorized to act as a representative of a CMA in providing Subscriber identity verification during the registration process. Trusted Agents do not have automated interfaces with CAs; they act on the behalf of the CA or the RA to only verify the identity and/or authority of the Subscriber. Trusted Agents do not have privileged access to CMA functions, are considered agents of the CMA. Trusted Agents are not considered CMA.*

Per the *Qualifications, Experience and Clearance Requirements* Section, individuals appointed in a Trusted Role must be U.S. citizens unless the identity proofing is carried out in one of the Five Eye (FVEY) countries listed in the ECA CP Section 11.1.3 - *Participating Countries*. In that case, the TA must either be a U.S. citizen or a citizen of the country where the identity proofing is performed.

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

By agreement with IdenTrust or an External RA organization, TAs are subject to the responsibilities imposed by the DOD ECA CP and this CPS and if affiliated with an External RA organization is also subject to any responsibilities as defined in the External RA's RPS document. TAs are required to obtain an ECA Certificate that is used to submit Applicant registration information to an authorized LRA for processing. All TAs must also submit an ECA Trusted Agent Addendum to an IdenTrust LRA before the TA designation can be authorized.

As specified in the ECA CP Section 1.3.7.1 – *Trusted Agents*, IdenTrust's TAs are considered to be agents of the CMA.

TAs are responsible to conduct identity proofing of Applicants and to confirm and document the identification of an Applicant in accordance with the *Authentication of Individual Identity* and *Performing Identification and Authentication Functions* Sections. Once identity proofing is successfully completed by a TA, he or she is responsible to submit all required registration artifacts to the IdenTrust or External RA LRA for processing.

A TA may be a Trusted Internal Agent or a Trusted External Agent.

NOTE: By stating Trusted Agents/TAs in this CPS, it is meant to include both Trusted Internal Agents and Trusted External Agents. However, if the responsibilities described are applicable to both External and Internal Trusted Agents/TAs, but not both, then the text will differentiate the roles by stating the full title.

1.3.4.3.6.2.1 Trusted Internal Agent

A Trusted Internal Agent is an employee of the same Subscribing Organization as the Individual Subscribers to be identified. A Trusted Internal Agent is ordinarily appointed by the Subscribing Organization subject to IdenTrust's approval.

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 Agent and cites the nominee's role in the Subscribing Organization and qualifications as a Trusted Internal Agent. The Subscribing Organization, in choosing Trusted Internal Agent 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 Agent. 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 Agent includes authorization by the Subscribing Organization to fulfill all responsibilities of a Trusted Internal Agent on behalf of the Subscribing Organization as prescribed in ECA CP and this CPS. The Trusted Internal Agent 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 Agent, should that be necessary.

1.3.4.3.6.2.2 Trusted External Agent

A Trusted External Agent is an independent third party under contract directly with IdenTrust and acceptable to the Subscribing Organization.

Trusted External Agents differ from their internal counterparts in that they are not employees of the Subscribing Organization and are not nominated by it. Instead, Trusted External Agents 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 Applicant for them to provide their services in a given instance. Like Trusted Internal Agents, Trusted External Agents are obligated by their contracts with IdenTrust to conform to ECA CP and this CPS.

1.3.4.3.6.2.3 TA Appointment and Removal

In both cases, a TA's qualifications and terms of service are contractually agreed to ensure trustworthiness. IdenTrust has the contractual right to supervise a TA 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 Agent, 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 Agent, IdenTrust attempts to resolve problems by communicating with the Trusted Internal Agent and the Subscribing Organization to avoid disrupting service and trust relationships.

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

- Conform to 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 TA by reading written instructions and any training materials provided by IdenTrust; and
- Demonstrate trustworthiness and competence during training and in performing verification services.

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

1.3.4.3.6.3 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 TA, a notary assists an IdenTrust or the External RA organization LRA by confirming and documenting the identification of an Applicant. Although IdenTrust provides forms and instructions for notaries, they are not contractually appointed; rather they 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 Applicant 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 Applicant's identity based on notarial representations; instead, the Applicant's identity must be established through a TA or by an LRA.

The *Enrollment Processes and Responsibilities* Section specifies how Registrars are to perform his or her role.

1.3.4.3.6.4 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[2] 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 in accordance with the *Identity Proofing by US Consular Officers and Judge Advocate General Officers* Section.

1.3.4.3.6.5 Authorized DoD Employees (ADE)

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 the *Authentication of Individual Identity* Section, or have their identity confirmed by a TA or an authorized DOD employee Department of Defense Employees who are authorized pursuant to the requirement stated in the ECA CP Section 11.2 – *Identity Proofing by Authorized DoD Employees*, may provide identify proofing services to foreign nationals under procedures described in the *Identity Proofing by Authorized DoD Employees* Section.

A representative of the ECA policy management team periodically emails IdenTrust an updated list of all Authorized DoD Employees. This list is used by IdenTrust LRAs to determine the authority of an ADE prior to approving a Certificate for Issuance.

IdenTrust disclaims any and all liability related to the identity proofing of foreign nationals or other registration services performed by DOD employees (ADEs) pursuant to the ECA CP Section 11.2 – *Identity Proofing by Authorized DoD Employees* .

[2] 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.

1.3.5 Subscribers

ECA CP Section 1.3.5 - *Subscriber* defines and limits who may be a *Subscriber*, as follows:

> *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 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 IdenTrust ECA Certificate profiles document and the *Certificate and CRL Formats* Section. The Individual Subscriber and Subscribing Organization are distinct entities, and the relationship between the two is described in the *Authentication of the Individual/Organization Affiliation* Section.

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.[3] In these cases, the Subscriber must establish to IdenTrust's satisfaction that he or she is acting in a professional capacity and not solely as an individual. NOTE: In this CPS document the term Applicant is used to describe an individual who has applied for a Certificate, but has not yet received the Certificate. The term Subscriber is used to describe an individual who has retrieved a Certificate following LRA approval for issuance.

1.3.6 Relying Parties

ECA CP Section 1.36 – *Relaying Parties* defines a *Relying Party* as:

> *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*

[3] 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).

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 the *Relying Party Representations and Warranties* Section.

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 IdenTrust ECA Certificate profiles document and the *Certificate and CRL Formats* Section 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. As such, 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 the *Other Business and Legal Matters*.[4] Section; 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 4) 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 these Sections:

- *Relying Party Representations and Warranties;*
- *Disclaimers of Warranties; and*
- *Limitations of Liability.*

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

1.3.7 Other Participants

1.3.7.1 Trusted Agents (TAs)

Refer to the *Trusted Agents* Section.

1.3.7.2 PKI Sponsor

A PKI Sponsor fulfills the role of an Applicant and 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 per the *Authentication of Component Identities* Section. 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 per the *Subscriber Representations and Warranties* Section.

The PKI Sponsor is not considered a Trusted Role.

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

[4] 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 sub-sections: *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).

1.3.7.3 Affiliated Organization

An Affiliated Organization is an organization that has a relationship with a subscriber and sponsors that subscriber for obtaining a Certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the Certificate if the affiliation is no longer valid.

1.3.7.4 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 LRA or a Trusted Internal Agent is also the PKI POC for the Organization; if a LRA or Trusted Internal Agent is not available, Personnel Office representatives, Security Officers or Management within the Organization may become PKI POCs after they have fulfilled the requirements in the *Qualifications, Experience and Clearance Requirements* and *Background Check Procedures* Sections.

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 LRA of the surrendered Cryptographic Module destruction and request the revocation of all Certificates associated with the surrendered Cryptographic Module.

1.3.7.5 Group/Role Manager

A Group/Role Manager shall be responsible for managing the Group/Role as described in the *Validation of Authority* Section. A Group/Role Manager is not a Trusted Role.

IdenTrust does not currently offer Group/Role Certificates under this ECA CPS.

1.3.7.6 Other Authorities

Refer to the *Additional Authorities* Section.

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 the *Prohibited Certificate Uses* Section.

This CPS applies only in relation to Certificates that are:

1. ECA Certificates, i.e., Certificates that contain one or more of the certificate policy OIDs specified in the *Document Name and Identification* Section;
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 the IdenTrust ECA Certificate profiles document and the *Certificate and CRL Formats* Section; 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.

1.4.1.1 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 Certificate type in compliance with the ECA CP Section 1.4.1.1 -*Level of Assurance*.

1.4.1.2 Factors in Determining Usage

As specified in the ECA Section 1.4.1.2 – *Factors in Determining Usage*, there are risk factors that should be considered by a Relying Party when establishing reliance upon a Certificate issued by IdenTrust. These factors include but are not limited to:

- The value of the information secured;
- The threat environment; and
- Any additional protection of the secured information environment.

1.4.1.3 Threat

In determining whether to rely, a prospective Relying Party is advised to consider the security threat under the circumstances as recapped in the ECA CP Section 1.4.1.3 – *Threat*, as follows:

> *Threat is any circumstance or event with the potential to cause harm. In terms of information systems, harm includes destruction, disclosure, or modification of data, processes, or processing components. Threats to systems include cyberattacks, environmental disasters, physical damage, system penetration, violation of authorization, human error, and communications monitoring or tampering.*

1.4.1.4 General Usage

As an ECA, IdenTrust issues Certificates having the three levels of assurance specified in the *Level of Assurance* Section. Guidelines for usage of these Certificate types, based on assurance level designation are as follows:

- **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.
- **PIV-I Assurance:** IdenTrust does not currently offer PIV-I Assurance Certificates under this CPS.

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

1.4.2 Prohibited Certificate Uses

Certificates issued under the provisions of this CPS may not be used for

1. 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; and
    e. Any other system whose failure could lead to injury, death, or environmental damage.
2. Transactions where applicable law prohibits the use of Certificates for such transactions or where otherwise prohibited by law; or
3. Applications that are classified or process classified data.

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 the *Policy Administration* and *Amendments* Sections.

When an RPS document is required for operation of an External RA, the IdenTrust Policy Management Authority must also approve the RPS prior to granting the External RA approval to operate. Refer to the *Registration Practices Statement (RPS)* Section for additional information.

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
policy@identrust.com
(888) 882-1104

1.5.3 Person Determining CPS Suitability for the Policy

As described in the same 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 as described in the *Amendments* Section. 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 the same Section 1.5.5 of the ECA CP.

When acting in any PKI participant's role provided for under the *PKI Participants*, Section, IdenTrust shall act in conformity with the obligations set forth in the *Representations and Warranties* Section that are applicable to such role; provided, however, in the event the EPMA grants IdenTrust a waiver under the provisions of the same 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

Acronyms are provided in the *Acronyms and Abbreviations* Section. Definitions are provided in the *Glossary* Section.

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; and
2. Provide access control mechanisms sufficient to protect Repository information as specified in the ECA CP Section 2.4 – *Access Control on Repositories* and the *Access Controls on Repositories* Section.

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 the 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. Availability is accomplished by building and maintaining fully redundant components and architecture in its primary facility as described in the *Primary Facility* Section. 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 per the *Disaster Recovery Facility* and *Offsite Backup* Sections. 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 the *Amendments* Section.

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 the *CRL Issuance Frequency* Section.

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 the *Computer Security Controls* and *Network Security Controls* Sections 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 IdenTrust ECA Certificate profiles document and the *Certificate and CRL Formats* Section.

Full details of the attributes listed in those distinguished names, their data content, and their interpretation can be found in the *Name Forms* Section. 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/TLS.

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 of Names to be Meaningful

The identifiers in a Certificate for Subscriber and Issuer are also defined based on the requirements for the ECA CP and the ECA Certificate Profile document. Relying Party can use the following information to interpret the components of an IdenTrust-issued ECA:

Field Name	Description
commonName	Lists the Individual Subscriber of the Certificate, together with the disambiguating number[5] explained in the *Uniqueness of Names* Section. 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. In the case of a component Certificate, the subject*: commonName* field identifies the component by its fully qualified domain name.
organizationalUnitName	Lists the Subscribing Organization with which the Individual Subscriber is affiliated. The IdenTrust ECA Certificate profiles document and the *Certificate and CRL Formats* Section 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 the *Establishment of a Parent Account for a Subscribing Organization Account* Section.
subjectAltName	When an email address is used in the subjectAltName, Internet Message Format RFC2822name guideline should be used to format 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. Alternatively, depending on the specifics of the implementation, subjectAltName may be used to provide 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 RFC2822.

The *Certificate and CRL Formats* Section and the IdenTrust ECA Certificate profiles document specify 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.

[5] The disambiguating number is also commonly known as and interchangeable with a globally unique identifier (GUID).

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 provided in the IdenTrust ECA Certificate profiles document and the *Certificate and CRL Formats* Section. 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 the *IETF RFC 2822* (formerly RFC 822, specifying the format of Internet e-mail messages), *IETF RFC 7230-7237* (on HTTP) and *IETF RFC 2253* which 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. The disambiguating number is also commonly known as and interchangeable with the term *globally unique identifier* (GUID).

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.

Alternatively, 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 re-keying of signing and encryption Certificates.

3.1.5.1 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) adheres to these requirements:

- Persists between a Subscriber's signing and encryption certificates;
- Persists for all renewals of a Subscriber's signing and encryption certificates;
- Persists for all re-keying of signing and encryption certificates;
- Does NOT persist to certificates issued after revocation; and
- Does NOT persist to certificates issued after expiration.

3.1.5.2 For Subscribing Organization-generated Disambiguating Numbers

Because the Subscribing Organization unequivocally assigns a unique identifier to each Subscriber and ensures that the numbers remain the same during the Subscriber'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 adheres to these requirements:

- Persists between a Subscriber's signing and encryption certificates;
- Persists for all renewals of a Subscriber's signing and encryption Certificates;
- Persists for all re-keying 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

In all cases when the CA does not generate the key, the CSR is submitted in PKCS-10 format. In order to obtain proof of possession of the private key, the CA verifies the signature on the PKCS-10 request using the subject public key information in the PKCS-10 request.

When encryption key escrow is required, the CA generates the keys and issues the Certificate during the Certificate Issuance process as described in the *Key Pair Generation* Section, and subsections listed under the *Private Key Delivery to Subscriber* Section.

3.2.1.1 Methodology for Key Generation and Submission of Certificate Request

All methods for key generation and requesting certificates must adhere to the following requirements:

1. signing keys are always generated by the requesting application (e.g.; CMS or Secure IdenTrust Retrieval Website);
2. When encryption key escrow is not required, encryption keys are always generated by the requesting application (e.g.; CMS or Secure IdenTrust Retrieval Website);
    a. When encryption key escrow is required, the CA generates the encryption keys and escrows the private key;
3. For all keys generated by the requesting application, a CSR/PKCS#10 is created;
4. Certificate requests generated by the requesting application are transmitted to the CA via a secure synchronous SSL/TLS Server-authenticated secured website session;
5. The CA receives the request and processes accordingly:
    a. Creates the signing Certificate;
    b. Creates the encryption certificate using the application generated request or the CA generated keys
        i. If encryption key escrow is configured for the requested encryption certificate type, the encryption key is generated on an HSM in the IdenTrust secure network, encrypted, and escrowed into the Key Escrow Database;
6. The CA returns the Certificates and any escrowed keys to the requesting application via the synchronous connection; and
7. The Certificate is installed for use.

3.2.1.2 Models for Key Generation and Submission of Certificates

There are four models managing Certificate applications that are authorized under this CPS. Within some of these application models, there are multiple options for Certificate retrieval and activation, as follows:

1. Approval of applications submitted via the Secure IdenTrust Registration Website
    a. IdenTrust provides Certificate activation material to Applicant with retrieval via the IdenTrust secure site;
    b. IdenTrust provides Certificate activation material to Applicant with CMS generation of keys in and insertion of certificates to the card via an External RA EWS/CMS; and
    c. IdenTrust provides Certificate activation material to a TA;
2. Submission of applications to IdenTrust via an online IdenTrust portal;
3. Approval of applications processed via an External RA using CMS:
    a. In-person card activation assisted by an LRA; and
    b. In-person card activation assisted by a TA;
4. Approval of applications processed using the IdenTrust secure online Certificate Lifecycle Management Tool;
    a. Online registration by Applicant; and
    b. LRA registration for Applicant.

These processes are described in further detail in the *Certificate Application* Section.

3.2.1.2.1 In-Person Card Activation Assisted by an LRA

In this retrieval model, the LRA assists the Applicant with smart card activation.

1. signing keys are always generated via the CMS on the smart card.
2. encryption keys may be generated via the CMS on the smart card, unless encryption key escrow is required.
    a. When key escrow is configured, the encryption key is generated by the CA, then encrypted and stored for escrow purposes, then passed to the CMS for insertion onto the smart card.
3. Following receipt of the requested Certificate(s) and keys (if encryption keys are generated by the CA) via the CMS interface, the Certificate and keys are installed in a new FIPS approved card or a FIPS approved card that is currently assigned to the Applicant.
4. Any required biometrics or other data is also inserted on the card.
5. If a new card has been generated, the Applicant selects his or her password that protects the card.
6. Possession of the card is then transferred to the Applicant

3.2.1.2.2 In-Person Card Activation Assisted by a TA

In this retrieval model, a TA assists the Applicant with smart card activation. Note that a different LRA than the LRA who coordinated the issuance of the smart card, may also act in the secondary role, in place of a TA. The following process will ensure proof of possession of the private keys:

1. Signature keys are always generated via the CMS and in the smart card;
2. encryption keys may be generated via the CMS in the smart card, unless encryption key escrow is required;
3. When key escrow is configured, the encryption key is generated by the CA, then encrypted and stored for escrow purposes, then passed to the CMS for insertion onto the smart card;
4. Following receipt of the requested Certificate(s) and keys (if the encryption keys are generated by the CA) via the CMS interface, they are installed in the FIPS approved card;
    a. Any required biometrics or other data is also inserted on the card;
5. Once the card has been generated, the LRA creates a temporary password to protect the smart card. The LRA sends the card to the requesting TA via courier and sends the temporary password for the card to the TA via a different out-of-band method such as secure email or other IdenTrust-approved method;
6. During an in-person session, the TA assists the Applicant with activation of the card, including creation of an Applicant-selected card password; and
7. Possession of the card is then transferred to the Applicant.

3.2.1.2.3 Processing Software-Based (Browser) Certificates via the CMS Interface

Refer to the *CMS Managed Registration* Section for information regarding deployment of this model via the CMS.

3.2.1.3 Submission of Applications via the IdenTrust Secure Online Certificate Lifecycle Management Tool

In this model approval of applications are performed by the LRA(s) designated by the External RA, via an online Certificate Lifecycle Management Tool provided by IdenTrust. This model requires that a separate queue be set up in the IdenTrust secure online Certificate Lifecycle Management Tool to allow separation of the External RA applications from all other applications submitted to IdenTrust. Additionally, each LRA designated by the External RA is issued an IdenTrust LRA Certificate that is configured in the secure online Certificate lifecycle system and processing permissions are established according to the user role. In order to access the secure online system, the LRA is required to authenticate using his or her active LRA Certificate. There are two processes available under this model.

3.2.1.3.1 Online Registration by Applicant

In this scenario, the Applicant visits the Secure IdenTrust Registration Website to submit his or her application. The application is then placed in the approval queue allocated to the External RA for processing.

1. Upon approval of the application by the External RA LRA an Activation Code is added to the secure online Certificate Lifecycle Management Tool database and is made available to the LRA.
2. The LRA then provides the Activation Code to the Applicant and directs him or her to the Secure IdenTrust Retrieval Website.
3. Upon receipt of the activation materials, the Applicant visits the Secure IdenTrust Retrieval Website and provides the LRA-provided Activation Code and the Applicant-selected Account Password which was selected during registration.
4. Following validation of this information, the Applicant generates his or her keys, downloads the Certificate and stores both in his or her Certificate store or Cryptographic Module.

3.2.1.3.2 LRA Registration for Applicant

3.2.2 Authentication of Organization Identity

3.2.2.1 Confirmation of Organization's Existence

In applying for a Certificate, the Applicant 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. If the External RA is also the Subscribing Organization, then the processes prescribed in this subsection to confirm the organization's existence need not be performed. Alternatively, if the External RA offers Certificates to external Subscribing Organizations, then the performance of these processes is required.

Designated LRAs for IdenTrust or an External RA[6] confirm 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; and

2. Presentation to IdenTrust of a copy of a governmentally issued[7] 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.

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 may be required.

[6] Although confirmation of an Individual Subscriber's identification is often performed by Trusted Agents on behalf of IdenTrust and/or an External RA, ordinarily the RA entity also confirms the corporate identity of a prospective Subscribing Organization. Often this confirmation is performed when concluding a contract for public key Certificate issuance and revocation services with that Subscribing Organization. In many cases the External RA is also the Subscribing Organization and does not require additional validation.

[7] 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.

The LRA 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 of Subscribing Organization is used by the LRA to validate the information provided in the Application. The Subscribing Organization name must be confirmed by the LRA to the extent that the LRA is confident that the organization named in the application is the same organization that has been independently verified as described above. The name of the Subscribing Organization that is provided in the Application is listed as the Organization (O) attribute in the Certificate. Once the IdenTrust or External RA LRA Confirms the existence of the Subscribing Organization and an account is established for that organization in the Subscriber Database per the requirements stated in the *Establishment of a Subscribing Organization Account* Section below.

3.2.2.2 Establishment of a Subscribing Organization Account

Prior to issuing an IdenTrust Certificate to an Applicant, the Subscribing Organization's existence must be confirmed. The existence can be based on the ongoing business relationship between IdenTrust and the Subscribing Organization or the External RA organization and the Subscribing Organization, which is maintained through correspondence or a payment stream and maintenance of a bank account. Following validation of the Subscribing Organization the LRA must establish an Account for the Subscribing Organization. The Account must be established before the CA can issue Certificates listing that Organization in the Certificate's subject field.

3.2.2.3 Authentication of the Individual-Organization Affiliation

IdenTrust ECA Certificates are not Issued to Applicants having no organizational affiliation or who are acting in a personal capacity and not a professional capacity as per the *Subscribers* Section. The Subscribing Organization need not be incorporated; however, it must conduct business. A Subscribing 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 *organizationalUnit* (OU) attribute in the subject field of the Certificate.

If the Applicant is located outside of the United States, IdenTrust may impose, through the Subscriber Agreement, additional restrictions in view of other jurisdictional 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 General Data Protection Regulation (GDPR) 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;
- A member or officer of;
- A 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 is determined by the authorization delegated by the Subscribing Organization to the Individual Subscriber for the transaction in question. That authority cannot be inferred from an ECA Certificate issued by IdenTrust. IdenTrust does not issue ECA Certificates that assert roles or authorizations.

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 the following approvals and confirmations.

3.2.2.3.1 Approval of the Subscribing Organization Confirming Applicant Affiliation

The authority of the Organization Officer to authorize an Applicant to receive a Certificate that is affiliated with the Subscribing Organization is established through application of the Organization Officer's signature on the Subscribing Organization Authorization Agreement form. This form provides the following assertions:

1. Certification that the Applicant is affiliated with the Subscribing Organization; and
2. An attestation that the individual signing the form is an officer of the Organization and has authority to make the representations and warranties in the Agreement on behalf of the Organization and to bind the Organization to the Terms and Conditions described in the form.

The authorization for the Applicant to receive a Certificate is conveyed to the RA through the submission of the application and all relevant forms.

The LRA must independently confirm that the Organization Officer named on the Subscribing Organization Authorization Agreement form has actually signed the form.

Affiliation between the Subscribing Organization and the Applicant is established through verification of the Subscribing Organization Authorization Form, which is completed by an authorized Officer of the Subscribing Organization as described in the *Approval of the Subscribing Organization Confirming Applicant Affiliation* Section. This is accomplished by performing the following procedures:

1. Review of the Subscribing Organization Authorization Form to ensure that the Applicant information is complete and matches the information provided on the In-Person Identification Form as described in the *In-Person Authentication* Section;
2. Ensure that all Organization Officer information is provided on the form;
3. Ensure that the named Organization Officer has signed the form; and
4. Verify the that the named Organization Officer is affiliated with the Subscribing Organization and that he or she has actually signed the Subscribing Organization Authorization Form (see details below).

In the situation where a TA performs the in-person verification, he or she confirms this affiliation through a third party within the Subscribing Organization. Alternatively, upon receipt of the forms submitted by the Applicant, the LRA initiates communication with the Subscribing Organization using an independently verified point of contact, i.e., the LRA obtains telephone numbers for the Subscribing Organization from a trusted, independent third-party source of such information. The third-party may also be the Human Resources department or any individual in a capacity within the Subscribing Organization to Confirm the affiliation. The LRA must confirm that the signing Organization Officer named on the Subscribing Organization Authorization Form did in fact sign such form.

The LRA records the performance of this confirmation in an auditable log.

3.2.3 Authentication of Individual Identity

Before the IdenTrust ECA issues a Certificate, the identification of the Applicant 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 an Applicant'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 the *Authentication of the Individual-Organization Affiliation* Section. During the in-person appearance an In-Person Identity Form is used to compile the information obtained from the forms of identification reviewed by the Registrar. The Applicant and the Registrar are required to sign the form and the Applicant must submit the form to the LRA for processing and archival. Additional details related to the enforcement of this 30-day requirement and processing of Certificate applications is detailed in the *CA Actions During Certificate Issuance* Section.

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 Applicant's identification. Registrars who are authorized to perform in-person identity validation will vary depending on various factors, including:

- The Assurance level of the Certificate;
- The citizenship of the Applicant; and
- The geographic location of the Applicant.

Citizenship is distinguished by three (3) categories, as follows:

- United States (US);
- Five Eyes (FVEY)*; or
- Other Countries**

Geographic local is distinguished by four (4) categories, as follows:

- United States (US);
- Five Eyes (FVEY)*;
- Non-FVEY Countries with a US Embassy; or
- Non-FVEY Countries**

*Five Eyes or FVEY refers to the intelligence alliance comprised of Australia, Canada, New Zealand, the United Kingdom, and the United States.

**IdenTrust is prohibited from issuing Certificates to any country that is sanctioned by the U.S. government. IdenTrust maintains a list of countries, including Five Eye countries, where IdenTrust certificates may be issued. The IdenTrust registration system will not allow Certificate applications to be accepted in countries that are not on the approved list.

The matrix provided in Section 3.2.3.1.3 establishes authority of the Registrar based on these factors.

3.2.3.1.2 Registrar Authority Guidelines

When applying for a DOD ECA digital certificate, Part 2 of the In-Person Identification Form must be signed in the presence of a person who is authorized to verify the Applicant's identity. As authorized persons vary depending on the type of DOD ECA certificate that the Applicant is purchasing, his or her citizenship and/or where he or she is geographically located, the matrix on the following is used to determine Registrar Authority for completion of in-person identity vetting.

NOTE: All non-Five Eyes citizens outside of the U.S. must have their *Part 2: In-Person Identification Form* signed by an Authorized DoD Employee (ADE).

3.2.3.1.3 Registrar Authority Matrix

Assurance Level	Availability	Scenario		Registration Authority	Trusted Agent	Notary	Consulate	Authorized DoD Employee	Judge Advocate General
		Citizenship	Applicant Location						
Medium Medium Token Medium Device	Offered to Applicants in the U.S. and in foreign countries	U.S.	In the U.S.	X	X	X			
		U.S.	In a non-U.S. with a U.S. Embassy	X	X		X		X
		FVEY	In the U.S.	X	X	X		X	
		FVEY	In a FVEY country	X	X		X	X	X
		FVEY	In a non-FVEY country					X	
		Non-FVEY	In the U.S.	X	X	X		X	
		Non-FVEY	Outside of U.S.					X	
Medium Hardware	Offered only to Applicants in the U.S.	U.S.	In the U.S.	X	X				
		FVEY	In the U.S.	X	X				
		Non-FVEY	In the U.S.	X	X				

3.2.3.1.4 Registrar by Certificate Type

3.2.3.1.4.1 Medium-Assurance (non-hardware) Certificates

These Certificates can be issued to individuals located in the U.S. and countries that are not sanctioned by the U.S. government.

All defined Registrars are permitted to act as Registrar for a Medium Assurance Certificate depending on the citizenship and location of the Applicant. Refer to the preceding Table: Registrar Authority Matrix, for specific scenarios. The Registrar may be a notary who is 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. TAs in accordance with the *Initial Identity Validation* Section, or authorized DoD employees (ADEs) in accordance with the *Identity Proofing Outside of the U.S*. Section, may also 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).

The requirements in this section also apply to applications for Medium Assurance Component Certificates.

3.2.3.1.4.2 Medium Token Assurance Certificate

These Certificates can be issued to individuals located in the U.S. and countries that are not sanctioned by the U.S. government.

All defined Registrars are permitted to act as Registrar for a Medium Token Assurance Certificate depending on the citizenship and location of the Applicant. Refer to the preceding Table: Registrar Authority Matrix for specific scenarios. The Registrar may be a notary who is 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. TAs in accordance with the *Initial Identity Validation* Section or authorized DOD employees (ADEs) in accordance with the *Identity Proofing Outside of the U.S*. Section, may also 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).

3.2.3.1.4.3 Medium Hardware Assurance Certificate

These Certificates are only available to Applicants who are located in the U.S. and IdenTrust requires that the Registrar before whom the Applicant appears must be one of the following:

1. LRA;
2. A TA; or
3. An employee performing the TA role; provided that the employee would not be precluded from acting as Registrar by the Separation of Role requirements of the *Roles Requiring Separation of Duties* Section.

A notary may not act as Registrar for this type of Certificate (unless he or she is also a TA).

In any case, whichever type of Registrar is appropriate; the authorized LRA for IdenTrust or the External RA 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 an Applicant for any notarial or other fees incurred for the services of the Registrar.

3.2.3.1.5 In-Person Registration Procedure

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

The Applicant must appear in person before an eligible Registrar, based on the Certificate type as described in the foregoing sub-sections. The Applicant must:

1. **Present Required Identification**

   The Applicant must provide 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 Applicant 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 Applicant but also must enable the Registrar to Confirm the Applicant'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[8], 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.

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

[8] 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 one (1) year of birth. A delayed birth certificate filed more than one year (1) 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.

Procedures and requirements for identity verification of U.S. citizens in foreign countries and non-U.S. citizens whether in the U.S. or in a foreign country are fully detailed in the *Identity Proofing Outside of the U.S*.

2. Sign an In-Person Identification Form

The *Certificate Application* Section describes the Certificate application process in detail. The Applicant must sign the In-Person Identification Form (ID Form) in the presence of the appropriate Registrar. The ID Form is used to record the identification of the Applicant 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 Applicant's signature must be in ink. By signing, the Applicant attests to the accuracy of the information on the form. After signing, the Applicant provides the original, signed ID Form to the Registrar for identity confirmation and endorsement under sub-section (3) below.

3. Confirm the Accuracy of the In-Person Identification Form

The Registrar is responsible to ensure that all information provided in the ID Form is recorded accurately. Unless otherwise specified below, these tasks are completed by the Registrar in the presence of the Applicant. The Registrar:

- Examines the official identification documents provided by the Applicant;
- Confirms that the documents are free of any apparent defect on their face; and, that at least one of the documents that has a photo must be within their validity period as of the date that the in-person identification is performed;
- Verifies that the photograph represents a likeness of the Applicant;
- Validates that the documents do not have any obvious inconsistencies between each other and with the ID form, unless the Applicant 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; and
- When Subscribing Organization-generated disambiguating numbers[9] are used, the Registrar positively matches the Applicant to his/her internal unique identifier documented in the ID form, using the applicable Subscribing Organization's databases or documents (e.g., work badge)[10]

Only if sufficient documentation meeting the requirements as stated in the ID form has been validated and, when necessary, the unique identifier has been matched to the Applicant the Registrar endorses and dates the ID form.

In confirming the identification of an Applicant, the TA or LRA has discretion to do any or all of the following:

- Require additional information or evidence from Applicant 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 Applicant; and/or
- Decline to proceed with the registration of a specific Applicant, with or without giving a reason.

[9] The disambiguating number is also commonly known as and interchangeable with a globally unique identifier (GUID).

[10] As employees for the Subscribing Organization, Trusted Agents have access to Subscribing Organization databases and training that allows them to accurately confirm the match. When an internal Trusted Agent is not available, external Trusted Agents, trusted employees of IdenTrust or IdenTrust LRAs may be granted authorization to access the same databases and training for its use.

In all cases, the TA or LRA 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 TA or LRA must also document all actions taken in the exercise of the above discretion.

Completion of the foregoing confirmation procedures are required in addition to any other tasks described in the *Identity Vetting Approval* and *CA Actions During Certificate Issuance* Sections for processing of a Certificate application.

3.2.3.1.6 Email Verification

Verification of the Applicant's email address is also required and can be conducted in one of two ways; electronically or manually as further described in the following subsections.

All ECA Certificate applications require verification of the email address provided in the application. If the email verification is not completed the application must not be approved.

3.2.3.1.6.1 Electronic Verification of Email

When an Applicant 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 and instructions for completing the verification process;

- A link to a Server-authenticated SSL/TLS secured website session; and
- A numerical code.

To confirm the email address, the Applicant selects the provided link, which will direct the Applicant to a secure IdenTrust email authentication website. The website requires the Applicant to input the provided numerical code, as well as the Applicant-selected Account Password that was generated during the online registration process. The numerical code is specific to the Applicant and unique for each application submission. Following validation of the numerical code and the Account Password, the IdenTrust database is updated to indicate that the Applicant's email address has been verified and the application approval process may be resumed.

3.2.3.1.6.2 Manual Verification of Email

Manual verification of an Applicant's email address can be completed by a TA or LRA, based on the internal knowledge of the Subscribing Organization. Internal databases and directories may be used to confirm the validity of the email address.

3.2.3.1.7 Identity Vetting Approval

When the Registrar has completed the identity validation per the requirements set forth in the *Enrollment Process and Responsibilities* Section, then the Registrar must sign the In-Person Identification Form attesting to the veracity of the identification forms provided by the Applicant. Any professional seals (such as a notary seal) must also be provided, as appropriate.

Once the In-Person Identification Form and the Subscribing Organization Authorization Form are completed, the Applicant or TA submits the forms to the LRA for processing.

The LRA reviews the required forms and performs verification procedures as required by this CPS. Once satisfied, then the request for a Certificate may be approved in accordance with the *Certificate Application* and *Certificate Issuance* Sections.

A Certificate Application can only be approved by an authorized LRA and Issuance of a Certificate can only be enacted by IdenTrust as the ECA. Following approval of an Application, the Applicant is provided with activation materials depending on the RA implementation as described in the *Method to Prove Possession of Private Key* and *Certificate Application* Sections.

The LRA is responsible to document the confirmation process in a form capable of being archived as required in the *Records Archival* Section.

An Applicant/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 the IdenTrust ECA, who will present information sufficient for registration at the level of the Certificate being requested, for both himself or herself 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 the *Identification and Authentication for Routine Re-Key* Section, if the following are all true:

- **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 Account;
- **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 the *Who May be A Registrar* Section, and following the procedure specified in the *In-Person Registration Procedure* Section, at least once within the time periods listed below:
    - For ECA Medium Assurance and ECA Medium Token Assurance Certificates, an Individual Subscriber may be digitally authenticated for Certificate renewal events for the period of nine (9) years between in-person identity proofing events; or
    - In the case of an Individual Subscriber of a Medium Hardware Assurance Certificate in-person identity proofing must occur every three (3) years.

  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.
- **Information from Authentication Certificate Remains Unchanged:** IdenTrust will issue a new Certificate containing the same attributes as follows:
    a. Subject Distinguished Name;
    b. Certificate Policy OID;
    c. Subject Alternative Names, and
    d. 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 the *Names Identifying the Subscriber* Section. Component Certificates also list the name of the Subscribing Organization associated with the device as per the *Authentication of the Individual-Organization Affiliation* Section.

The devices 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 this section and provide to IdenTrust or a TA 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 TA to communicate with the PKI Sponsor when required.

The LRA Confirms the accuracy of the information using the following steps:

3.2.3.3.1 Verification of Documents

For requests for Component Certificates, the PKI Sponsor will submit completed and authorized forms as described in the *In-Person Registration Procedure* Section, to the LRA before an application for a device Certificate can be reviewed. A TA may also submit such forms on behalf of the PKI Sponsor.

3.2.3.3.2 Confirmation of Authorization

The PKI Sponsor is required to establish authorization to obtain a Component Certificate by submitting a Subscribing Organization Authorization Agreement signed by a representative of the Subscribing Organization as described in the *Part 1: Subscribing Organization Authorization Agreement* Section. Contact information for the confirming authorization (address and telephone number of Organization) is independently obtained from existing Subscriber or Subscribing Organization account records or a third-party database. The LRA contacts the registered domain administrator, human resource manager, or the authorizing official listed in the Subscribing Organization Authorization Agreement contract 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 Subscribing Organization Authorization Agreement. The new PKI Sponsor may provide such agreement proactively at any time. Alternatively, a new agreement will be required during re-key and revocation lifecycle events when requested by a different PKI Sponsor.

3.2.3.3.3 Authentication of Component-Organization Relationship

As detailed in the Names Identifying the Subscriber, Certificate and CRL Formats and in the IdenTrust ECA Certificate profiles document, 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 the 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.

During the authentication process, the relationship between the Subscribing Organization and the Component is confirmed 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, authorization of which is provided in the Subscribing Organization Authorization Agreement. In cases that the Component common name is not recorded in databases external to the Subscribing Organization, the LRA will communicate with the Subscribing Organization to confirm the relationship, which may include submission of an authenticated digitally signed email or a form letter on letterhead from the Subscribing Organization signed by a TA (preferably by a Trusted Internal Agent) or counter-signed by a notary may be used. If proof of relationship cannot be confirmed, then the application must not be approved.

3.2.3.3.4 Verification of Domain Ownership

If a registered Domain Name or IP address is to be used in the Certificate one of the following validations may be used:

- A verification against third-party databases;
- A reverse lookup to Confirm that the Subscribing Organization owns or controls the Domain Name or IP address;
- A constructed email to Domain Contact;
- Agreed upon change to website;
- Notification of DNS change; or
- IP address.

3.2.3.3.5 Verification of Request

The LRA contacts the PKI Sponsor via verified email address or confirmed telephone 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.

If deemed necessary, the LRA may also request additional information in the form of a signed letter printed on letterhead of the Subscribing 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 by an LRA.

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.

Group Certificates are not currently offered by IdenTrust. For more information pertaining to Group Certificates, refer to the ECA CP Section 3.2.5 – *Validation of Authority*.

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, including a Re-Keyed Certificate is issued based on confirmation of a valid, earlier issued Certificate, the limits specified in the *Electronic Authentication of Individuals* Section will apply, including restrictions to enforce rules to ensure that the *notAfter* date field in a Certificate may not extend beyond the next in-person identity proofing date. This is restriction is enforced by the IdenTrust ECA system.

During the process of 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 the *Glossary* Section). If confirmation of a new Certificate is based on a digital signature, according to the *Electronic Authentication of Individuals* Section, which requires that that digital signature be verifiable as 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

Requests for Certificate Re-Key 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 the *In-Person Authentication* Section.

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 in accordance with the procedures provided in the *Procedure for Revocation Requests* Section. Requests to revoke a Certificate may be also be authenticated using that Certificate's associated private key, regardless of whether or not the private key has been compromised.

3.5 Identification and Authentication for Key Recovery Request

3.5.1 Subscriber Key Recovery Request

The Subscriber will establish his or her identity to the KRA, or the KRO as an intermediary for the KRA, in person or via digital signature authentication. Authentication will be commensurate to the assurance level of the key being requested and will be in accordance with the processes described in the IdenTrust *ECA Key Recovery Practice Statement* document.

IdenTrust's KRA or the Organization's KRO can authenticate Subscribers in person or using digital signatures. IdenTrust's KROs may only perform in-person authentication, since a Subscriber performing self-authentication with a digital Certificate would communicate directly through electronic means with an IdenTrust KRA.

KROs will personally Confirm the identity of the Subscriber prior to initiating the Key Recovery request using practices specified in the *In-Person Authentication* Section. KRAs and KROs will be acting as Registrars as defined in the *Who May Be a Registrar*. Section.

The Subscriber may also use a digital signature to authenticate his or her identity. An IdenTrust KRA or Subscribing Organization KRO may accept a digital signature created with the Signature Key corresponding to the Subscriber's IdenTrust-issued ECA Certificate of at least the same assurance of the Decryption Key to be recovered. The confirmation process will follow the practices outlined in the *Electronic Authentication of Individuals* Section. Refer to the IdenTrust *ECA Key Recovery Practice Statement* document for additional details.

3.5.2 Third Party Key Recovery Request

In order for a Key Recovery request to be accepted, a third party Requestor will establish his or her identity to the KRA, or the KRO as an intermediary for the KRA, through in-person identity proofing or through verification of their digital signature.

KROs may Confirm the identity of the Requestor by in-person identification prior to processing a Key Recovery request. This method can be used if the Requestor does not have access to their digital certificate. Should in-person identification be used, KRAs and KROs will act as Registrars as described in the *In-Person Registration Procedure*. Section.

The Requestor may use a digital signature to authenticate his or her identity based on meeting the criteria in the *Electronic Authentication of Individuals* Section. To do this IdenTrust's KRA or a KRO may validate the Requestor's digital signature by reference to an IdenTrust-issued ECA Certificate. The confirmation requires the digital signature be created by a Valid ECA Certificate with an assurance level equal to or higher than the Decryption Key requested to be recovered, which is verified manually by comparing the Certificate Policy OIDs in the Requestor's Certificate with the assurance level of the Certificate being requested. Refer to the IdenTrust *ECA Key Recovery Practice Statement* document for additional details.

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 TA acting on behalf of the Applicant.

4.1.2 Enrollment Process and Responsibilities

Applicant registrations for IdenTrust-issued signing and encryption Certificates may be initiated through various registration processes as described in the following sub-sections.

In all registration processes related to approving and issuing a Certificate, an Account for the Subscribing Organization must be established. Once an 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 Account associated with the Subscribing Organization (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 several methods as described in the *Registration Processes* Section.

- Online Registration
- LRA Assisted Registration
- CMS Managed Registration (for Hardware Certificates and for Software Certificates)
- Portal Registration
- Bulk Load Registration

4.1.2.1.1 Required Information for all Certificates (Signing, Encryption, and Component)

All signing, encryption and component Certificate Applicants must provide the following information:

- 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);
- Payment information such as credit card details, purchase order number or voucher number; and
- When, applicable, an external disambiguating number[11] (see below for additional details).

4.1.2.1.2 Required Information for signing and encryption Certificates Only

In addition to the requirements in the *Required Information for all Certificates (signing, encryption, and Component)* Section, the following information must be collected for signing and encryption Certificates:

- Applicant's Citizenship(s)

[11] The disambiguating number is also commonly known as and interchangeable with the term *globally unique identifier* (GUID).

- 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 the *Authentication of Individual Identity* Section.

4.1.2.1.3 Required Information for Component Certificates Only

For the issuance of a Component Certificate, the PKI Sponsor submits the certificate application, which includes a PKI Sponsor generated key pair for the Component and submits the PKCS#10 Certificate request as an initial step during registration.

In addition to the required in the *Required Information for all Certificates (signing, encryption, and Component)* Section, the following information must be collected for component Certificates:

- Server name; and
- RSA PKCS#10 Certificate signing Request (CSR).

4.1.2.2 Account Password Generation and Reset

An Account Password serves two purposes:

- Facilitates retrieval of a Certificate, when used in conjunction with an LRA provided Activation Code; and
- Facilitates access to the Secure User Certificate Management Tool for Certificate maintenance.

4.1.2.2.1 Account Password Generation

In some registration processes an Account Password[12] is selected by the Applicant which consists of at least eight characters and 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 also required to create three questions and secret answers. This information will be used as a mechanism to reset his or her Account Password in the event that his or her Account Password is misplaced or otherwise unavailable for Certificate retrieval or maintenance.

4.1.2.2.2 Using a Security Code to Select an Account Password

In cases where the Applicant has not selected an Account Password during the Registration process, such as when a TA submits a bulk load request, the Applicant must be provided with a mechanism to select an Account Password during the Certificate Retrieval process. In this scenario, a unique, randomly-generated Security Code is also requested by the LRA and provided to the Applicant in a separate channel from the Activation Code.

Both the Security Code and the Activation Code will be required during the secure online retrieval process. Following authentication of the Security Code and the Activation code, the Applicant will then be required to create an Account Password.

4.1.2.2.3 Account Password Reset

The password reset process is initiated by a Subscriber who provides his or her Certificate Activation Code[13] and selecting the Account Password reset URL. This process sends a One-Time-Code (OTC) and specified URL to the confirmed 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

---

[12] This Account Password is separate from—and should not be confused with—the password required by the ECA CP Section 6.4.1 – *Activation Data Generation and Installation*, and this CPS for protection of a private key stored in a FIPS 140-evaluated Cryptographic Modules. See also the Method to Prove Possession of the Private Key Section above.

[13] The Activation Code is provided by the LRA or TA to the applicant when his or her Certificate is initially approved.

questions that were randomly generated from a pool of password-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.

4.1.2.3 Disambiguating Numbers

An external disambiguating number assigned by the Subscribing Organization and provided to IdenTrust by the with the Applicant's registration data, consists of eight (8) to 20 numbers. The term disambiguating number is also commonly known as and interchangeable with the term globally unique identifier (GUID). Disambiguating numbers are based on Subscribing Organization unique identifiers that:

1. Will remain unchanged during the Subscriber's tenure;
2. Are decommissioned or made inactive when the Subscriber is no longer affiliated with the Organization; and
3. Are never re-used by the Subscribing Organization with a different Subscriber.

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 is confirmed by the Registrar. The IdenTrust system will also automatically compare a new disambiguating number against all accounts associated with the Subscribing Organization to ensure the number is used for only one Subscriber. IdenTrust also confirms that the Organization-assigned number with leading zeros does not match any number assigned by IdenTrust to the Subscribing Organization.

For additional details regarding disambiguating numbers, see the *Uniqueness of Names* and *Glossary* Sections.

4.1.2.4 Registration Documents

Following submission of the registration information and acceptance of the online Subscriber Agreement[14], the Applicant is provided with the Subscribing Organization Authorization Agreement (the "Authorization Agreement") and In-Person Identification Form (ID Form). Forms must be retained by the LRA for archival and audit purposes per the *Records Archival* Section.

4.1.2.4.1 Subscriber Agreement

During the online registration process, the Applicant is required to accept the Subscriber Agreement; however, in cases where the Certificate application is submitted via other methods besides the online registration process as described sub-sections of the *Registration Processes* Section, the LRA is obligated to obtain a signed copy of the Subscriber Agreement and retain a paper or electronic copy of the document according to the archival requirements set forth in the *Records Archival* Section.

4.1.2.4.2 Part 1: Subscribing Organization Authorization Agreement

The Authorization Agreement is required for each Applicant and 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 cases where the Subscribing Organization cannot determine who, within the organization, is authorized to execute the agreement or where the law of the Subscribing Organization's jurisdiction does not recognize apparent authority, a power of attorney may be required.

[14] 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.

4.1.2.4.3 Part 2: In-Person Identification Form

Applicants are instructed to take the ID Form to an authorized Registrar, as defined in the *Who May be a Registrar* and further *Registrar Authority Guidelines* Sections. The Applicant will present the completed ID Form and necessary credentials to a Registrar as required by the *In-Person Registration Procedure* Section. The ID Form contains documentation including a Subscriber acknowledgement, Registrar instructions, and designated space for the Registrar to initial or complete when verifying the accuracy of the identifying information presented.

The Applicant must sign the ID Form in the presence of the authorized Registrar. The Registrar completes the following tasks:

1. Records the type, serial numbers and expiration dates for the identification documents presented by the Applicant;
2. Verifies that the identification document is protected against forgery, modification, or substitution (e.g., holograms and other security features);
3. That the Applicant is the holder of the identification documents presented and that the picture and name on the Photo ID match the appearance and name of the Applicant; and
4. Signs (or notarizes if the Registrar is a notary) the ID Form.

In accordance with the *Authentication of Individual Identity* Section and upon completion of the in-person identity confirmation before the Registrar, the Applicant's ID Form contains:

1. A record of the identity of the Registrar;
2. A signed declaration by the Registrar that he or she has 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. The date of the in-person identity confirmation.

4.1.2.4.4 Forms Submission

Following completion of all forms and validation of all information collected from the Applicant, the ID Form and the Authorization Agreement are submitted by the Applicant or the Registrar to IdenTrust or External RA LRA depending on the defined registration model. Refer to the *Registration Processes* Section for more specific details regarding submission of registration forms by registration model. Submission of the required registration artifacts must adhere to the following guidelines:

- The original, paper ID Form must be submitted to the LRA;
- The signed paper Authorization Agreement may be submitted; or alternatively, 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 LRA or the External RA LRA, in-person or via courier or mail service; and
- In the case in which the Registrar is a TA, the TA will submit the information to IdenTrust LRA or the External RA LRA in-person or via a mail or courier package containing the original paper documentation.

4.1.2.5 Documentation Review

Following receipt of all application data and artifacts, the IdenTrust or External RA LRA will:

1. Review the information submitted to assess the adequacy and timeliness of the in-person identity confirmation;
2. 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);
3. Review the Authorization Agreement for organizational affiliation; and
4. Verify the signature of the Registrar who performed the in-person identity confirmation in accordance with the *In-Person Authentication* Section.

Confirmation of an authorized signature must adhere to the following guidelines:

- Review of the TA's signature will consist of a visual confirmation of the TA's manual signature on the in-person identification form; and
- Review of the 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.

Use of a PDF program to perform a signature verification and revocation check of digital signatures included on Authorization Agreements that are submitted electronically.

4.1.3 Registration Processes

There are multiple registration models utilized in conjunction with the approval and issuance of Certificates under the ECA policy. The processes prescribed for the various registration models is dictated by certain variables which including:

- Which organization acts as the RA;
  - IdenTrust or an authorized External RA
- Who may conduct identity vetting;
  - Assurance level
  - Citizenship
  - Geographic location
  - Role designation (ADE, JAG, TA, LRA, etc.)
- Who is authorized or delegated authority to approve applications;
  - IdenTrust or External RA LRAs
- What tools are utilized for processing Certificate requests, such as:
  - Direct application via Secure online registration;
  - Online IdenTrust provided Certificate Lifecycle Management Tool;
  - Portal registration by TAs or LRAs;
  - Secure interface between the CA and RA using CMS processing; and/or
  - Bulk load registration by TAs or LRA.

The following sub-sections provide the description of application procedures by processing methodology.

- **Online Registration:** Individual Applicants can provide registration information via an online Certificate application process over a Server-authenticated SSL/TLS secured website hosted by IdenTrust. Refer to the *Online Registration* Section for processing details related to this model.
- **LRA Assisted Registration**: LRAs designated by External RAs can provide Applicant registration information via an online Certificate Lifecycle Management Tool over a *Client-authenticated SSL/TLS* secured website hosted by IdenTrust. Refer to the *LRA Assisted Registration* Section for processing details related to this model.
- **CMS Managed Registration:** LRAs designated by External RAs, where a Card Management System (CMS) implementation has been deployed, can provide Applicant registration information via the CMS interface, using a standard API and secure request/return exchanges to request and issue a hardware-based Certificate via a Server-authenticated SSL/TLS secured channel. Refer to the *CMS Managed Registration* Section.
- **Portal Registration:** Individual Applicants can provide registration information to a TA, who will forward the information to IdenTrust via a secure online client-authenticated SSL/TLS channel. IdenTrust acts as the LRA in this model. Refer to the *Portal Registration* Section.
- **Bulk Load Registration:** In this model, an authorized TA compiles registration and identity proofing information and utilizes a predetermined bulk load template to submit one or more applications for a Certificate to IdenTrust for LRA review and approval. Refer to the *Bulk Load Registration* Section.

4.1.3.1 Online Registration

In this model the Applicant will utilize the IdenTrust Secured Registration website to provide all information required to process a Certificate application.

4.1.3.1.1 Registration Authentication Method

In this model, the client visits the Server-authenticated SSL/TLS secured IdenTrust Registration website and is directed to the proprietary registration page for the Certificate type desired by the Applicant. See additional information under the definition of *Server-authenticated SSL/TLS* in the *Glossary* Section.

4.1.3.1.2 Data Input

In this model, the Applicant provides all application data and payment information via the Server-authenticated SSL/TLS secured IdenTrust Registration website.

In the case where the Applicant is requesting a Component Certificate, the Applicant must also provide a pre-generated CSR file that will be used for Certificate Issuance following approval of the Certificate application. The Server-authenticated SSL/TLS secured IdenTrust Registration website provides for submission of the CSR. The CSR is then associated with all Applicant information stored in the Certificate Lifecycle Management Tool database.

4.1.3.1.3 Account Password

The Applicant creates an Account Password which is used to facilitate key generation and Certificate retrieval after his or her application has been approved. See additional information in the *Account Password Generation and Reset* Section.

4.1.3.1.4 Identification and Authentication

The Applicant must meet with an individual who is authorized to conduct in-person identity proofing. The individual performing the in-person identity proofing must complete and sign the required form. The form must be submitted to IdenTrust in order for the Application to be processed. Refer to the *Authentication of Individual Identity* Section for more information about who is eligible to perform in-person identity proofing and the requirements for conducting the session.

4.1.3.1.5 Required Documents

If specific registration documents are required to process the application, the Applicant will download the forms during the registration session. The forms are completed by the Applicant and submitted to the LRA for processing. Refer to the *Registration Documents* Section for additional details.

4.1.3.1.6 Application Submission

Applicant provided data is added to the Certificate Lifecycle Management Tool database, where an authorized LRA is queued to process the Certificate application.

4.1.3.1.7 LRA Authentication Method

The LRA will authenticate to the Client-authenticated SSL/TLS secured Certificate Lifecycle Management Tool, using a hardware-based LRA Certificate. The LRA Certificate must be valid and also configured in the Access Control List for the Tool. Refer to the *Application Approval* Section, where processing guidelines are provided. The LRA can only access application queues for which he or she is authorized and configured in the tool.

4.1.3.1.8 Application Processing

Before approving the application, the LRA will perform all verifications required based on the type of Certificate for which the Applicant has registered. Refer to the *Application Approval* Section where processing guidelines are provided. Refer to the *Initial Identity Validation* Section for details regarding validation of personal and affiliation information.

In the case where the Applicant is requesting a Component Certificate, the Applicant-generated CSR is included in the application record in the Certificate Lifecycle Management Tool database and is automatically utilized for Certificate Issuance.

4.1.3.1.9 Activation Code Distribution

Following approval of the application, the Activation Code is generated by the Certificate Lifecycle Management Tool and distributed to the Applicant in one of the following methods:

- Via email to the applicant's verified email address; or
- Letter sent via regular mail or courier to applicant's verified home or business address.

4.1.3.1.10 Hardware Device Fulfilment

If a hardware Certificate has been requested, the device will be shipped to the Applicant for use during Certificate Retrieval. In this processing method, the hardware device will never contain any key material or Certificates; only FIPS certified hardware, based on the Certificate type requested, is provided to the Applicant. The Applicant will choose the hardware device password that protects the keys and certificates on the device.

4.1.3.1.11 Authentication to the Secure IdenTrust Retrieval Website

The Applicant accesses the Client-authenticated SSL/TLS Secure IdenTrust Retrieval website. The Applicant inputs the Account Password that he or she chose during registration and the LRA-provided Activation Code. Following validation of both codes the automated retrieval process is initiated.

4.1.3.1.12 Key Generation and Certificate Request

The Applicant utilizes the automated IdenTrust Key Generation and Certificate request retrieval process.

Keys are generated in the storage device during a secure SSL/TLS session and the Certificates are subsequently uploaded to the Applicant storage mechanism, as described in detail in the *CA Actions During Certificate Issuance and Private Key Delivery to Subscriber* Sections.

The Applicant installs the Certificates and encryption key pair by downloading them into his or her Certificate store (for software-based certificates) or the IdenTrust provided Cryptographic Module (for hardware-based certificates).

Once an Applicant has been issued a Certificate(s), he or she is referenced as a Subscriber.

4.1.3.2 LRA Assisted Registration

In this model approval of applications is performed by the LRA(s) designated by the External RA, via an online Certificate Lifecycle Management Tool provided by IdenTrust. This model requires that a separate queue be set up in the IdenTrust secure online Certificate Lifecycle Management Tool to allow separation of the External RA applications from all other applications submitted to IdenTrust.

4.1.3.2.1 LRA Authentication Method

The LRA will authenticate to the Client-authenticated SSL/TLS secured Certificate Lifecycle Management Tool, using a hardware-based LRA Certificate. The LRA Certificate must be valid and also configured in the Access Control List for the Tool. Refer to the *Application Approval* Section where processing guidelines are provided. The LRA can only access application queues for which he or she is authorized and configured in the tool.

4.1.3.2.2 Data Input

The External RA designated LRA directly inputs the Applicant data into the secure Client-authenticated SSL/TLS IdenTrust Certificate Lifecycle Management Tool (Tool). See additional information under definition of *Client-authenticated SSL/TLS* in the *Glossary* Section.

4.1.3.2.3 Account Password

An Applicant-selected Account Password is not created during the initial registration process. Rather a random, system generated Security Code is provided to the Applicant to be used during the Certificate retrieval process. The Applicant will select an Account Password during the Certificate retrieval process. See additional information in the *Using a Security Code to Select an Account Password* Section.

4.1.3.2.4 Identification and Authentication

Identity-proofing is completed during the in-person session between the LRA and the Applicant. Refer to the *Authentication of Individual Identity* Section for more information about who is eligible to perform in-person identity proofing and the requirements for conducting the session.

4.1.3.2.5 Required Documents

All required forms will be completed during the in-person session between the LRA and the Applicant. Refer to the *Registration Documents* Section for additional details. The LRA is eligible to complete both the Part 1: Subscribing Organization Agreement form and the Part 2: In-Person Identification Form and must obtain a signed copy of the Subscriber Agreement from the Applicant.

4.1.3.2.6 Application Submission

Applicant-provided data is added by the LRA to the Certificate Lifecycle Management Tool database.

4.1.3.2.7 Application Processing

Following submission of the Applicant data, the LRA can immediately process the application or if necessary, will authenticate to the Client-authenticated Certificate Lifecycle Management Tool using a hardware-based LRA Certificate, at a later time. Refer to *Application Approval* Section, where application processing guidelines are provided. Refer to the *Initial Identity Validation* Section for details regarding validation of personal and affiliation information.

4.1.3.2.8 Activation Code Distribution

Following approval of the application, the Activation Code is generated by the Certificate Lifecycle Management Tool and distributed by the LRA to the Applicant in one of the following methods:

- In-Person;
- Via email to the applicant's verified email address; or
- Letter sent via regular mail or courier to applicant's verified home or business address.

The system generated Security Code is also distributed to the Applicant in a separate out-of-band delivery in the same manner as the Activation Code, unless delivered in-person. The Activation Code and the Security Code may not be provided to the Applicant in the same email or regular main or courier correspondence.

4.1.3.2.9 Hardware Device Fulfilment

If a hardware Certificate has been requested, the device will be either provided by the LRA during the in-person session or shipped to the Applicant to be used during Certificate Retrieval. In this processing method, the hardware device will never contain any key material or Certificates. Only FIPS certified hardware, based on the Certificate type requested, is provided to the Applicant. The Applicant will choose the hardware device password that protects the keys and certificates on the device.

4.1.3.2.10 Authentication to the Secure IdenTrust Retrieval Website

The Applicant accesses the Client-authenticated SSL/TLS Secure IdenTrust Retrieval website and authenticates to the site using the LRA-provided Activation Code and Security Code.

Following validation of this information, the Applicant is prompted to select an Account Password, after which the retrieval process is initiated and the Applicant generates his or her keys, downloads the Certificate and stores both in his or her Certificate store or Cryptographic Module as described in the next subsection.

4.1.3.2.11 Key Generation and Certificate Request

The Applicant utilizes the automated IdenTrust Key Generation and Certificate request retrieval process.

Keys are generated in the storage device during a secure SSL/TLS session and the Certificates are subsequently uploaded to the Applicant storage mechanism, as described in detail in the *CA Actions During Certificate Issuance* and *Private Key Delivery to Subscriber* Sections.

The Applicant installs the Certificates and encryption key pair by downloading them into his or her Certificate store (for software-based certificates) or the IdenTrust provided Cryptographic Module (for hardware-based certificates).

Once an Applicant has been issued a Certificate(s), he or she is referenced as a Subscriber.

4.1.3.3 CMS Managed Registration

In this model approval of applications for Hardware-based ECA certificates is performed by the LRA(s) designated by the External RA, via a CMS deployment. This model requires that a CMS (Card Management System) be installed at the LRA location. The CMS must also have the ability to communicate, via a secure mechanism direct with the IdenTrust CA. Keys generation is managed by the CMS, in combination with the IdenTrust CA. An IdenTrust API is the mechanism by which all secure channels between the CMS and the IdenTrust CA is managed.

4.1.3.3.1 CMS Implementation Components

This section defines the roles of each of the components required for a CMS deployment (EWS, CMS, API, and CA) and how these components interact and are used by the LRA during the Certificate issuance processes. The methods of authentication for each of these components are also described.

- **Employee Work Station (EWS)**: The designated workstation assigned to the LRA to access the CMS application and process certificate applications. The LRA authenticates to the EWS using a password-protected, hardware-based LRA digital credential.

  The Subscriber, assisted by the LRA, utilizes the smart card software application available through the EWS to select a PIN to protect the card, thereby signifying activation and acceptance of the keys and Certificate.

- **Card Management System (CMS)**: The CMS consists of a vendor-provided application and hardware that manages the issuance of a smart card to the Applicant. The CMS generates the private signing keys in a smart card and creates a PKCS#10 Certificate that is passed to the IdenTrust CA for processing.

  The LRA access the CMS application via the EWS and must authenticate using a hardware-based, password protected LRA Certificate. The Certificate must be active, configured in the CMS and associated with an LRA user role.

  The CMS also inserts the following into the smart card, using Secure Channel Protocol (SCP), which is a mechanism defined by GlobalPlatform to preserve a level of security on the communication channel between a card and an external entity. Legacy smart cards use the SCP01 based on DES cryptography, which is now deprecated by NIST. For all recently supported smart cards, the CMS utilizes SCP03 based on AES cryptography, which is recommended by the GlobalPlatform Card Specification.

  - Certificates issued by the IdenTrust CA,
  - Personally Identifying Information (PII)
  - Biometrics (if required)
  - Escrowed encryption keys generated by the IdenTrust CA (if not generated by the CMS)

The CMS hardware is used to imprint and personalize the card.

- **The Application Programming Interface (API)**: The API is developed and maintained by IdenTrust and might have variable functionality based on the CMS that is utilized by the External RA. Basically, the API manages the communications between the CMS and the IdenTrust CA, via a Server-authenticated SSL/TLS asynchronous secured session. Once the LRA initiates the Certificate request, via the CMS, the API must authenticate the request in one of two-ways, depending on the API configuration:
    - The request message is sent via port 443, using Hypertext Transfer Protocol over TLS/SSL (HTTPS);
    - The request message is digitally signed by the requesting CMS; or,
    - The session is authenticated by using a pre-configured API Key and Password.

  The API also communicates a request to the IdenTrust CA if encryption key escrow is required and encryption keys must be generated (no encryption PKCS#10 is generated by the CMS).

  The API manages the return of requested certificates and any keys generated by the IdenTrust CA, via the asynchronous session, including:
    - Confirmation information;
    - Certificates;
    - encryption keys (only if key escrow is configured and keys are generated by the CA); and
    - Certificate chain (if the CMS requested the chain).
- **The IdenTrust CA**: The IdenTrust CA performs the following functions:
    - Authenticates the Certificate request based configured protocol;
    - Issues Certificate(s) using provided PKCS#10 request;
    - Generates encryption keys, when encryption key escrow is required; and
    - Archives encryption keys, when encryption key escrow is required.

4.1.3.3.2 LRA Authentication Method

The LRA will use two-factor authentication to access the EWS and the CMS by presenting a hardware-based LRA Certificate and hardware password. The Certificate must be valid and in order to access the CMS, the Certificate must also be configured within the CMS and associated with a specific user role. Permissions are granted based on the user role. In this case, the user must be assigned an LRA role. See additional details in the *CMS Implementation Components* Section.

4.1.3.3.3 Data Input

The External RA designated LRA directly inputs the CMS application data. The application data is then stored for key generation and submission of certificate requests. If biometrics are required for the requested Certificate type, then the CMS is used to gather and store this data, as well.

4.1.3.3.4 Account Password

In this model, an Account Password is not generated or required, as Key Generation is performed by the CMS and/or the IdenTrust CA and Certificates are passed from the IdenTrust CA via a Server-authenticated asynchronous SSL/TLS secured session managed by the installed API. All Certificate lifecycle events are managed through the CMS and not the Secure User Certificate Management Tool; therefore, an Account Password is unnecessary.

4.1.3.3.5 Identification and Authentication

Identity-proofing is completed during the in-person session between the LRA and the Applicant. Refer to the *Authentication of Individual Identity* Section for more information about who is eligible to perform in-person identity proofing and the requirements for conducting the session.

4.1.3.3.6 Required Documents

All required forms will be completed during the in-person session between the LRA and the Applicant. Refer to the *Registration Documents* Section for additional details. The LRA is eligible to complete both the Part 1: Subscribing Organization Agreement form and the Part 2: In-Person Identification Form and must obtain a signed copy of the Subscriber Agreement from the Applicant. It is also allowable for the information contained in required forms to be integrated into the CMS process and database, in lieu of using paper agreements.

4.1.3.3.7 Application Submission

Applicant-provided data is added by the LRA to the CMS database. When the electronic certificate request is processed, the IdenTrust Certificate Lifecycle Management Tool database is also updated.

4.1.3.3.8 Application Processing

The LRA reviews all identity credentials and approves the application. The LRA initiates the key generation and Certificate request process via the CMS.

4.1.3.3.9 Activation Code Distribution

No Activation Code is generated or distributed as the CMS will manage key generation and certificate issuance.

4.1.3.3.10 Hardware Device Fulfilment

In this model, the smart card is populated with the private keys and certificates through the CMS as described below in subsection Key Generation and Certificate Request. Only FIPS certified hardware, based on the Certificate type requested, is provided to the Applicant. Once key material and certificates are inserted into the card (along with any required biometrics) the LRA will assist the Applicant in activating the card and selection of the smart card password that protects the keys and certificates on the device.

NOTE: In the situation where credentials are to be inserted on a FIPS approved card that is currently assigned to a Subscriber, the insertion of any new credentials must be done in the presence of the LRA, to ensure that the card is always in possession of the Subscriber.

4.1.3.3.11 Authentication to the Secure IdenTrust Retrieval Website

In this model, this step is not applicable.

4.1.3.3.12 Key Generation and Certificate Request

In this model, the LRA initiates the key generation and Certificate request process via the CMS and an IdenTrust provided API used to establish an asynchronous Client-authenticated SSL/TLS session between the CMS and the IdenTrust CA. Refer to the *Key Generation via the CMS* Section for a detailed description of this process.

4.1.3.3.13 Activation Code Distribution

In this model, there is no Activation Code required, as the key generation and Certificate issues is managed through the CMS and API.

Once an Applicant has been issued a Certificate(s), he or she is referenced as a Subscriber.

4.1.3.4 Portal Registration

In this TA assisted model, a TA performs initial identity proofing and coordinates submission of the Certificate application with the Applicant. An IdenTrust LRA reviews and approves the Certificate application. An online Portal is utilized to upload data and artifacts and to facilitate communication between TAs.

4.1.3.4.1 Prerequisite Tasks – TA Registration

As a prerequisite to submission of a bulk load, a TA (or, in the case of a Trusted Agent, 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. IdenTrust registers a ECA Medium Token Assurance Certificate or an ECA Medium Hardware Assurance Certificate to each TA for authentication of his or her digital signature upon submission of 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 TAs 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 LRA). Following this issuance, IdenTrust Confirms in writing that the TA has been duly appointed by his or her employer. IdenTrust then adds the thumbprint of the TA's Certificate to an Access Control List for TAs.

4.1.3.4.2 TA Authentication Method

In this model, the TA will authenticate to the secure portal using an ECA Medium Assurance Certificate which has been previously registered with IdenTrust. The TA is also assigned permissions that allow for submission of certificate applications on behalf of the Subscribing Organization with which the TA is affiliated.

4.1.3.4.3 Registration Authentication Method

Based on a TA issued invitation, the Applicant visits the Server-authenticated SSL/TLS secured IdenTrust Registration website and is directed to the proprietary registration page for the Certificate type desired by the Applicant. See additional information under the definition of *Server-authenticated SSL/TLS* in the *Glossary* Section.

4.1.3.4.4 Data Input

The Applicant provides all application data and payment information via a *Server-authenticated* SSL/TLS secured IdenTrust Registration website.

4.1.3.4.5 Account Password

The Applicant creates an Account Password which is used to facilitate key generation and Certificate retrieval after his or her application has been approved. See additional information in the *Account Password Generation and Reset* Section.

4.1.3.4.6 Identification and Authentication

The Applicant must meet with the TA who extended the invitation to apply for the Certificate and is authorized to conduct in-person identity proofing. The TA performing the in-person identity proofing must complete and sign the required identity form. The form must be submitted to IdenTrust, via the Portal in order for the Application to be processed. Refer to the *Authentication of Individual Identity* Section for more information about who is eligible to perform in-person identity proofing and the requirements for conducting the session.

4.1.3.4.7 Required Documents

The TA assists the Applicant with completion of the required forms and documentation. Once completed, the TA authenticates to the Portal and uploads the forms and any other registration artifacts to the associated Applicant record. The IdenTrust LRA is provided access to the application data and artifacts for processing. Refer to the *Registration Documents* Section for additional details about required forms. It is also allowable for the information contained in required forms to be integrated into the portal process and database, in lieu of using paper agreements.

4.1.3.4.8 Application Submission

The Applicant provided data is automatically added to the Certificate Lifecycle Management Tool database, where an authorized LRA is queued to process the Certificate application. The Portal application is able to access limited Applicant Registration information in the IdenTrust database, sufficient to facilitate the upload of Registration artifacts and to facilitate the distribution of Activation materials to the Applicants to whom the TA is associated.

4.1.3.4.9 LRA Authentication Method

The LRA authenticates to the Client-authenticated SSL/TLS secured Certificate Lifecycle Management Tool, using a hardware-based LRA Certificate. The LRA Certificate must be valid and also configured in the Access Control List for the Tool. Refer to the *Application Approval* Section where processing guidelines are provided. The LRA can only access application queues for which he or she is authorized and configured in the tool.

4.1.3.4.10 Application Processing

Before approving the application, the LRA must perform required verifications based on the type of Certificate for which the Applicant has registered. Once the application is approved, the Portal will be updated and the TA will be queued for further processing. Refer to the *Application Approval* Section where processing guidelines are provided. Refer to the *Initial Identity Validation* Section for details regarding validation of personal and affiliation information.

4.1.3.4.11 Activation Code Distribution

Following approval of the application, the Activation Code is generated by the Certificate Lifecycle Management Tool and made available to the TA with whom the registration record is associated. The TA is responsible to provide the Activation Code to the Applicant in one of the following ways:

- In-person;
- Via the Portal following applicant authenticated login to the Portal;
- Via email to the applicant's verified email address; or
- Letter sent via regular mail or courier to applicant's verified home or business address.

4.1.3.4.12 Hardware Device Fulfilment

If a hardware Certificate has been requested, the device will be provided to the Applicant by the TA for use during Certificate Retrieval. In this processing method, the hardware device will never contain any key material or Certificates. Only FIPS certified hardware, based on the Certificate type requested, is provided to the Applicant. The Applicant will choose the hardware device password that protects the keys and certificates on the device.

4.1.3.4.13 Authentication to the Secure IdenTrust Retrieval Website

The Applicant accesses the Client-authenticated SSL/TLS Secure IdenTrust Retrieval website. The Applicant inputs the Account Password that he or she chose during registration and the TA-provided Activation Code. Following validation of both codes the automated retrieval process is initiated.

4.1.3.4.14 Key Generation and Certificate Request

The Applicant utilizes the automated IdenTrust Key Generation and Certificate request retrieval process.

Keys are generated in the storage device during a secure SSL/TLS session and the Certificates are subsequently uploaded to the Applicant storage mechanism, as described in detail in the *CA Actions During Certificate Issuance* and *Key Pair Generation* Sections.

The Applicant installs the Certificates and encryption key pair by downloading them into his or her Certificate store (for software-based certificates) or the IdenTrust provided Cryptographic Module (for hardware-based certificates).

Once an Applicant has been issued a Certificate(s), he or she is referenced as a Subscriber.

4.1.3.5 Bulk Load Registration

In this model, an authorized TA compiles registration and identity proofing information and utilizes a predetermined bulk load template to submit one or more applications for a Certificate to IdenTrust for LRA review and approval.

4.1.3.5.1 Prerequisite Tasks – TA Registration

As a prerequisite to submission of a bulk load, a TA (or, in the case of a Trusted Agent, 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. IdenTrust registers a ECA Medium Token Assurance Certificate or an ECA Medium Hardware Assurance Certificate to each TA for authentication of his or her digital signature upon submission of 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 TAs 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 LRA). Following this issuance, IdenTrust Confirms in writing that the TA has been duly appointed by his or her employer. IdenTrust then adds the thumbprint of the TA's Certificate to an Access Control List for TAs.

4.1.3.5.2 TA Authentication Method

The TA will submit bulk load requests via signed email and will not access any IdenTrust registration system. As such, only enrollment of an individual in the ECA TA program is required.

4.1.3.5.3 Registration Authentication Method

The bulk Certificate request is digitally signed by the TA and the bulk Certificate request is submitted to IdenTrust via a signed and encrypted email, using his or her ECA Medium Token/ECA Medium Hardware Assurance Certificate. This ensures that the registration data is delivered in a secure manner to IdenTrust so as to preserve the confidentiality and integrity of the Applicant's data during transport.

4.1.3.5.4 Data Input

Upon receipt of the bulk Certificate request, an IdenTrust LRA reviews and validates the submission. Once validated, the LRA authenticates to the client-authenticated TLS/SSL secured Certificate Lifecycle Management Tool database and upload the data into the Tool. The applications are then queued for processing.

4.1.3.5.5 Account Password

An Applicant-selected Account Password is not created during the initial registration process. Rather a random, system generated Security Code is provided to the Applicant to be used during the Certificate retrieval process. See additional information in the *Using a Security Code to Select an Account Password* Section.

4.1.3.5.6 Identification and Authentication

The Applicant must meet with the TA who is responsible to submit the bulk Certificate request. The TA performing the in-person identity proofing must complete and sign the required identity form. The form must be submitted to IdenTrust, for the Application to be processed. Refer to the *Authentication of Individual Identity* Section for more information about who is eligible to perform in-person identity proofing and the requirements for conducting the session.

4.1.3.5.7 Required Documents

The TA will assist the Applicant with completion of the required forms and documentation. Once completed, the TA includes the forms and any other artifacts in the signed email as referenced in the *Registration Authentication Method* Section. Alternatively, the TA may submit the forms via mail or courier to IdenTrust for processing. Refer to the *Registration Documents* Section for additional details about required forms.

4.1.3.5.8 Application Submission

This step is not required. Refer to the *Data Input* Section for additional information.

4.1.3.5.9 LRA Authentication Method

The IdenTrust LRA will authenticate to the Client-authenticated SSL/TLS secured Certificate Lifecycle Management Tool, using a hardware-based LRA Certificate. The LRA Certificate must be valid and also configured in the Access Control List for the Tool. Refer to the *Application Approval* Section, where processing guidelines are provided. The LRA can only access application queues for which he or she is authorized and configured in the tool.

4.1.3.5.10 Application Processing

Before approving the application, the LRA will perform all verifications required based on the type of Certificate for which the Applicant has registered. Refer to the *Application Approval* Section, where processing guidelines are provided. Refer to the *Initial Identity Validation* Section for details regarding validation of personal and affiliation information.

4.1.3.5.11 Activation Code Distribution

Following approval of the application, the Activation Code is generated by the Certificate Lifecycle Management Tool and distributed to the Applicant in one of the following methods:

- Via email to the applicant's verified email address; or
- Letter sent via regular mail or courier to applicant's verified home or business address.

The system generated Security Code is also distributed to the Applicant in a separate out-of-band delivery in the same manner as the Activation Code. The Activation Code and the Security Code may not be provided to the Applicant in the same email or regular main or courier correspondence.

4.1.3.5.12 Hardware Device Fulfilment

In this model, if a hardware Certificate has been requested, the device will be shipped to the Applicant to be used during Certificate Retrieval. In this processing method, the hardware device will never contain any key material or Certificates. Only FIPS certified hardware, based on the Certificate type requested, is provided to the Applicant. The Applicant will choose the hardware device password that protects the keys and certificates on the device.

4.1.3.5.13 Authentication to the Secure IdenTrust Retrieval Website

The Applicant accesses the Client-authenticated SSL/TLS Secure IdenTrust Retrieval website and authenticates to the site using the LRA-provided Activation Code and Security Code.

Following validation of this information, the Applicant is prompted to select an Account Password, after which the retrieval process is initiated and the Applicant generates his or her keys, downloads the Certificate and stores both in his or her Certificate store or Cryptographic Module. After which the automated retrieval process is initiated.

4.1.3.5.14 Key Generation and Certificate Request

In this model, the Applicant utilizes the online, automated IdenTrust Key Generation and Certificate request retrieval process.

Keys are generated in the storage device during a secure SSL/TLS session and the Certificates are subsequently uploaded to the Applicant storage mechanism, as described in detail in the *CA Actions During Certificate Issuance* and *Private Key Delivery to Subscriber* Sections.

The Applicant installs the Certificates and encryption key pair by downloading them into his or her Certificate store (for software-based certificates) or the IdenTrust provided Cryptographic Module (for hardware-based certificates).

Once an Applicant has been issued a Certificate(s), he or she is referenced as a Subscriber.

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 the *Registrars* Section or by an authorized LRA.

For Certificates issued to Individual Subscribers, the Registrar or LRA examines the identification documents for the Applicant as specified in the *In-Person Authentication* Section. When Registrars perform this function, they sign the ID Form and forward it to an IdenTrust LRA or an External RA LRA for review and processing as explained in the *Registration Processes* Section.

For Certificates issued to Components, the Registrar or the LRA examines the identification document for the PKI Sponsor as specified in the *In-Person Authentication* Section. When Registrars perform this function, they sign the ID Form and forward it to an authorized IdenTrust LRA or External RA LRA for review and processing as explained in the *Registration Processes* Section. For the Component itself, the LRA examines the documentation as specified in the *Authentication of Component Identities* Section.

Specific processing requirements based on Certificate type are detailed in the following subsections of this CPS.

4.2.2 Approval or Rejection of Certificate Applications

The LRA 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:

1. Is complete and supported by required documentation; and
2. Consistent with the information contained in the application for the Certificate.

4.2.2.1 Application Approval

All applications must be approved by a designated LRA. There are three primary models for LRA Managed Approval depending on the RA deployment model:

- Approval by an IdenTrust LRA;
- Approval by an External RA with no CMS; or
- Approval by an External RA with a CMS.

The LRA may approve Certificate issuance if all required steps as detailed in the following sections of this CPS are successfully completed, as defined by the type of Certificate requested by the Applicant. Issuance of an IdenTrust ECA Certificate occurs once an application for that Certificate:

1. Has been approved by an authorized LRA;
2. The LRA provides activation materials (including a storage mechanism, when appropriate) in the form of a retrieval kit to the Subscriber; and
3. The Subscriber initiates the web-based retrieval process in accordance with the *Activation Code Distribution* Section.

Upon approval of the Certificate by the authorized LRA, activation materials are prepared and provided to the Subscriber use during Certificate issuance, as described in the *Generation of Activation Materials* Section.

4.2.2.1.1 Approval of Human Certificates

The LRA must successfully complete identification and authentication of applicant data prior to approving an application for a Human Certificate for issuance, per the requirements detailed in these Sections:

- *Method to Prove Possession of Private Key;*
- *Authentication of the Organization Identity;*
- *Authentication of the Individual-Organization Affiliation;*

- *Approval of Subscribing Organization Confirming Applicant Affiliation;*
- *Authentication of Individual Identity;* or
- *Validation of Authority.*

Once the Certificate application is approved the LRA will initiate actions to send activation materials to the Applicant per the *Generation of Activation Materials* Section.

4.2.2.1.2 Approval of Component Certificates

The LRA must successfully complete identification and authentication of applicant data prior to approving an application for a Component Certificate for issuance, per the requirements detailed in these Sections:

- *Method to Prove Possession of Private Key;*
- *Authentication of the Organization Identity;*
- *Authentication of the Individual-Organization Affiliation;*
- *Approval of Subscribing Organization Confirming Applicant Affiliation;*
- *Authentication of Component Identities;*
- *Authentication of Individual Identity; and*
- *Validation of Authority.*

Once the Certificate application is approved the LRA will initiate actions to send activation materials to the Applicant per the *Generation of Activation Materials* Section.

4.2.2.2 Application Rejection

The LRA will reject a Certificate application if:

1. One of the required steps as detailed in the *Application Approval* Section cannot be successfully completed;
2. The Applicant fails to respond or does not provide requested documentation within a reasonable timeframe;
3. Payment has not been received or other satisfactory payment arrangements have not been made; or
4. The LRA reasonably believes that issuance of the Certificate may create an unnecessary risk to the reputation of IdenTrust.

If a certificate request is denied, then IdenTrust will not sign the requested Certificate and the LRA will work with the Applicant in an attempt to resolve the problem.

4.2.3 Time to Process Certificate Applications

Because only thirty days may elapse between in-person identity confirmation and retrieval of a Certificate, LRAs will respond promptly to all Certificate applications and Certificates will be made available for retrieval by Applicants following completion of the steps listed in the *Certificate Application Processing* Section (provided that the Applicant promptly responds to a notice from an LRA 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, he or she must re-apply using the processes listed in the *Certificate Application Processing* Section. In this situation the Applicant will receive another Activation Code upon approval of his or her new application. The previous Activation Code will expire and is disabled to prevent any use or reissuance.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

4.3.1.1 Generation of Activation Materials

Certificate activation requires the delivery of activation materials to the Applicant that are used during the Certificate retrieval process. Activation during an in-person meeting with the Applicant and LRA is also permitted.

This section provides a description of the materials and methods that are required for Certificate activation. More detailed information is included in the *Registration Processes* Section.

There are multiple methods for providing the activation materials that will be used by the Applicant to retrieval an ECA Certificate.

4.3.1.1.1 Activation Materials for Online Issuance

In cases where the Applicant uses the Secure IdenTrust Retrieval website, the following activation material is provided:

- **Activation Code:** The unique, randomly generated Activation Code is created by the IdenTrust Certificate Lifecycle Management Tool and delivered to the Applicant in a secure manner. An Activation Code is always required for online retrieval.
- **Account Password:** The Applicant-selected Account Password is created during the online registration process. The Account Password is known only to the Applicant and is used in conjunction with the Activation Code to initiate the online retrieval process. The Account Password is also used by the Applicant/Subscriber to manage account and certificate lifecycle events
- **Security Code:** In the event that the Applicant information is not provided by the Applicant via the secure IdenTrust Registration website, such as through LRA/TA input or Bulk load submission, a unique randomly generated Security Code is created by the IdenTrust Certificate Lifecycle Management tool. The Security Code is provided to the Applicant via an out-of-band method and separate from the Activation Code. The Security Code is used in conjunction with the Activation code to initiate the online retrieval process. Additionally, during the retrieval session, the Applicant will be required to create an Account Password to be used by the Applicant/Subscriber to manage account and certificate lifecycle events.

4.3.1.1.2 Activation Materials for In-Person Issuance

In cases where a CMS model is used for key generation and Certificate issuance during an in-person session, there are no activation materials required. Refer to the *CMS Managed Registration* Section.

4.3.1.2 Certificate Issuance and Activation

Based on the registration method, following approval of a Certificate and distribution of activation materials, the Certificate is issued via one of the following models:

- Online Certificate Issuance; or
- In-person Certificate Issuance.

Processing nuances, based on the registration method are described in this section.

4.3.1.2.1 Online Certificate Issuance and Activation

4.3.1.2.1.1 Online Certificate Issuance with Confirmation of Account Password

For applications submitted via the IdenTrust online registration process as described in the *Certificate Application* Section, an Account Password is submitted by the Applicant at the time of online enrollment. The Account Password is hashed and stored in the database. At a later point, the LRA approves the application by verifying that the information, such as Subscriber name and Subscribing Organization, in the paperwork provided by the Applicant matches the information in the request. Then, the LRA provides activation materials to the Applicant using a verified piece of information from the application as an out-of-bound delivery method (e.g., physical address, email address or mobile phone). In order to retrieve the Certificate, the Applicant must provide the registration Account Password and the Activation Data provided by the LRA.

A retrieval kit may also be sent that includes a Cryptographic Module containing unique identifier (e.g., the manufacturer serial number) that is recorded in the Subscriber. 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 these Sections:

- *Method to Prove Possession of Private Key;*
- *Registration Processes; and*
- *CA Actions During Certificate Issuance.*

4.3.1.2.1.2 Online Certificate Issuance with Confirmation of Security Code

There are two scenarios where applications are not submitted by the Applicant via the Secure IdenTrust Registration website:

1. The application is submitted by an authorized External RA LRA directly into the RA System per the *LRA Assisted Registration* Section; or
2. The application is submitted by an authorized TA via a bulk load submission per the *Bulk Load Registration* Section

In these models, the Certificate is approved by an LRA and then activations materials are provided to the Applicant in person or by using a verified piece of information from the application as an out-of-band delivery method (e.g., physical address, email address or mobile phone). In these models, the Applicant has not yet selected an Account Password; therefore, the Applicant is provided with a Security Code that is used during the Certificate retrieval process. If the approval materials are not provided by the LRA in person, then the Activation Code and Security Codes must be provided to the Applicant in a separate communication channels.

Upon receipt of the activation materials, the Applicant accesses a Secure IdenTrust Retrieval website and is prompted to provide the Activation Code and the Security Code. Upon validation of these codes the secure system will prompt the Subscriber to choose an Account Password, after which the automated retrieval process is initiated.

4.3.1.2.1.3 Online Certificate Issuance and Activation Procedure – Human Certificates

The following procedure is representative of online Certificate issuance and activation for ECA Human Certificates.

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. In the case where the Applicant has not pre-selected an Account Password, the activation materials will also include a Security Code, which will be used during the Certificate retrieval process and will allow the Applicant to designate an Account Password.

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

1. The Subscriber initiates the Certificate retrieval by accessing the Secure IdenTrust Retrieval website provided by the authorized LRA, via his or her browser. In the resulting web session, the IdenTrust CA system authenticates itself to the Subscriber and encrypts all communication utilizing a Server-authenticated SSL/TLS secured encrypted channel verifiable by a Certificate issued by a distinct IdenTrust Certification Authority natively trusted in browsers;
2. The Subscriber authenticates 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 the *Account Password Generation* Section, or alternatively, the Security Code provided by the LRA as described in the *Using a Security Code to Select an Account Password* Section. In either case, both pieces of information are required for all Certificate retrievals by a Subscriber from IdenTrust;

a. In the case where a Security Code is used during the process, following validation of the required codes, the Subscriber is prompted to select an Account Password;

3. Upon authentication of the Subscriber to the Secure IdenTrust Retrieval Website and verification of approved status of the Subscriber's Certificate application and that no more than 30 days have transpired since in-person identity confirmation, the Subscriber may proceed with the retrieval;

4. The secure retrieval application assures that the Cryptographic Module used is approved hardware when ECA Medium Token and ECA 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, where encryption key escrow is required, IdenTrust performs key generation for encryption key, which is securely transported to the client, as described below in the *Private Key Delivery to Subscriber* Section. 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 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 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 the *Private Key Delivery to Subscriber* Section;

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 the 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 the Secure IdenTrust Retrieval Website and the Subscriber's client platform. Upon successful installation of the Subscriber's Certificates, both signing and encryption Certificates are published in IdenTrust's Repository; and

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.

4.3.1.2.1.4 Online Certificate Issuance and Activation Procedure – Component Certificates

For the issuance of a Component Certificate, the PKI Sponsor need only follow Steps 1 and 2 as stated above in the *Online Certificate Issuance and Activation Procedure – Human Certificates* Section. 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 as described in the *Online Registration* Section. The Certificate issuance process described in this section complies with the ECA CP and 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; and
5. IdenTrust has published the Subscriber's Certificates to the IdenTrust Repository.

4.3.1.2.2 In-Person Certificate Issuance and Activation

4.3.1.2.2.1 In-Person Certificate Issuance with In-Person Activation

For Certificates issued via a CMS, the application data is submitted by an authorized External RA LRA via a secure transmission using a CMS per the *CMS Managed Registration* Section, and the activation process is facilitated via the LRA through the validation of applicant data at time of card and Certificate activation.

This is accomplished through the EWS and CMS, whereby applicant data is provided at the time of Certificate activation, via an in-person session with an authorized LRA and inserted into the smart card. As gathering of application data and submission of the certificate request is done in real time, no activation data is required.

Card activation is accomplished according to the following procedure:

1. A local External RA LRA conducts in-person identity proofing and inputs registration data into the CMS.
2. The local LRA completes the Certificate request and issuance process;
3. After the smart card has been successfully produced by the CMS, the local LRA assists the Applicant in selecting a password to protect the smart card; and
4. Possession of the card is then transferred to the Applicant.

NOTE: Once an Applicant has been issued a Certificate(s), he or she is referenced as a Subscriber.

The binding processes between Subscriber, Certificate and Cryptomodule are more fully described in the *CMS Managed Registration* Section.

4.3.1.2.3 In-Person Certificate Issuance with Remote Activation

For Certificates issued via a CMS, the application data is submitted by an authorized External RA LRA via a secure transmission using a CMS per the *CMS Managed Registration* Section and the activation process is facilitated via the LRA through the validation of applicant data at time of card and Certificate activation.

This is accomplished through the EWS and CMS, whereby applicant data is input by the LRA and the Certificate is approved and issued through the CMS and inserted into the smart card. As gathering of application data and submission of the certificate request is done in real time, no activation data is required.

The binding processes between Subscriber, Certificate and Cryptomodule are more fully described in the *CMS Managed Registration* Section.

In this model, the LRA utilizes the CMS to produce the smart card, a second local LRA manages the creation of a temporary smart card password and a remote TA or LRA assists the Applicant with activation of the smart card. Registration and card activation are accomplished according to the following procedure:

1. A remote TA or LRA is pre-designated to assist with registration and card activation;
2. The remote TA or LRA conducts in-person identity proofing and provides a local External RA LRA with registration data and required artifacts;
3. A local LRA completes the Certificate issuance process as prescribed in the *In-Person Certificate Issuance and Activation* Section;
4. After the smart card has been successfully produced by the CMS, a second local LRA creates a temporary password to protect the smart card;
5. The first local LRA sends the smart card to the pre-designated, requesting TA or LRA via courier or other secure means;

6. The second LRA send the temporary password for the smart card to the Applicant via an out-of-band method, such as secure email or other IdenTrust-approved method and separate from the smart card.
7. The remote TA or LRA receives the smart card;
8. The Applicant receives the temporary card password;
9. The remote TA or LRA provides the smart card to the Applicant and he or she uses the smart card utility software to select a new Applicant-provided password for the smart card; and
10. Possession of the card is then transferred to the Applicant.

NOTE: Once an Applicant has been issued a Certificate(s), he or she is referenced as a Subscriber. Lorraine

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 stated in the ECA CP Section 9.6.3 – *Subscriber Representations and Warranties,* and in this CPS in applying for, reviewing, and using the Certificate. The Subscriber is also required to request revocation when appropriate. In cases where the Applicant does not register for a Certificate via the online registration process, it is the responsibility of the LRA processing the application to obtain a signed Subscriber Agreement and to maintain the agreement according to archival requirements as defined in the *Retention Period for Archive* Section.

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 the *Publication of Certification Information* Section, 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 may not use his or her 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 may only use his or her 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.

These requirements are conveyed in the Subscriber Agreement that the Subscriber must accept during the registration process.

4.5.2 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; rather, a Subscriber may request certificate re-key for a Certificate that is due to expire per the *Certificate Re-key* Section.

OCSP Responder Certificates are renewed on a monthly basis as long as use of the corresponding key pair has not extended its usage period according to the *Certificate Operational Periods and Key Usage Periods* Section, 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 the *Primary Facility* and *Key Pair Generation* Sections.

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 the *Publication of Certification Information* Section, 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 identity validation performed for an earlier Certificate, the limits specified in the *Electronic Authentication of Individuals* Section will apply. Thus, the *notAfter* date field in a Certificate may not extend beyond the next in-person identity proofing date. This is restricted by the ECA system as also explained in the *Electronic Authentication of Individuals* Section.

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 LRA, 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 continue with the re-key request.

If confirmation of a new Certificate is based on the verification of a digital signature, per the *Electronic Authentication of Individuals* Section, the digital signature must 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 and authorized representative of the RA may request the re-key of a Subscriber Certificate.

4.7.3 Processing Certificate Re-Keying Requests

During the re-keying process, 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 the definition of *Client-authenticated SSL/TLS* in the *Glossary* Section)

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

During the subscription re-keying process, the Subscriber will complete the steps provided below. If the Subscriber successfully uses their Certificate to enter the Secure User Certificate Management Tool, he or she will complete the re-key online through an automated process. This process is completed when the Subscriber:

1. Checks to ensure that no information in the Certificate has changed;
2. Reviews and accepts the terms of the Subscriber Agreement; and
3. Makes arrangements to pay for the new Certificate.

If the Subscriber changes any information during the process, their re-key application will be submitted to and authorized LRA for manual review. If it is determined that the Subscriber has changed his or her name, affiliation,

or any data contained in the Certificate, the Subscriber must appear for in-person identity proofing and the re-key request cannot be completed. If the information is determined as minimal and is not information included in the Certificate, (such as a telephone number), the LRA may approve the re-key request. Upon approval, the LRA will 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 his or her Certificate or changes specific information, related to verification (can, organization affiliation, etc.) he or she must appear for in-person identity proofing and is not eligible for Certificate re-key.

Subscription re-keying is provided for ECA Medium Assurance Certificates, for ECA Medium Token Assurance Certificates, and for ECA Medium Hardware Certificates issued by IdenTrust.

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

Refer to the *Notification to Subscriber by the CA of Issuance of Certificate* Section.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Refer to the *Conduct Constituting Certificate Acceptance* Section.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Pursuant to the *Publication of Certification Information* Section, 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 the *Certificate Re-Key* Section.

4.8.1 Circumstance for Certificate Modification

Refer to the *Certificate Re-Key* Section.

4.8.2 Who May Request Certificate Modification

Refer to the *Certificate Re-Key* Section.

4.8.3 Processing Certificate Modification Requests

Refer to the *Certificate Re-Key* Section.

4.8.4 Notification of New Certificate Issuance to Subscriber

Refer to the *Certificate Re-Key* Section.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Refer to the *Certificate Re-Key* Section.

4.8.6 Publication of the Modified Certificate by the CA

Refer to the *Certificate Re-Key* Section.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to the *Certificate Re-Key* Section.

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 if any of the following events occur:

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:

- The private key corresponding to the public key listed in the Certificate has been compromised;
- 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;
- 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;
- 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
- 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 the *Procedure for Subscribing Organization Request Revocation Request* Section, upon compromise of an LRA or a TA, 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 the *Procedure for Subscriber*

or PKI Sponsor Submitted Revocation Request Section. 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;
- An authorized LRA;
- A Trusted Agent, the PKI POC or an official or supervisor within the Subscribing Organization listed in the Certificate;
- The TA 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 the *Circumstances for Revocation* Section. 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 Agent or other authorized individual in the Subscribing Organization, which is in a form specified by IdenTrust, then IdenTrust will revoke the specified Certificate.

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 or the External RA organization responsible for management of the Certificate, either directly or through a TA or PKI POC. Self-service revocation is available to the Subscriber through the Secure User Certificate Management Tool (to the Subscriber of a valid ECA Signature Certificate). Otherwise, a revocation request can be initiated through a digitally signed email to IdenTrust or to the authorized LRA of the Certificate is managed by an External RA. Contact information for IdenTrust is provided at www.IdenTrust.com/contact.

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 or her. The Cryptographic Module will be zeroized or destroyed promptly upon surrender and will be protected from malicious use between the time of surrender and zeroization or destruction of the module. The TA 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 subsequent procedures.

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 or the External RA 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 or the External RA, when request has validated 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 authorized LRA 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 the *CRL Issuance Frequency* Section. Information about a revoked Certificate will remain in the status information until the Certificate expires.

4.9.3.1 Procedure for Subscriber or PKI Sponsor Submitted Revocation Request

1. The Subscriber, PKI Sponsor or Subscribing Organization submits the revocation request according to one of the following processes:
    a. A Subscriber's revocation request must be communicated electronically to IdenTrust by either authenticating through the Secure User Certificate Management Tool 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;
    b. If the request is sent by email, then as a redundant measure, the request must also be submitted by contacting the IdenTrust Customer Support (contact information available at *https://www.identrust.com/contact*);
    c. Alternatively, if the Certificate is managed by an External RA, then an authorized LRA as designated by the External RA may assist with the revocation procedure;
2. The revocation request must include 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;
3. The IdenTrust or External RA LRA must validate the revocation request:
    a. In case where an email is submitted to the LRA, upon positive verification of the digital signature the LRA will revoke the Subscriber's IdenTrust ECA Certificate that was used to create the signature; or
    b. If the signature belongs to the PKI Sponsor who initially requested the Component Certificate according to the *Authentication of Component Identities* Section, 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; or
4. Upon positive confirmation the LRA will revoke the Subscriber's or Component Certificate(s) using the RA system.

4.9.3.2 Procedure for TA Submitted Revocation Request

In case the where a TA is involved in the revocation request, the following procedure is followed:

1. The Subscriber or PKI Sponsor submits a signed email to the TA or the PKI POC, the TA will:
    a. Verify the Subscriber or PKI Sponsor's signature;
    b. Ensure a revocation reason is provided;
    c. Collect and zeroize any hardware Cryptographic Module;
    d. Create a record; and
    e. Submit the request to IdenTrust Customer Support or the External RA LRA via a signed e-mail and phone call.
2. If the revocation request pertains to a Component Certificate, the TA or PKI POC will provide:
    a. The Subscriber's or PKI Sponsor's information;
    b. The domain name (Fully Qualified Domain Name for Component Certificates) of the Certificate(s) to be revoked; and
    c. A revocation reason.
3. The TA will attach the original signed request (from the Subscriber or PKI Sponsor) and digitally signs the message with his or her IdenTrust ECA Certificate and submits the request to IdenTrust Customer Service or External RA LRA.

a. For ECA Medium Token Assurance Level and ECA Medium Hardware Assurance Level Certificates, the request must also indicate whether the Cryptographic Module was returned and zeroized and include its serial number.

4. Upon receipt of the request, the IdenTrust LRA or External RA LRA will verify the following:
   a. TA's or PKI POC's digital signature;
   b. Confirm completeness of request information; and
   c. Ensure that the TA 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 TA appointment by the Subscribing Organization as detailed in the *TA Appointment and Removal Section.*
5. Upon positive confirmation the LRA will revoke the Subscriber's or Component Certificate(s) using the RA system.

4.9.3.3 Procedure for Subscribing Organization Requested Revocation Request

A Subscribing Organization should request revocation through its authorized TAs or PKI POC, if either one exists. The TA or PKI POC is responsible for authenticating requests from all requesters within the Subscribing Organization. The TA or PKI POC may confirm the identity of the requester using the method explained in the *Authentication of the Individual-Organization Affiliation* Section or by confirming a digitally signed email message submitted by the Requestor, using an IdenTrust ECA Certificate. revocation may be requested by a person with authority. The Requestor's authority is established by verifying a supervisory relationship of the Requestor 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.

Once the Requestor has submitted the revocation request to a TA or PKI POC, the procedures described in the *Procedure for TA Submitted Revocation Request* Section above.

In the event that the Subscribing Organization does not have immediate access to a TA or PKI POC (i.e., the TA 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 IdenTrust Customer Support, the External RA LRA, 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.

4.9.3.4 Procedure for Revocation of an LRA or TA Certificate

If a Certificate issued to an LRA or a TA is revoked because of a compromise, all Subscribers' Certificates that were directly or indirectly authorized for issuance by the person may be revoked by the IdenTrust ECA depending on when the compromise occurred. The decision to Revoke Certificates approved by an LRA or TA is at the discretion of the IdenTrust ECA and will be coordinated with the organization for which the LRA or TA is associated. Identification of the Subscribers affected by the revocation of an LRA Certificate is performed by querying the RA system about all the Subscriber Certificates authorized by the LRA since the compromise date. In the case of a TA Certificate being revoked, electronic records (i.e., bulk load spreadsheets or XML data structures) that hold the information related to requested Certificates will be reviewed to identify compromised Certificates. revocation of Certificates deemed to be compromised by the IdenTrust ECA is performed by an authorized LRA for each Certificate. The CRL reason code for the revocation will be populated with *KeyCompromise*. Returning Cryptographic Modules is not necessary since they will be reused to generate and store replacement Certificates.

4.9.3.5 Procedure for DoD Requested Revocation

IdenTrust maintains a list of individuals who are authorized by the DoD to request revocation of any Subscriber or CA Certificate. The list includes 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 to confirm the addition of such new liaison officer. 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).

revocation requests submitted by an ECA Liaison Officer should be directed to IdenTrust Customer Support. revocation support for the DoD is available on a 24x7 basis via telephone. If a Certificate needs to be revoked after-hours (nights, holidays, and weekends), then the person calling IdenTrust Customer Support should tell the person answering the phone that a Certificate must be revoked immediately. IdenTrust will then begin efforts to Confirm the requesting individual's identity, authority, and basis for requesting revocation of the Certificate.

Contact information for IdenTrust Customer Support is available at *https://www.identrust.com/contact*.

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. The IdenTrust Subscriber Agreement requires Subscribers to notify IdenTrust of the need for revocation as soon as it comes to the Subscriber's 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 the *Time Within Which CA Must Process the Revocation Request* Section.

4.9.5 Time Within Which CA Must Process the Revocation Request

IdenTrust processes all revocation requests within one hour of receipt. Revocations will be process according to the procedures described in the *Procedure for Revocation Request* Section and published to the CRL as described in the *CRL Issuance Frequency* Section.

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 secured website 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.

The 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 the *Key Pair Generation* Section. The OCSP Responder key will be held under strict controls as explained in the *Primary Facility* Section. The OCSP Responder Certificate is signed with the same CA key as the Certificate being validated.

The OCSP Responders will ensure that accurate and 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 the *CRL Issuance Frequency* and *On-Line revocation/Status Checking Availability* Sections.

4.9.12 Special Requirements Related to Key Compromise

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

See *Publication of Certificate Information*.

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 offers key escrow and key recovery services in accordance with the ECA CP. For additional details, refer to the IdenTrust *ECA Key Recovery Practice Statement* document available online at the *IdenTrust ECA Library,* under the "Policies – Current" section.

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 currently 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 production and backup Cryptographic Modules, is located in IdenTrust's primary facility located in Utah. Backup ECA equipment, excluding Cryptographic Modules are also located at the disaster recovery facility located in Colorado.

IdenTrust has three facilities dedicated to hosting CMA equipment:

- Primary Data Center in Utah;
- Operations Center in Utah; and
- Disaster Recovery Data Center in Colorado.

In selecting the appropriate facilities, controls have been designed to mitigate specific risks. IdenTrust's CA and CSA and the RA's server-side equipment are hosted in a primary facility that provides the highest-risk protection. IdenTrust's RA workstations are located in the Operations Center, which is 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.

5.1.1 Site Location and Construction

Physical security controls protecting the certification platform and Cryptographic Modules[15] 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

[15] Hardware Cryptographic Module private key storage practices are described in Section 6.2.2.

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 on the second floor and resides within an area without 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 metal fencing and slab-to-slab protection.

CA, CSA, and RA server equipment are protected by multiple layers of security. These include but are not limited to:

- Full-perimeter security fencing;
- 24x7 external and internal video surveillance;
- 24x7x365 monitoring of the facility, with co-location facility staff onsite during normal business hours;
- Dedicated facility staff are responsible for monitoring the facility outside of normal business hours and are available to respond to any issues that may arise;
- Mantraps at exterior doors;
- Secured roof access;
- Programmable electronic badge for exterior site access;
- Programmable electronic badge plus other authentication for data processing area access;
- Separate security system owned and maintained by IdenTrust for Secure Room access;
- Two-person, dual-factor authentication including biometrics for Secure Room access;
- Two-person authentication for access to the Secure Room safes holding CA cryptographic modules; and
- Locked server cabinets.

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 on the first floor within an area without windows. The Secure Cage, housing IdenTrust equipment, is in the center of the data center floor away from the external walls.

Security pertaining to the CMA equipment in the disaster recovery center consists of a Secure Cage which is protected on all 6 sides by metal caging/fencing material. Video and motion protections are the same as for the primary site.

5.1.1.1.3 The IdenTrust's RA Site

RA Operations workstation 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 on the fourth floor of the building.

Multiple layers of security surround the RA client-side workstation equipment: Internal floor door with restricted access (proximity card controlled); and, RA Operations Room door with further restricted, card-based access.

5.1.1.1.4 External RA and LRA Facilities

In cases where RAs are external to IdenTrust, RAs and LRAs are obligated by contract and policy to host the RA System and LRA workstation equipment in a facility with controls that reduce the risk of unauthorized access to the equipment. Documentation of these controls is provided in the Registration Practices Statement (RPS) submitted by the External RA. Refer to the *External RAs* and *IdenTrust Policy Management Authority* Sections for more information regarding the IdenTrust PMA and RPS approval.

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 video surveilled grounds. The building entryways and passageways are also under continuous recorded video surveillance. The facility is actively monitored 24x7x365, with co-location facility staff onsite during normal business hours. Dedicated facility staff are responsible for monitoring the facility outside of normal business hours and are available to respond to any issues that may arise.

IdenTrust's co-location facility staff conducts daily physical security systems checks against unauthorized access. Additionally, the staff provides continuous (24x7x365) site monitoring and video surveillance. The co-location facility staff, also provides weekly records of both the physical checks that have been conducted and records of IdenTrust-related personnel entering the facility. Video surveillance is also available to IdenTrust Security Office staff upon request.

The co-location provider provides only space and physical security measures to IdenTrust, along with environmental protections such as power, water, heating/cooling, and fire suppression. The co-location facility staff does not have any access to the IdenTrust secure room where all of the items specified in the ECA CP Section 5.1.2 – *Physical Access* are located. Controls mentioned in the ECA CP Section 5.1.2 - *Physical Access* are performed by IdenTrust Trusted Roles personnel prior to leaving the secure room.

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 programmable electronic badges to enter through the external property gate and to enter the mantrap at the building entrance. The programmable electronic badge and PIN number are required to enter the building. Entry to IdenTrust areas within the building also requires the presentation of programmable electronic badge. Programmable electronic badge for IdenTrust personnel working in the building are granted upon authorization from IdenTrust Security Officers.

Co-location facility staff members are prohibited from permitting unknown or unauthorized persons to pass through 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 IdenTrust Operations Management.

Visitors to the facility are allowed within the fenced perimeter only with authorization from the guard in the control center after properly identifying themselves and the purpose for the visit. Also, visitors are allowed access to the IdenTrust data center based only on a pre-determined need, such as an audit review or customer visit. Visitors' identities must be verified; and they must sign an entry log. Only following these requirements, will an IdenTrust employee escort the visitor(s) into the IdenTrust space. IdenTrust visitors are not allowed to roam in any area of the facility without an IdenTrust escort; the facility has similar restrictions in place for visitors not related to IdenTrust.

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, with video retained for a minimum of 90 days. Only authorized IdenTrust Trusted Role employees are granted access to the Secure Room. In some instances, a visitor may also be authorized to enter the Secure Room. In those cases, the visitor(s) must be pre-authorized by the Head of IdenTrust Operations or the Security Office, must present valid identity at the co-location center's front desk, and must be given a visitor's badge to be worn visibly at all times. At no time is any single individual able to gain access to or be left alone in the Secure Room. Two approved IdenTrust Trusted Role employees will accompany any approved visitors or contractors at all times within the Secure Room and other non-public areas of the facility.

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, or exiting from it.

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 in tamper-evident bags and separate safes from activation materials. Cryptographic keys and activation materials are secured and can only be accessed by two individuals who serve in separate designated Trusted Roles. No single individual can access one or any of the ECA cryptographic keys under these controls.

All entry and exit from the Secure Room is logged with the respective date, time, and reason for access. The process for exiting the Secure Room requires that one of the Trusted Role employees will 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 offsite facility as described in the *Media Storage* Section.

IdenTrust 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 reviewed as needed.

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 programmable electronic badges to access the building, and those badges plus biometric identification to enter the data processing areas. Entry to IdenTrust-specific areas within the building requires separate two-factor authentication including biometrics, using a separate access control system owned and maintained by IdenTrust. Programmable electronic badges for personnel working in the IdenTrust-controlled areas of the building are issued upon authorization by the IdenTrust Security Officer.

The building is equipped with cameras that cover the general data processing area 24x7x365 that are continually monitored by data center hosting company personnel. The IdenTrust Secure Cage 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 Cage. Each Trusted Role employee's authorization is granted and preregistration in the Secure Cage security system is performed using the same procedures as listed in the *Primary Facility* Section, which recaps the procedures implemented for the primary facility's Secure Room. In some instances, a visitor may be authorized to enter the Secure Cage. In those cases, the visitor(s) must:

1. Be pre-authorized by the Head of IdenTrust Operations or the Security Office;
2. Present valid identity at the co-location center's front desk; and
3. 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 Cage. Two approved, Trusted Role employees must accompany any approved visitors or contractors at all times.

The following equipment is kept in the disaster recovery facility Secure Cage:

- CA, CSA, and RA server equipment is located inside locked computer cabinets within the IdenTrust Secure Cage. By policy, access to computer cabinet keys are for persons who serve in a Trusted Role and are pre-authorized by the Security Office and the CIO. The number of authorized persons is kept at a minimum necessary for proper maintenance of the system; and
- 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 the *Primary Facility* Section.

5.1.2.2 Physical Access to RA Operations room

RA Operations workstation equipment is located in a building separate from the CA site. The equipment is stored in a building not identified as IdenTrust in a publicly visible way. IdenTrust office space is 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 IdenTrust office areas 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 company's best-practices audits including WebTrust for Certificate Authorities.

IdenTrust personnel require programmable electronic badges to access the IdenTrust offices and the RA Operations Room. Programmable electronic badges for personnel working in IdenTrust's offices are granted upon authorization from IdenTrust Security Officers based on the employee's Trusted Role and needs to perform that role. Employees are prohibited from permitting unknown or unauthorized persons to gain access to the RA Operations Room. Authorization to enter must be obtained in advance from Operations Management. Visitors are allowed within the RA Operations Room after properly identifying themselves and their purpose for the visit. Visitors are not allowed to roam without escorts.

RA Operations equipment is located in an isolated and restricted-access RA Operations Room on the fourth floor of the building. Access is granted only to IdenTrust personnel with a business need for access. Multiple layers of security protect the RA Operations equipment:

1. External building doors that are locked outside of normal business hours with restricted access controlled by programmable electronic badges;
2. Internal floor doors are secured by mantraps, with restricted access controlled by programmable electronic badges; and
3. Access to the RA Operations Room is further restricted based on business need as described above.

All entry to the RA Operations 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 if it is (1) written down in a secure password utility, or (2) kept securely with the user and not at the workstation itself (such as in a wallet). Recording of passwords on Post-it Notes or in spreadsheets is forbidden. When not in use, modules are locked or under control of its primary user.

5.1.2.2.1 External RA and LRA Facilities

In cases where RAs are external to IdenTrust, RAs and LRAs are obligated by contract, the ECA CP and this CPS to implement physical Access Controls to reduce the risk of equipment tampering even when the Cryptomodules for the RA System and Cryptomodules for the LRA workstations are not installed or activated. LRA obligations also include memorizing and not writing down Activation Data for the Cryptomodules used to access LRA workstations, as well as locking or keeping them under control of their primary users when not in use. RA Administrators obligations include protecting Activation Data for the Cryptomodules used to access the RA System, as well as locking or keeping them under control of their primary users when not in use. These controls are documented in the Registration Practices Statement (RPS) submitted by the External RA. Refer to the *External* RAs and *IdenTrust Policy Management Authority* Sections for more information regarding the IdenTrust PMA and RPS approval.

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:

The facility has a single utility power feed with an oversize backup generator and redundant UPS's. The facility is located approximately ¼ mile from the power generating plant substation, and the power feed comes directly from the substation to the building over private land, so it is protected from events such as traffic accidents or upstream building failures. This setup is audited several times annually by third parties against industry standards, with no exceptions noted. In case of public power failures, a full battery backup and a diesel generator with a 4,000-gallon fuel tank for power redundancy are available. Redundant uninterruptible power supplies (UPS) provide temporary power for the facility and automatically activate the generator when a power failure is detected. The fuel tank can be refueled on the go for continuous service.

The power system is maintained on the following schedule:

- Physical inspections daily;
- Generator operation testing at least monthly;
- UPS preventive maintenance semiannually; and
- Generator preventive maintenance and with full-load end-to-end system testing at least annually.

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 multiple uninterruptable power supply systems, incorporating battery banks for instant load transfer, and diesel power generator for longer-term power requirements.

The generator can be refueled on the go for continuous service. The systems provide both secondary and tertiary power redundancy.

The datacenter where the Secure Cage 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%.

5.1.3.3 External RA Facility

Because External RA functions are typically enacted via secure online interaction with the IdenTrust CA, there are no specific requirements regarding Power and Air Conditioning imposed by IdenTrust and implementation of controls is at the discretion of the External RA organization.

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 approximately 18 inches 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 moisture detection cable is located below the floor and is capable of detecting the smallest amount of water and alerting the datacenter operations staff to the precise location of the potential leak.

The IdenTrust Secure Room fire suppression system is maintained by the facility, and provides non-liquid oxygen evacuation to stifle combustion.

5.1.4.2 Disaster Recovery Facility

In the disaster recovery facility, equipment sits on a 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. As such, the building is equipped with advanced fire response aspects including:

- Fire-retardant construction materials;
- Advanced chemical, smoke, and heat-based detection systems;
- Inergen (inert noble gas) fire suppression in the Secure Room;
- 24x7x365 monitoring by data center staff with fire control console/panel access; and
- 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 doors resistant to forcible entry.

A description of IdenTrust's disaster recovery plan in the event a disaster should occur is described in the *Business Continuity Capabilities After a Disaster* Section.

5.1.5.2 Disaster Recovery Facility

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

- 24x7x365 monitoring by data center staff with fire control console/panel access;
- Dual action, pre-action dry pipe system;
- Certified computer room smoke detection system; and
- Doors resistant to forcible entry.

5.1.5.3 External RA Facilities

Fire prevention and protection controls that are implemented by an External RA organization are documented in the Registration Practices Statement by the External RA organization.

5.1.6 Media Storage

5.1.6.1 IdenTrust Controls

Sensitive ECA information (including audit and archive data) written to magnetic tape, hardware Cryptographic Modules, or other storage media, is stored at an offsite 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 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 written to digital media and stored offsite in locked containers that are physically separated from non-security data, and to which only the Security Office has access. As offline archives, they are not accessible for modification by any human or automated 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 items removed from or added 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 offsite 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 containing sensitive ECA information is locked in similar enclosures when not in use or when not in a clearly visible and attended area.

5.1.6.2 External RA Controls

Controls regarding media storage that have been implemented by an External RA organization are documented in the Registration Practices Statement by the External RA organization.

5.1.7 Waste Disposal

5.1.7.1 IdenTrust Controls

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 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 and occurs under IdenTrust Trusted Role supervision.

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 per the *Primary Facility* Section.

Hardware Cryptographic Modules remain in locked safes within the Secure Room; sensitive backup tapes remain in the offsite secure location’s vault prior to destruction. All Cryptographic Modules are zeroized after the keys stored in the Cryptographic Module 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.

5.1.7.2 External RA Controls

Controls regarding waste disposal that have been implemented by an External RA organization are documented in the Registration Practices Statement by the External RA organization.

5.1.8 Offsite Backup

5.1.8.1 IdenTrust Controls

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 offsite, hardened, secure, mountain storage vault described in the *Media Storage* Section.

At least annually, backup tapes are consolidated and archive media is identified and stored in the offsite storage vault described in earlier in this section and in the Section Media Storage to satisfy the 10.5-year data retention requirement. Every PKI related transaction is also backed up in near-real time to the backup database at the disaster recovery site.

Components needed to restore the ECA system are stored in separate areas of the secure vault facility, per the *Media Storage* Section. 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 with Trusted Role designation to access each mini-vault. Different groups are authorized to access different mini-vaults, 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. 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 pre-authorized by the CIO, are allowed to request data from the offsite storage facility. In cases where a request is made, the request is verified by a member of the Security office or the Head of IdenTrust Operations, who must be a different individual than the requestor. Two Trusted Role employees, upon confirmation of their identification, receive any delivery of PKI materials such as Cryptographic Modules and PED keys.

5.1.8.2 External RA Controls

Any controls regarding offsite backup that have been implemented by an External RA organization are documented in the Registration Practices Statement by the External RA organization.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

For the purposes of this CPS, all employees, contractors, and consultants of IdenTrust or authorized External RA organizations who have access to or control over ECA cryptographic operations that may materially affect the issuance, use, or revocation of Certificates, including access to restricted operations of ECA systems, shall be considered to be in a Trusted Role. Such personnel include, but are not limited to, LRAs, 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 per the *Number of Persons Required for Task* and *Roles Requiring Separation of Duties* Sections. 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 Head of IdenTrust Business Unit. 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 Head of IdenTrust Operations and the Security Office have an up to date copy of the list. This list will be made available during a compliance audit:

- CA Administrator;
- RA Administrator;
- LRA;
- System Administrator;
- Network Engineer;
- Security Officer;
- Software Engineer;
- Development Operations;
- Customer Support Representative; and
- Operations Management Personnel.

External RA organizations are required to document the description of all Trusted Roles in the External RA Registration Practices Statement, as well as to maintain a list of individuals who are selected to serve in a Trusted Role. Procedures to achieve these requirements are documented in the External RA organization's RPS document per the *External RAs* Section.

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 WebTrust Program for Certification Authorities, in compliance with the ISO 21188 *Public Key Policy and Practices Framework* standard. IdenTrust also performs Registration Authority functions. The responsibilities fall on a LRA) explained in the following section.

5.2.1.2 Registration Authority (RA) and Local Registration Authority (LRA)

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.

An LRA is a Trusted Role defined by this CPS. IdenTrust LRAs and External RA LRAs are required to comply with the practices pertinent to their functions in this CPS. LRA'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 TAs;
- 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 LRA 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 WebTrust Program for Certification Authorities, in compliance with the *ISO 21188 Public Key Policy and Practices Framework* standard.

5.2.1.3 Other Trusted Roles

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

5.2.1.3.1 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 offsite 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 WebTrust Program for Certification Authorities, in compliance with the *ISO 21188 Public Key Policy and Practices 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 LRAs per the *Number of Persons Required for Task* and *Roles Requiring Separation of Duties* Sections.

5.2.1.3.2 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 WebTrust Program for Certification Authorities, in compliance with the *ISO 21188 Public Key Policy and Practices Framework* standard.

5.2.1.3.3 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 the *Audit Logging Procedures* and *Records Archival* Sections; and
- Administrative functions such as compromise reporting.

5.2.1.3.4 Software Engineer

Software Engineers, also known as developers, have the following tasks:

- Build clean and efficient code based on user needs;
- Test software and debug for any issues;
- Collaborate with other developers, managers, systems personnel, and UX designers in building software;
- Identify and deploy software tools, systems, and components;
- Implement quality assurance standards;
- Write and update technical documentation; and
- Handle incident response and incident management.

As Software Engineer roles perform functions that can introduce security problems if not carried out properly, whether accidentally or maliciously, controls are in place requiring approval from the Security Officer or from Operations Manager roles prior to the execution of any tasks that bridge Software Engineer roles.

All such controls are audited annually by a third party auditor as part of the WebTrust Program for Certification Authorities, in compliance with the *ISO 21188 Public Key Policy and Practices Framework* standard.

5.2.1.3.5 Development Operations (DevOps)

DevOps roles have the following tasks:

- Build clean and efficient code based on user needs;
- Provide infrastructure and automation to support software development and deployment of applications;
- Coding to support process automation; i.e., infrastructure as code;
- Collaborate with other developers, managers, and technical operations;
- Identify and deploy software tools, systems, and components;
- Implement quality assurance standards;
- Write and update technical documentation; and
- Handle incident response and incident management.

As DevOps roles perform functions that can introduce security problems if not carried out properly, whether accidentally or maliciously, controls are in place requiring approval from the Security Officer or from Operations Manager roles prior to execution of any tasks that bridge DevOps roles.

All such controls are audited annually by a third party auditor as part of the WebTrust Program for Certification Authorities, in compliance with *the ISO 21188 Public Key Policy and Practices Framework standard*.

5.2.1.3.6 Customer Support Representative

Customer Support Representatives perform the following duties:

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

5.2.1.3.7 Operations Management Personnel

A list of IdenTrust's Operations Managers is kept at all times as approved and authorized by IdenTrust's the Head of IdenTrust Operations or the Head of the IdenTrust Business Segment. 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 Customer Support Representatives and IdenTrust LRAs;
- Acts as a custodian of the activation data for the Certificate that administers the Certification Authority software;
- Works closely with the Security Office to review requests for privileged information or sensitive system related requests; and
- Participates as an active member of the Risk Management Committee.

5.2.1.3.8 Trusted Agent (TA)

The identity of a TA is confirmed through the same steps used for issuance of an ECA Certificate to the TA at an assurance level equal to or higher than the Certificates for which the TA will act as Registrar per the *Who May be a Registrar* Section. This role is further described in the *Trusted Agents* Section.

5.2.1.3.9 PKI Point of Contact (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 per the *Authentication of Individual Identity* Section. This role is further described in the *PKI Point of Contact (POC)* Section.

5.2.1.4 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);
- Establishment and maintenance of system accounts and configuring audit parameters; and
- 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 the *Public Key Parameters Generation and Quality Checking* Section 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.

5.2.2 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 according to the *Roles Requiring Separation of Duties* Section 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.

Refer to the *Physical Access to CA, CSA Platforms* and *Private Key (n out of m) Multi-Person Control* Sections. 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 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 LRA, Security Officer, Customer Support Representative, or Operations Management.
- **LRA.** An LRA 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 LRA, Security Officer, Customer Support Representative, or Operations Management role.
- **Network Engineer.** The Network Engineer may not assume the LRA, Security Officer, Customer Support Representative, or Operations Management role.
- **Security Officer.** The Security Officer may not serve in the roles of CA/CSA Administrator, LRA, Systems Administrator, or Network Engineer.
- **Software Engineer.** Software Engineers may not assume any other roles.
- **Development Operations (DevOps).** Development Operations may not assume any other roles.
- **Customer Support Representative.** Customer Support Representatives may not serve in the role of CA/CSA Administrator, System Administrator, or Network Engineer.
- **Operations Management Personnel.** The Operations Management may not serve as CA/CSA Administrator, Systems Administrator, LRA, 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 can assume more than one identity in the system.

Additional Separation-of-Duties/Multi-Party Control and Split Knowledge information is addressed in the *Trusted Roles* Section.

5.2.4 Identification and Authentication for Each Role

The physical identity vetting of IdenTrust personnel in Trusted Roles is defined in the *Qualifications, Experience and Clearance Requirements and Background Check Procedures* Sections. Identification and authentication for logical and physical access to CA system resources is described in this section. In accordance with IdenTrust' security policies, IdenTrust's CA personnel must first authenticate themselves before they are:

1. Included in the access list for any component of the CA system;
2. Included in the access list for physical access to a component of the CA system;
3. Issued a Certificate for the performance of their Trusted Role;
4. Given an account on a computer connected to the CA system, or
5. Otherwise granted physical or logical access to any component of the CA system.

These access methods are:

1. Directly attributable to the trusted individual;
2. Password/Account Password protected; and
3. Not shared.

CA, CMS, RA and LRA equipment is configured with the minimum number of accounts necessary for operation of the equipment. The production environments containing the CSA and RA systems are remotely accessible under these controls: the CSA system requires the use of public/private key protocols such as SSH, and the RA system requires certificate-based access via a browser application. In all cases, data is encrypted from workstation to host.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience and Clearance Requirements

All personnel for any Trusted Role, as described in the *Trusted Roles* Section, are selected on the basis of loyalty to the United States, their trustworthiness and integrity. All IdenTrust Trusted Role employees are U.S. citizens. PKI POCs and TAs are not required to be U.S. citizens. While operating as an ECA, all CA Administrators must be under the direct control of IdenTrust. LRAs must be under the direct control of IdenTrust or an External RA.

External RA organizations must define the Trusted Roles that are deployed and indicate how the individuals who serve in Trusted Roles are selected and how they meet the requirements defined in the ECA CP and this CPS. The External RA RPS document is used to record this information per the *External RAs* Section.

ECA Operations are administered by the IdenTrust's Operations Management as identified in the *Certification Authority* and *Operations Management Personnel* Sections. 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;
- 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 the *Trusted Roles* Section, 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 results of background checks are reviewed by IdenTrust's Human Resource Department to confirm the results and follow up with the investigator 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. Background checks are kept confidential and are not released except as described in the *Privacy of Personal Information* Section and to the employee who is the subject of the background check at his or her request.

External RA Organizations must document background check requirements and processes used to perform background checks in the External RA RPS document per the *External RAs* Section.

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 or is otherwise 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. External RA organizations must document training requirements in the External RA RPS document per the *External RAs* Section.

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

The specific training required will depend on the equipment used and the personnel selected.

Depending on the type of training conducted, a record of the training is maintained in the online training tool, by the IdenTrust Security Office and/or the IdenTrust Human Resources Department.

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

5.3.3.1 CA Administrator:

Any employee serving in the CA Administrator role will maintain training 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.

5.3.3.2 LRA:

Any employee serving in the LRA role will maintain training in the following areas:

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

5.3.3.3 System Administrator:

Any employee serving in the System Administrator role will maintain training 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.

5.3.3.4 Network Engineer:

Any employee serving in the Network Engineer role will maintain training 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.

5.3.3.5 Security Officer:

Any employee serving as Security Officer or in the security auditing role will maintain training 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.

5.3.3.6 Software Engineer

Any employee serving as Software Engineer role will maintain training in the following areas:

- Security risk assessment and analysis;
- Security policies and guidelines;
- Logging and auditing;
- Physical security;
- Computer attack trends and vulnerabilities;
- Basic PKI and cryptosystems;
- Proper secure handling of sensitive customer information; and
- Trouble tracking software.

5.3.3.7 Development Operations (DevOps)

Any employee serving as DevOps role will maintain training in the following areas:

- Security risk assessment and analysis;
- Security policies and guidelines;
- Logging and auditing;
- Physical security;
- Computer attack trends and vulnerabilities;
- Basic PKI and cryptosystems;
- Proper secure handling of sensitive customer information; and
- Trouble tracking software.

5.3.3.8 Customer Support Representative:

Any employee serving in the Customer Support Representative role will maintain training in the following areas:

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

5.3.3.9 Operations Management Personnel:

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

5.3.4 Retraining Frequency and Requirements

Those individuals who serve in Trusted Roles must be aware of changes in IdenTrust's CMA operations. Any significant change to the IdenTrust CMA operation will require retraining of any individual acting in a Trusted Role that is impacted by the significant change. Through IdenTrust's change control process as described in the *Life Cycle Technical Controls* Section, an awareness plan is prepared for any significant change to the CMA system (e.g., a planned upgrade of CMA equipment or software). Depending on the type of training conducted, a record of the training is maintained in the online training tool, by the IdenTrust Security Office and/or the IdenTrust Human Resources Department.

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).

External RA organizations must document procedures in the External RA RPS to describe how retraining opportunities are identified and administered per the *External RAs* Section.

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.

External RAs should document any circumstances where Job Rotation is required in the External RA RPS document per the *External RAs* Section.

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, is subject to immediate removal 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.

External RA organizations must provide documentation in the External RA RPS per the *External RAs* Section describing how sanctions for unauthorized actions are managed and documented.

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 the *Personnel Controls* Section. 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.

If independent contractors are engaged by an External RA organization, that organization must provide documentation describing how such contractors are managed in the External RA RPS per the *External RAs* Section.

5.3.8 Documentation Supplied to Personnel

Personnel filling the roles of CA Administrator, LRA, System Administrator, Network Engineer, Security Officer, Customer Support Representative, and Operations Management will be provided documentation defining the duties and procedures of such roles.

External RA organizations must provide details in the External RA RPS document per the *External RAs* Section describing how documentation is provided to personnel involved in the PKI operation.

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.

In the case where CMA equipment operates in a virtual machine environment (VME), requirements in this section and sub-sections apply to both the host[16] and the hypervisor event logs.

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 these Sections:

- *Physical Controls*
- *Computer Security Controls*
- *Life Cycle Technical Controls*
- *Network Security Controls*

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.

[16] The various operating systems executing on a hypervisor are referenced by one or more of the following terms which are considered synonymous in this CP: host, virtual machine (VM), and guest operating system.

External RA organizations must provide documentation in the External RA RPS document per the *External RAs* Section describing how audit functions are conducted as prescribed by the ECA CP and this CPS.

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 the Secure Room/Cage and managed by the Security Office. The documents are converted to a digital medium to be included with the other digitally logged events described 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 audit requirements apply to trusted roles and CA, CSA, and RA equipment and any machines that are used to administer or manage the CA or CSA and any CMA equipment operated in a VME, including both the host and hypervisor. All of these machines are considered CMA equipment.

All security logs, both electronic and non-electronic, are retained in accordance with requirements of the *Retention Period for Audit Log* Section and will be made available during compliance audits.

Auditable Events
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.
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 • Identification of user attempting modification
Obtaining a third-party time-stamp
IdenTrust's system clock time is derived from multiple trusted third party time sources and used to establish various time-stamps. System time for servers providing CA, OCSP and CMS services is updated per the *Time Stamping* Section. Updates to the system time are logged and include at least the following information: • date and time • Host • Action performed • Entity performing the action (e.g., the internal time server)
IDENTITY PROOFING

Auditable Events
Successful and unsuccessful attempts to assume a role
The operating system and/or Certificate Lifecycle Management Tool automatically records: • date and time of attempted login • Username asserted at time of attempted login • Success or failure indication
The value of maximum authentication attempts is changed
The operating system records changes to the maximum authentication attempts allowed, including: • date and time • Type of event • Identification of user making modification. Changes in configuration files, security profiles and administrator privileges are all logged.
Number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login
Unsuccessful authentication attempts are automatically logged by the operating system, including when the pre-established maximum authentication attempts are exceeded. Logged data includes the following: • date and time of attempted login • Username asserted at time of attempted login When External RA LRAs utilize the IdenTrust Certificate Lifecycle Management Tool, LRA authentication attempts are also captured by the operating system.
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An administrator for end-user accounts would typically be a customer support representative. Requests to unlock accounts are captured in the IdenTrust operating system as the transaction occurs and includes: • date and time of event • Identification of account holder • Identification of the administrator An administrator for service account would be an individual serving in a System Administrator Trusted Role. Updates to unlock service accounts are automatically logged by the operating system and include: • date and time of event • Identification of account holder • Identification of the administrator
An Administrator changes the type of authenticator, e.g., from password to biometrics
Not applicable. IdenTrust does not change passwords to biometrics.
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
All data entry is associated with the local operator who has performed the data entry. All events added to the audit log indicate what data has been accepted into the production environment and the identity of the user who entered the data.
REMOTE DATA ENTRY
All security-relevant messages that are received by the system
The system logs security relevant messages that are received, including the following data: • date and time • Digital signature/authentication mechanism • Received message
DATA EXPORT AND OUTPUT

Auditable Events
All successful and unsuccessful requests for confidential and security relevant information
All application-based requests from end users for their own confidential information are authenticated and logged by the appropriate application. All such requests made by other means are manually or electronically logged by the IdenTrust Trusted Role employee receiving the information. All requests for individual information requested by someone who is not the owner of that information must be processed by IdenTrust Privacy Officers and handled on a case-by-case basis. Requests for security-relevant information requested by any individual who does not have a business-related need and authorization to obtain that information must be processed through the Security Team for consideration and handled on a case-by-case basis. All other requests for security-relevant information submitted using two-factor authentication are logged by the operating system or relevant application.
KEY GENERATION
Whenever the CA generates a key
This control is not mandatory for single session or one-time use symmetric keys. • The CA system automatically records all significant events related to CA operations, including key generation and Certificate signing • CA and CSA key generation ceremonies are scripted, recorded and artifacts are archived for audit purposes • RA key and Certificate generation events are automatically recorded by the CA system.
PRIVATE KEY LOAD AND STORAGE
The loading of Component private keys
A manual log of all physical access to production CA and CSA HSMs is maintained by IdenTrust. The log record includes at least the following data: • Action taken/task performed • date and time action was taken • Name of person(s) who performed the action A record of authorization to access HSMs is also maintained which specifies: • date and time • Reason for access • Name of person(s) authorizing access
All access to Certificate subject private keys retained within the CA for key recovery purposes
Access to Certificate Private Keys are automatically logged by the operating system, including at least the following data: • date and time • Messages between the CA and the requesting component • Indicator of success or failure of the action
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE
All changes to the trusted public keys, including additions and deletions
IdenTrust maintains a formal change management process, which requires that these types of changes are requested, authorized, and recorded. Additionally, additions and deletions of component public keys are automatically logged through the relevant service application.
SECRET KEY STORAGE
The manual entry of secret keys used for authentication

Auditable Events
Use of secret keys (PED Keys) for access to the CAs and CSAs' HSMs is recorded manually at the time of Cryptographic Key use. The manual log records at least the following data: • Action taken • date and time • Name of the person(s) who performed the action(s) Additionally, a record of authorization to access HSMs is also maintained which includes at least the following data: • date and time • Reason for access • Name of person authorizing access
PRIVATE AND SECRET KEY EXPORT
The export of private and secret keys
Keys used for a single session or message are excluded from this control. For end-entity private/secret key export, key generation and exportation occurs during the secure online Certificate retrieval process. The Subscriber must authenticate using a secret password provided by the Subscriber during certificate registration process, in conjunction with activation material provided by IdenTrust. The retrieval tasks are recorded by the operating system. Private and secret key export involving the CA's HSM take place in accordance with the principles stated in the *Roles Requiring Separation of Duties* Section. At the time of export, a record is made in a manual log which includes at least the following: • Action taken • date and time the action was taken • Name of person(s) who performed the action A record of access to HSMs are also maintained which includes at least the following: • date and time • Reason for access • Name of the person(s) authorizing access to the HSM
CERTIFICATE REGISTRATION
All certificate requests
All certificates are requested via online submission or via a direct interface. In all cases certificate requests are added to the operating system database and includes at least the following in the database record: • date and time of request • Type of event requested • Relevant request information • Disposition of request
CERTIFICATE REVOCATION
All certificate revocation requests
Subscribers or other authorized PKI Participants may also request revocation by contacting IdenTrust Customer Support for assistance. Following authentication of the requestor, the IdenTrust representative utilizes the operating system to execute the revocation. Additionally, any relevant information gathered by the IdenTrust representative used in the process of authenticating the requester, such as telephone and means used to authenticate the requester, are manually added as notes in the operating system record.
CERTIFICATE STATUS CHANGE APPROVAL
The approval or rejection of a certificate status change request

Auditable Events
All certificate status changes are initiated either automatically based on configured processing rules or through a Subscriber or LRA initiated change. In either case the transaction is logged by the operating system and will include at least the following data: • Identity of initiator of the status change • Message contents, source, and destination • Indication of success or failure of change
COMPONENT CONFIGURATION
Any security-relevant changes to the configuration of the CA
IdenTrust maintains a formal change management process, which requires that these types of changes are requested, authorized, and recorded, including but not limited to: • date and time of modification • Name of owner of modification • Description of modification • Build information (i.e., size, version number) of any modified files • Reason for modification
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
Requests for addition or deletion of roles and users is managed through an online ticketing system submitted by an authorized requester. Details relating to the request are recorded in the ticket. When the user is added, the transaction is recorded in the operating system a log record is created that includes at least the following information: • date and time • Type of even • Identification of the user making the modification
The access control privileges of a user account or a role are modified
Requests for modification of a user account or role is managed through an online ticketing system submitted by an authorized requester. Details relating to the request, including authorization and approval for the change are recorded in the ticket. Changes in configuration files, security profiles and administrator privileges are logged via the operating system. Change records capture at least the following data: • date and time • Type of change • Reason for modification • User making the modification
CERTIFICATE PROFILE MANAGEMENT (Including both CA and CSA)
All changes to the certificate profile

Auditable Events
All changes to certificate profiles are first documented in the IdenTrust ECA Certificate profiles document. The documented changes must be reviewed and approved according to established procedures before the certificate profile configuration can be made. Once approved, the profile changes are assigned via the internal ticketing system and to the individual(s) who is authorized to execute the change. Approved configuration changes are logged by the operating system which records at least the following data: • date and time • Type of change • Reason for the change • User making the requested change(s) The requester and Quality Assurance teams are required to confirm accuracy of the change(s).
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
Certificate profiles that are controlled by the ECA cannot be modified by IdenTrust. For changes to any OCSP or CRL profile that are controlled and maintained by IdenTrust, the procedures described above for *CA* and *CSA* apply.
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
All changes to the certificate revocation list profile are handled in the same manner as described above in *All changes to the certificate profile*.
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Appointment of individuals to a Trusted Role are the responsibility of the Head of IdenTrust Operations and are implemented under the direction of that individual. All nominees for a Trusted Role must meet the requirements stated in the ECA CP and this CPS. Trusted Role investigations are conducted and results are recorded by IdenTrust Human Resources and confirmed with IdenTrust Executive Management before appointment to a Trusted Role can be finalized. Artifacts retained by the HR department must include at least the following pertaining to each appointment: • Name of the appointee • Title of the delegated Trusted Role • date of the appointment • Signature of the authorizing member of the IdenTrust Executive team • A full list of all employees serving in Trusted Roles, and the Trusted Role in which he or she serves.
Designation of personnel for multiparty control
Stipulations defining functions requiring multi-party control and who is authorized to participate in those functions is incorporated into the Trusted Role designation and delegation process, as described above.
Installation of the Operating System
Installation of the Operating System must be authorized through the *Change Management* process described above. As a part of this process, at least the following information is documented: • Name of installation approver • date and time of server installation • Name of installer • Details of the installation process During the server installation, the automatic security auditing capabilities of the underlying operating system hosting the software are enabled.

Auditable Events
Installation of the CA
Installation of a CA must be authorized through the *Change Management* process as described above. As a part of this process, at least the following information is documented: • Name of installation approver • date and time of server installation • Name of installer • Details of the installation process During the CA installation, the automatic security auditing capabilities of the underlying operating system hosting the software are enabled. Any keys that are generated to support the CA installation are document and recorded according to the procedures as described above in the *Whenever the CA generates a key* section.
Installing hardware cryptographic modules
A list of HSMs is maintained and details at least the following: • Action taken (installing, removing, destruction, etc.) • date and time the action was taken • Name of individual who performed the action
Removing hardware cryptographic modules
Same as procedure describe above for **Installing hardware cryptographic modules**.
Destruction of cryptographic modules
Same as procedure describe above for **Installing hardware cryptographic modules**.
System Startup
The operating system's event log automatically captures the time of system startup.
Logon Attempts to CA Applications
Attempts to logon to CA, RA and CSA applications are automatically logged by the specific application. The log record includes at least the following data: • date and time of event • Type of event • Identity of user accessing the system • Indication of success or failure
Receipt of Hardware/Software
Receipt of hardware and/or software is recorded in a database that records at least the following information: • Hardware and software possessed • Whether licensed • Whether owned or leased
Attempts to set passwords
All attempts to set passwords used to access workstations are logged. The record contains at least the following information: • date and time of attempt • Identity of user attempting to set password • Indication of success or failure of attempt to set password On all CA, CSA, RA, and ECA equipment that uses password authentication:

Auditable Events

• All attempts to set passwords are logged.
• The record contains at least the following information:
  ▪ date and time of attempt
  ▪ Identity of user attempting to set password
  ▪ Indication of success or failure of attempt
System components not using passwords are authenticated via public/private key methodologies.
• Changes are logged by the operating system and include the information as described above.

Attempts to modify passwords
All attempts to modify passwords used to access workstations are logged. The record contains at least the following information: • date and time of attempt • Identity of user attempting to set modify password • Indication of success or failure of attempt to modify password
Backing up CA internal database
IdenTrust retains a backup log that includes at least the following information: • date and time of the backup event • Location of backup
Restoring CA internal database
IdenTrust retains disaster recovery records that include at least the following information: • date and time of restoration (tests or actual)
File manipulation (e.g., creation, renaming, moving)
The operating system automatically records at least the following information in the case of file manipulation: • date and time of modification • Identity of the local operator who created or last modified the file • Type of modification
Posting of any material to a repository
For CRL generation and publication to a directory, at least the following information is automatically logged: • date and time of CRL generation • DN of Issuing CA • Success or failure of publication of CRL For transactions or other material that is configured for posting to a repository, the operating system automatically logs at least the following information: • date and time of posting to repository • Transaction identifier • Indication of success or failure indication of posting
Access to CA internal database
The operating system automatically logs attempts to access the CA internal database and records at least the following information: • date and time of login attempt • Username asserted at the time of login attempt • Indication of success or failure of the login attempt
All Certificate compromise notification requests

Auditable Events
IdenTrust or External RA personnel who receive notification of Certificate compromise (such as Customer Support Representatives or LRAs) log the request and take appropriate action based on the veracity of the request. Information logged in the system includes at least the following: • date and time of compromise notification • Identity of person notifying of compromise, and verification of identity • Details of the notification • Identification of entity compromised • Description of compromise • Action taken
Loading tokens with certificates
When tokens (HSMs) are loaded with CMA certificates (CA, CSA, RA), a pre-established procedure is conducted that requires that record is logged that includes at least the following information: • Action taken (including transferring keys to or from and backing up the HSMs) • date and time action was taken • Name of person(s) who performed action A record of authorization to access HSMs is also maintained which specifies at least: • date and time of access to HSMs • Reason for access to HSMs • Name of person authorizing access to HSMs IdenTrust does not load KSMs with certificates.
Shipment of Tokens
KSMs shipped to end-users or to External RA organizations for distribution to end-users are never pre-loaded with credentials or private keys. For HSMs issued and shipped to CA, CSA and/or RA, the transaction is recorded with details including at least the following information: • Action taken (such as return, receipt, etc.) • date and time action taken • Name of person performing action • Reason for action • Shipping information
Zeroizing tokens
IdenTrust maintains a list of all HSMs. At least the following information is included in the list: • Action taken (including zeroization) • date and time action was taken • Name of person who performed action • Name and role of person authorizing the action IdenTrust maintains an inventory of KSMs used for end-entity certificates, but does not track zeroization of any KSM. Subscriber obligations, with respect to KSM destruction and/or zeroization, are described in the *IdenTrust Subscriber Agreement*.
Re-key of the CA

Auditable Events
CA, CSA, and RA key generation events are documented by scripted ceremonies are scripted, recorded and artifacts are archived for audit purposes includes: • Action taken/task performed • date and time action was taken • Name of person(s) who performed and witnessed the action A record of authorization to access HSMs is also maintained which specifies: • date and time • Reason for access • Name of person(s) authorizing access
CONFIGURATION CHANGES TO THE CA SERVER
Hardware
IdenTrust maintains a formal change management process, which requires that these types of changes are requested, authorized, and recorded. Following approval, changes are schedule and implemented according to the stipulations named in the Change Control approval.
Software
IdenTrust maintains a formal change management process, which requires that these types of changes are requested, authorized, and recorded. Following approval, changes are schedule and implemented according to the stipulations named in the Change Control approval.
Operating System
IdenTrust maintains a formal change management process, which requires that these types of changes are requested, authorized, and recorded. Following approval, changes are schedule and implemented according to the stipulations named in the Change Control approval.
Patches
IdenTrust maintains a formal change management process, which requires that these types of changes are requested, authorized, and recorded. Following approval, changes are schedule and implemented according to the stipulations named in the Change Control approval.
Security Profiles
IdenTrust maintains a formal change management process, which requires that these types of changes are requested, authorized, and recorded. Following approval, changes are schedule and implemented according to the stipulations named in the Change Control approval.
PHYSICAL ACCESS / SITE SECURITY
Personnel Access to room housing CA
Access to the Secure Room housing the CA is controlled. Procedural details are described in the *Physical Access* Section.
Access to the CA server
Access to the CA server is controlled. Procedural details are described in the *Physical Access* Section.
Known or suspected violations of physical security

Auditable Events
Any known or suspected violations of physical security are reported to the IdenTrust Security Team which is responsible to record the report and determine disposition. Details include at least: • date and time • Description of suspected event • Name of person reporting the event • Disposition and resolution
ANOMALIES
Software Error conditions
The application or the operating system, depending on the software and/or error will log the issue including at least the following information: • date and time of event • Description of the event
Software check integrity failures
The application or the operating system, depending on the software, and/or the integrity failure will log the issue including at least the following information: • date and time of event • Description of the event
Receipt of improper messages
The application or the operating system, depending on the type of message and the alert will log the issue including at least the following information: • date and time of event • Description of the event
Misrouted messages
The application or the operating system, depending on the type of the misrouted message will log the issue including at least the following information: • date and time of event • Description of the event
Network attacks (suspected or confirmed)
The Security Officer is responsible to record and investigate the details related to any network attack or suspected attack. The record should include at least the following information: • date and time of suspected event • Description of suspected event • Name of person reporting the event • Disposition and resolution
Equipment failure
Systems Administrators are responsible to record and investigate the details related to any equipment failure, and report their findings to the Security Office for logging. The log record should include at least the following information: • date and time of failure • Description of failure • Name of person reporting the failure • Disposition and resolution
Electrical power outages

Auditable Events
The Security Officer is responsible to create an incident report to record and investigate the details related to any electrical power outage. The record should include at least the following information: • date and time of outage • Description of outage • Name of person reporting the outage • Disposition and resolution The Systems Operations team is responsible to resolve the issue.
Uninterruptible Power Supply (UPS) failure
The Security Officer is responsible to record and investigate the details related to any UPS failure. The record should include at least the following information: • date and time of failure • Description of failure • Name of person reporting the failure • Disposition and resolution The Systems Operations team is responsible to resolve the issue.
Obvious and significant network service or access failures
The Security Officer is responsible to record and investigate the details related to any obvious and significant network service or access failure. The record should include at least the following information: • date and time of failure • Description of failure • Name of person reporting the failure • Disposition and resolution The Systems Operations team is responsible to resolve the issue.
Violations of Certificate Policy
The PMA Secretary is responsible to record the details related to violations of any Certificate Policy and request that the IdenTrust PMA review the report to determine appropriate action. The record should include at least the following information: • date and time of violation • Description of violation • Name of person reporting the violation • Disposition and resolution
Violations of Certification Practice Statement
The PMA Secretary is responsible to record the details related to violations of any Certification Practice Statement and request that the IdenTrust PMA review the report to determine appropriate action. The record should include at least the following information: • date and time of violation • Description of violation • Name of person reporting the violation • Disposition and resolution
Resetting Operating System clock
The operating system logging facility automatically records operating system clock resets. The log record must include at least the following: • date and time of reset • Description of the reset event • Name of the person executing the reset

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, a member of the Security Office 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 Office 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 the *Communication of Results* Section.

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 to archive on a monthly basis by IdenTrust's Security Officer in accordance with the *Protection of Audit Log* Section.

5.4.3 Retention Period for Audit Log

Audit log information as listed in the *Types of Events Recorded* Section is generated on IdenTrust's ECA equipment and kept on the ECA equipment until it is reviewed by an IdenTrust Security Officer, after which he or she will archive the information and prepare the archive data to be moved to IdenTrust's the offsite archive facility described in the *Offsite Backup* Section. 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

1. Ensure the integrity of the data; and
2. Ensure that the backup files are encrypted using the IdenTrust standard backup software.

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 media to offsite storage for archiving and EPMA audit purposes. The audit logs are stored within the offsite facility as described in the *Media Storage* Section.

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. Modification of the security audit log is restricted through access controls and operating system logging facility. The Security Officers have read-only access to the directories where the logs are maintained on the local servers. After offsite archiving, the local logs are deleted by authorized trusted personnel (i.e., the System Administrators and/or Security Officers). 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 the *Retention Period for Audit Log* Section.

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 the *Offsite Backup* Section. 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 at least each month in accordance with the *Retention Period for Audit Log* and *Protection of Audit Log* Sections, 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 as defined in the *Offsite Backup* Section ,in a separate, locked secure 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 in the *Protection of Audit Log* Section. The external audit collection systems are managed separately by the Security Officer in accordance with the *Retention Period for Audit Log* Sections. IdenTrust systems invoke audit processes at system startup, which cease only at system shutdown.

Manually collected audit information is gathered and stored by authorized personnel. 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 use its backup copies of security events that are stored on the hosts and on the systems logging server and thus does not need to manually cease all operations. When the separate audit security system capability is restored, the backup copies are integrated.

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 Office, 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 a member of the Security Office 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 the *Frequency of Processing Log* Section.

5.5 RECORDS ARCHIVAL

In the case where CMA equipment operates in a VME, requirements in this section and sub-sections apply to both the host and the hypervisor event logs.

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;
- CMA contractual agreements by which IdenTrust is bound;
- CMA system equipment configuration;

Data collected during CMA operation:

- Modifications or updates to any of the above items;
- Certificate issuance requests, revocation, suspension, restoration and key recovery requests and validation requests;
- Key recovery requestor identity authentication documentation as required by the *Identification and Authentication for Key Recovery Request* Section;
- Documentation of authority of the requestor, receipt and acceptance of recovered keys as required by the *Key Escrow and Recovery Policy and Practices* Section;
- Escrowed keys;
- Subscriber identity authentication documentation as required by the *Authentication of Individual Identity* Section;
- Documentation of receipt and acceptance of Certificates as described in the *Conduct Constituting Certificate Acceptance* Section;
- All Certificates and CRLs (or other revocation information) issued or published;
- Security audit data, as described in the *Types of Events Recorded* Section;
- Other data or applications sufficient to verify archive contents are archived; and
- All work-related communications to or from the EPMA, other CAs, and compliance.

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, and archived in three separate secure locations. 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.

Information may be transferred to other media if readability or usability of the data is in question; however, no transfer to new media will invalidate readability or usability. Host backups and archives are written using approved drives, media, and encryption tools. Encryption keys are physically separated from the backup archives.

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. IdenTrust will provide the EPMA with such data or information in a mutually acceptable format.

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 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 the *Offsite Backup* Section. 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 the *Disclosure Pursuant to Judicial or Administrative Process* Section.

Access to the offsite storage facility is strictly limited to authorized individuals and must be authorized by IdenTrust Operations management. IdenTrust maintains a list of the Trusted Role employees authorized to request retrieval of 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 offsite storage location, and access to the materials is further limited.

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 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 the *Offsite Backup* Section.

5.5.7 Procedures to Obtain and Verify Archive Information

Access to archive data is restricted to IdenTrust Trusted Role employees in accordance with the *Protection of Archive* Section. 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, the following steps will be taken to fulfill the request:

1. IdenTrust technical, systems and security personnel will identify the backup media on which the requested archive information is located.
2. The backup media will be ordered for delivery by a Trusted Role employee. Following validation of the order, the media will be securely transported from the offsite storage facility to the IdenTrust Security Office.
3. IdenTrust Security Office will sign and document the arrival of the requested archive media.
4. The IdenTrust Security Office will verify the integrity of the archived data in accordance with the *Protection of Archive* Section.
5. 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 in the *Retention Period for Archive* Section.

5.6 KEY CHANGEOVER

Key Changeover is facilitated with each Intermediate CA (ICA) rollover. The IdenTrust ECA offering consists of certificates offered to Subscribers issued with a validity period of up to 3 years. ICA are issued with a 6 year validity period.

Rollovers are timed to begin issuance off of the new ECA ICA at 3 years to avoid issuing truncated subscriber certificates. See table below:

YEARS					
1	**2**	**3**	**4**	**5**	**6**
ECA S22 and ECA S22 OCSP/CRL issuance*			ECA S22 rollover**		
ECA S23 and ECA S23 OCSP/CRL issuance*			ECA S23 rollover**		
*Issued with new keys			**Rollover at 3 years with same keys		

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.

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.

5.7.1.1 CA Key Compromise

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

- IdenTrust will immediately 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 immediately notify all affected parties (e.g., Subscribers, Subscribing Organizations, RAs, LRAs and TAs) of compromise via signed e-mail;
- IdenTrust will request that the Root ECA revoke IdenTrust's CA Certificates via signed email from the IdenTrust PMA, followed by a written letter 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 the *Method of Destroying Private Key* Section;
- After archiving data and prior to re-use, IdenTrust will purge all CA data storage devices in accordance with NIST Guidelines for Media Sanitization, NIST Special Publication 800-88 current revision. No media that contains or has contained sensitive information may leave IdenTrust control in a usable form.
- 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 LRA, TA, OCSP Responder and Subscriber Certificates. IdenTrust will follow established policies and procedure for re-issuance after revocation as described in the *Identification and Authentication for Re-Key After Revocation* Section (i.e., the procedures for initial issuance provided in the *Authentication of Individual Identity* Section*).*

5.7.1.2 OCSP (CSA) Key Compromise

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 the *Method of Destroying Private Key* Section;

- 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 four hours following the compromise of an OCSP Responder key.

5.7.1.3 LRA or TA Key Compromise

If a TA's or LRA's private key has been or is suspected to have been compromised:

- IdenTrust's Head of IdenTrust Operations, IdenTrust's Security Office and, in the case of a TA, 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 TA or the LRA 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 TA's or LRA'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 LRA or TA will generate a new key pair and IdenTrust will issue a new Certificate for the LRA or TA.

In case of the CA or CSA compromise or loss, the Security Office 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 Head of IdenTrust Operations. The Head of IdenTrust Operations and/or IdenTrust PMA will provide a summary of the final report to the EPMA.

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

IdenTrust performs tape backups on a daily basis. Backup tapes and backups of CA Cryptographic Modules are stored offsite in a secure location. In the event of disaster whereby both principal and backup CA operations become inoperative, IdenTrust's CA operations will be re-initiated on appropriate hardware using the backup copies. 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 the procedures outlined in the *Incident and Compromise Handling Procedures* Section.

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 addition, IdenTrust writes a copy of each database transaction to a backup database at the disaster recovery 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 the *Disaster Recovery Facility* Section and be recovered to the point of the last copied transaction. If needed, backup copies of the CA's signing keys per the *Private Key Backup* Section 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.
- 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. IdenTrust performs tape backups on a daily basis. Backup tapes and backup Cryptographic Modules are stored offsite 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 that has been stored offsite, 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 *nextUpdate* 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 the *Incident and Compromise Handling Procedures* Section and in the ECA Section 5.7.3 – *Entity Private Key Compromise Procedures*.
- 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 the *Compromise and Disaster Recovery* Section. The IdenTrust PMA or designee 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 the *Compromise and Disaster Recovery Procedures* Section.

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 the *Incident and Compromise Handling Procedures* Section. In this case, IdenTrust will notify all Subscribers and TAs 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 the *Retention Period for Archive* Section, 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 and External RA LRAs 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 and corresponding sections.

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

6.1.2 Private Key Delivery to Subscriber

Key generation and delivery to the Subscriber may be conducted using one of the following methods:

- Keys are generated via the online Certificate retrieval process
- Keys are generated by the CMS and/or the CA and injected onto a smart card

These processes are described in detail in the following subsections.

6.1.2.1 PKCS#10 Provided and Bound during Online Application

During the registration phase outlined in the *Information Collection* Section, the Applicant's information, PKCS#10, and hash of the Applicant-selected Account Password are bound together via the Server-authenticated SSL/TLS-encrypted transmission to the CA. Because only the hashed value of the password is stored, the value of the password is only known to the Applicant.

1. After the I&A process is completed, the IdenTrust LRA provides an Activation Code to the applicant through an out-of-band confirmed channel as described in the *Registration Processes* Section.
2. The Applicant-selected secret Account Password and Activation Code are used in combination by the Applicant to retrieve the Certificate during a Server-authenticated SSL/TLS-encrypted secured session as explained in the *CA Actions During Certificate Issuance* Section.

This is a common method for Subscribers of ECA SSL/TLS Certificates when providing a Certificate signing request during the application phase.

6.1.2.2 PKCS#10 Provided During Certificate Retrieval

Much like the process described above and outlined in the *Information Collection* Section, this method is similar except that the PKCS#10 is not created initially when the application is submitted to the CA via a Server-authenticated SSL/TLS-encrypted secured transmission.

1. After the I&A process is completed the IdenTrust LRA provides an Activation Code to the Applicant through an out-of-band confirmed channel as described in the *Registration Processes* Section.
2. The Applicant-selected secret Account Password and Activation Code are used in combination by the applicant to create the PKCS#10 request and retrieve the Certificate during a Server-authenticated SSL/TLS-encrypted secured session as explained in the *CA Actions During Certificate Issuance* Section.

In some cases, based on the registration model, an Applicant may choose his or her Account Password during the Certificate retrieval process. In this scenario, the Applicant is provided a Security Code which is delivered to the Applicant separately from the Activation Code. Both the Security Code and the Activation Code are required to initiate key generation and Certificate retrieval. The Applicant is then required to generate an Account Password to use for management of his or her Certificate. More details regarding this model are described in the *Account Password Generation and Reset* Section.

6.1.2.3 PKCS#10 Provided at Retrieval-Bulk Load Processing

1. When a Bulk Load Certificate application batch is submitted to IdenTrust, it is uploaded as described in the *Bulk Load Registration* Section, an IdenTrust LRA enrolls the Applicant and approves issuance of a Certificate to the Subscriber.
2. The Activation Code is generated and sent to the Applicant at a confirmed destination via out-of-band notification
3. Upon receipt of the out-of-band notification, the Applicant accesses a Secure-authenticated SSL/TLS session where he or she selects a secret Account Password. The Applicant then supplies the Activation Code provided by the LRA. Once these factors are authenticated, the public key is submitted to the RA/CA in a PKCS#10 and a Certificate is returned back to the Applicant during the same session.

6.1.2.4 PKCS#10 Submitted via CMS Request

For Certificate issuance using a CMS implementation, a PKCS#10 is also used. An IdenTrust PKI Consultant works with the RA or CMS Administrator during the system setup process to ensure that there is adequate binding between the Public Key and the Certificate Issued to the system. For additional information, refer to the *CMS Managed Registration* Section.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered to the CA in different methods, depending on the registration model used to apply for the Certificate.

A PKCS#10 file which binds the Private and public keys and is submitted to the CA during a Server-authenticated SSL/TLS-encrypted secured 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.

Alternatively, when an EWS/CMS registration model is used, a signed request is submitted via an API that facilitates secure communication with the IdenTrust CA. Upon validation of the request, the Certificate and keys are returned via the communication channel and inserted directly into the approved smart card.

Also refer to the *Key Pair Generation* and *Private Key Delivery to Subscriber* Sections for additional details regarding key generation and delivery processes using the online retrieval process or a CMS.

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.gds.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 that may be sent by IdenTrust to Relying Parties directing them to download the CA Certificate from a designated page located IdenTrust.com (at the website, 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. 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. Signatures on Certificates and CRLs that are issued by IdenTrust are SHA-256.

When generating SHA-256 digital signatures on Certificates, all their associated 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-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

When generating SHA-384 digital signatures on Certificates, all their associated CRL and OCSP responses are signed using the SHA-384 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-384	SHA-384	SHA-384	SHA-384	• Id-eca-medium-sha384 • Id-eca-medium-token-sha384 • id-eca-medium-hardware-sha384 • Id-eca-medium-device-sha384	• Id-eca-medium-sha384 • Id-eca-medium-token-sha384 • id-eca-medium-hardware-sha384 • Id-eca-medium-device-sha384

OCSP Responders shall sign responses using 2048 bit RSA and SHA-256 or stronger algorithms until 12/31/2030. After 12/31/2030, OCSP Responders shall sign responses using 3072 bit RSA and SHA-384 or stronger algorithms.

CMSs that sign content for PIV-I cards shall sign content using the SHA-256 hash algorithm

In all cases where Secure Socket Layer/Transport Layer Security (SSL/TLS) 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 adheres to the latest version of Transport Layer Security protocols as recommended by the browser community and/or industry ecosystem.

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.

6.1.8 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 and External RA LRAs 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 and corresponding sections.

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

6.1.8.1 Key Generation for Certificate Pair

All ECA Medium Assurance, Medium Token Assurance and Medium Hardware Assurance certificates are issued in certificate pairs-one signing certificate and one encryption certificate. A signing certificate will be generated based on the type of certificate that the Applicant has requested. IdenTrust has traditionally, issued the same type of encryption certificate as the requested signing certificate.

By March 31, 2021, the encryption certificate that is issued in the certificate pair will always be a Medium Assurance encryption certificate. By issuing a software certificate for encryption, the Subscriber can store the encryption in either software or hardware and the private keys are exportable, facilitating the ability for the Subscriber to create a backup copy of his or her encryption certificate. Additionally, if an encryption key recovery is needed, the keys can be exported to either software or hardware, which will enhance the end-user experience.

Following the implementation of this change, existing Medium Token and Medium Hardware Assurance encryption certificate types will be deprecated and no longer issued. IdenTrust will continue to support these certificate types until the Certificate has expired.

6.1.8.2 Key Generation via Online Certificate Retrieval

Procedural Overview

In this model the Applicant access the Secure IdenTrust Retrieval website to manage key generation and certificate issuance.

1. Following approval of a Certificate Application, a unique Activation Code is generated by the Certificate Lifecycle Management System and provided by the approving LRA to the Applicant.
2. The applicant authenticates to the Secure IdenTrust Retrieval website by providing the LRA-provided Activation Code and the Applicant-selected Account Password that was provided during the Certificate Application process. The retrieval application confirms that the Activation Code and Account Password are both associated with the same Certificate Application record.
3. Following authentication, the key generation and Certificate process is initiated.
4. Key generation is managed by the Secure IdenTrust Retrieval website application. The underlying Key Storage Provider performs a 2048-bit RSA Key generation.
    a. For Hardware-based certificates the Key Storage Provider is the actual FIPS approved smart Card or USB Token.
    b. For Software based certificates the Key Storage Provider depends on the Operating System; Windows CAPI Key store, and Apple Keychain for macOS.
5. signing keys are generated in the hardware device or in the browser certificate store, according to the type of Certificate purchased.
6. The signing certificate is added to the hardware device or browser store. signing keys are never stored by IdenTrust.
7. If key escrow is not active for the requested encryption certificate type, the encryption keys are also generated in the hardware device or in the browser certificates store, depending on the type of Certificate purchased.
    a. If key escrow is active for the requested encryption certificate type, the encryption key is generated on an HSM in the IdenTrust secure network, encrypted, and escrowed into the Key Escrow Database, then the encryption keys are added to the hardware device or the browser store.
8. Following installation of the certificates, the Applicant is then prompted to test the certificates to ensure that key generation and certificate download have been successfully completed.

Technical Overview

For Certificate retrieval via the Secure IdenTrust Retrieval website, on the client's side, an IdenTrust-written browser component (e.g., ActiveX control) manages the key generation and Certificate Issuance process. When the Applicant access the retrieval website and initiates the retrieval process, this browser component establishes a Server-authenticated SSL/TLS secured session which will remain open until keys and Certificates are returned.

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. Refer to the *Method to Prove Possession of Private Key* Section.

The encryption key pair, along with a symmetric 256 bit key (AES key), are generated on an IdenTrust-hosted, dedicated FIPS 140-validated hardware Cryptographic Module. If encryption key escrow is required, 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 and archived for future purposes. Additional details can be found in the IdenTrust *ECA Key Recovery Practice Statement* document available online at the *IdenTrust ECA Library,* under the "Policies – Current" section.

For Certificate retrieval, on the client's side, the IdenTrust-written browser component generates an RSA 2048 bit key pair. The browser component uploads the public key to the IdenTrust system over the Server-authenticated SSL/TLS secured session at the start of the retrieval process (refer to the *CA Actions During Certificate Issuance* Section) for more information. 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 the same Server-authenticated SSL/TLS secured 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 then 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.

Once this process is completed the Cryptographic Module's import function, supported through its application programming interface, is used to insert the encryption keys, and requested Certificates into the storage mechanism specific to the Certificate type requested.

Following completion of the import, 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.

6.1.8.3 Key Generation via the CMS

Once the LRA has confirmed all application data, he or she will use the CMS to initiate the key generation and Certificate request procedure as follows:

1. The CMS application utilizes the API to establish the asynchronous Client-authenticated connection
2. The CMS generates the signing keys in the smart card and a Certificate request in the form prescribed by RSA PKCS#10 is generated for the signature key.
3. If encryption key escrow is not required, then the CMS also generates the encryption keys and a separate PKCS#10.
    a. If key escrow is required the API manages the request to create for the escrowed encryption keys and Certificate.
4. The CMS then passes the PKCS#10 request(s), using a standard API and secure request/return exchanges to request and issue a Certificate. The Individual Subscriber's digital signature on the RSA PKCS#10 Certificate request(s) is verified using the algorithm specified in the request and the public key included in the request.
5. All data included in the Certificate request is added to the IdenTrust Certificate Lifecycle Management Tool database and associated with the Applicant record.
6. Following validation of the request, the IdenTrust CA issues the Certificates.
    a. If encryption key escrow is configured, then the encryption keys and PKCS#10 are generated by IdenTrust CA and then the encryption Certificate is issued.

7. The signing and encryption Certificates (and encryption keys, if generated by the IdenTrust CA) are then passed back to the CMS, during the same Server-authenticated SSL/TLS secured session as described in the *Private Key Delivery to Subscribe*r Section.
8. The Certificates (and encryption keys, if generated by the IdenTrust CA) are then inserted into the smart card and the Applicant, now Subscriber uses the CMS to select the smart Card password.
9. The smart card is provided to the Subscriber.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

Medium Assurance Software Certificates are stored in a Cryptographic Module validated as conforming to at least FIPS 140-2 Level 1 and Medium Token Assurance and Medium Hardware Assurance Certificates are stored in a hardware Cryptographic Module validated to at least FIPS 140-2 Level 2. Higher levels are available if desired. Hardware-based modules will not allow the user to export key pairs.

When a single cryptographic module has the private keys of more than one entity, the private keys are protected in a cryptographic module validated at FIPS140-2 Level 2 hardware or higher. When a single cryptographic module is controlled by a single entity and has multiple private keys for certificates of different types or with different DNs that have been issued to or provided to that entity by the PKI, this requirement does not apply.

The Subscriber of an IdenTrust ECA Certificate is the only individual who has access to his or her private signing key. Private encryption keys are only held by the Subscriber or parties authorized to request key recovery as described in the IdenTrust *ECA Key Recovery Practice Statement* document available online at the *IdenTrust ECA Library,* under the "Policies – Current" section. Key recovery requestors protect recovered keys as also described in the same referenced document.

TAs and all LRAs 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 Cryptographic Modules that have been validated as conforming to FIPS 140-2 Level 3 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 for Medium Token Assurance and Medium Hardware Assurance certificates.

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 one or more safes located in the IdenTrust Secure Room, which is under two-person control as described in the *Primary Facility* Section. The PIN Entry Device keys (PED keys) used to activate the Cryptographic Module are kept in separate safes also located 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 and 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.

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' CIO, a member of the Security Office, or a separate member of the Risk Management Committee, prior to accessing any cryptographic material. These logbooks are periodically audited in accordance with the *Frequency of Processing Log* Section.

For purposes of disaster recovery, two backups of the ECA signing key are maintained. One is secured in a separate safe within the Secure Room located in the primary facility and the other is in the offsite facility. To access either backup of the ECA signing key two-person controls are implemented as explained in the *Offsite Backup* Section.

Escrowed encryption keys are extracted from the Key Escrow Database (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 process description for key recoveries.

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 the ECA CP and the process description for key recoveries.

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

6.2.4 Private Key Backup

Medium assurance Subscribers may make backup copies (encrypted, protected by password) of their own encryption (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 the *Media Storage* and *Offsite Backup* Sections. 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 the *Private Key Escrow* Section and the IdenTrust *ECA Key Recovery Practice Statement* document.

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 the *Private Key Delivery to Subscriber* Section. As additional security, the private encryption key will be protected by the use of a Server-authenticated SSL/TLS secured session during the retrieval process as per the *Certificate Application Processing* Section.

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 the *Primary Facility* Section. The second backup copy is stored in the offsite facility described in the *Media Storage* Section. 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.

LRA 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 the *Cryptographic Module Standards and Controls* Section 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 the *Activation Data Generation and Installation* Section. 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 as described in these Sections:

- *Primary Facility*;
- *Key Pair Generation*; and
- *Private Key (n out of m) Multi-Person Control*.

The private key is activated by use of one of the PED keys.

6.2.9 Method of Deactivating Private Key

Subscribers, LRAs, and TAs are notified of their obligation to protect his or her keys by not leaving Cryptographic Module unattended or open to unauthorized access while active. Subscribers, LRAs, and TAs are required to deactivate the modules either by a manual logout or by configuring a passive timeout that will automatically force timeout.

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 the *Primary Facility* Section.

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 is provided to Subscribers via the Subscriber Agreement.

LRAs use Medium Hardware Assurance Certificates installed in appropriate Cryptographic Modules. LRAs 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 the *Cryptographic Module Standards and Controls* Section.

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 the *Key Changeover* Section, 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

6.4.1 Activation Data Generation and Installation

IdenTrust, its LRAs, 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 per the *Private Key Delivery to Subscriber* Section), 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.

LRAs and TAs are under obligation to maintain passwords that comply with the foregoing requirements. LRAs and TA 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.

LRAs and TAs 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. LRAs 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 the *Primary Facility* Section.) 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.

Where a single cryptographic module has the private keys of more than one entity, remote activation requires authentication commensurate with the assurance level of the Certificate of the key being activated.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

All CA, CSA, CMS, RA and LRA equipment will use a self-protecting operating system that prevents and detects attempts to alter it, or to disable its security functions. CA, CSA, CMS, RA and LRA equipment is configured and hardened using industry best practices and IdenTrust's system configuration guides. Procedures also pertain to those portions of the CA operating in a VME, and also pertain to the hypervisor. CA, CSA, CMS, RA and LRA equipment uses operating systems that require Individual I&A for authenticated logins, discretionary Access Control (including managing privileges of users to limit their assigned roles), Access Control restrictions that limit services based on authenticated identity, residual information protection, trusted path for I&A, security audit

capability, a protected audit record, self-protection, recovery mechanisms for Keys and system failure and process isolation. CA, CSA, CMS, RA and LRA equipment is scanned for malicious code on first use and at least weekly afterward.

CA, CMS, RA and LRA equipment is configured with the minimum number of accounts necessary for operation of the equipment. The production environments containing the CSA and RA systems are remotely accessible under these controls:

The CSA system requires the use of pre-configured SSH public/private key protocols. For these hosts, SSH is configured as follows:

- Version 2
- 2048 bit RSA
    - Ciphers: aes128-ctr,aes192-ctr,aes256-ctr
    - MACs: hmac-sha1,hmac-sha2-256,hmac-sha2-512
- Key exchange algorithms:
    - diffie-hellman-group14-sha256
    - diffie-hellman-group16-sha512
    - diffie-hellman-group18-sha512
    - diffie-hellman-group-exchange-sha256
    - ecdh-sha2-nistp256
    - ecdh-sha2-nistp384
    - ecdh-sha2-nistp521
    - curve25519-sha256

The RA system requires certificate-based access via a browser application.

In all cases, data is encrypted from workstation to host.

IdenTrust's Computer Architecture documents and equipment configurations are available for review on-site by external auditors and major customers upon request and under an appropriate nondisclosure agreement.

RA Systems (including CMSs) of Participant CAs and External RAs are required to be implemented as multi-server systems in a multi-tier network architecture. Such RA Systems consist of:

1. Aa web server layer,
2. An application layer,
3. An application database, and
4. A RA communication layer.

The web server layer is implemented in a DMZ network tier that is separated via a firewall receiving/sending network traffic from/to a public network (i.e., the internet). The application server layer and application database server are implemented in a secure network tier that does not directly receive any network traffic from a public network (e.g., internet). The RA communication layer is dedicated to communications between the application layer of the RA System and the IdenTrust CA. The RA Communication layer manages XKMS messages and the RA's Cryptomodule. The application layer hosts the functionality that supports the LRA and Applicant/Subscriber functions explained in the *Certification Authorities* Section. External RAs are obligated by contract and this CPS to implement and document computer security controls, in the External RA RPS document, that are compliant with this CPS.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

IdenTrust develops appropriate documentation establishing that PKI components are properly installed and configured, and operate in accordance with required technical specifications. This includes:

- Installation qualification plans, procedures/scripts/data, acceptance criteria, and results; and
- Operational qualification plans, procedures/scripts/data, acceptance criteria, certifications, and test results.

IdenTrust's PKI components have been designed and developed to meet applicable security standards for PKI systems. IdenTrust's design and development processes are sufficiently documented to support third party security evaluation of IdenTrust components and third party verification of process compliance, and on-going assessments to influence security safeguard design and minimize residual risk.

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 of remaining viable companies in the future. Controls ensure that 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.

CA, CSA, CMS, RA and LRA hardware and software PKI components are shipped directly to a Trusted Role Individual using shipping providers that have shipment tracking mechanisms allowing continuous tracking. Tracking information is provided to IdenTrust directly by the equipment vendor. Cryptomodules are received in tamper-evident containers. A Cryptomodule's shipment-specific information (e.g., serial number) is requested by IdenTrust in order to confirm the content when it is received. Other major PKI components (e.g., servers) are shipped under standard conditions. At reception, a chain of custody is maintained from that point forward and information provided by the vendor during the purchase order process is used to confirm the correct equipment has been received. From the point of the tamper-evident container being opened, Cryptomodules are maintained under multi-person control by Individuals in Trusted Roles.

IdenTrust develops some the PKI software components used to provide PKI services. Standard development methodologies are used. Strict quality assurance is maintained throughout the process and supporting documentation maintained. Development and test environments are maintained on separate servers in a separate network from the main operational (production) environment with appropriate segregation rights restricting developers and testers from having access to production equipment or operating environments. When open source software is used, it is selected focusing on specific functionality and goes through unit and integration testing on a controlled environment. Prior to use in production, the entire developed module goes through the standard change control process.

6.6.2 Security Management Controls

IdenTrust dedicates a PKI platform specifically to its PKI production operations including the CA, CSA, CMS, and RA System functions. IdenTrust utilizes VME for some functions. All VM systems operate in the same security zone as the CA. This includes server hardware, operating system software, Cryptomodules, PKI application software and the VME hypervisor. Non-PKI applications are not installed on production PKI platforms. Functionality for a given PKI's CA, CSA, CMS, and RA Systems, as well as databases, networking and physical housing is shared with other PKI systems.

IdenTrust maintains controls to prevent malicious software from being loaded. CA, CSA, CMS, and internal RA System platforms are protected by host-based intrusion detection systems that monitors file in the system to detect any unapproved changes and inform System Administrators, CA Administrators, and the Security Office, enabling them to correct the situation.

LRAs and TAs are required to take reasonable care to prevent malicious software from being loaded on their equipment. Only applications required to perform the RA function are loaded on an LRA's computer, and all such software will be obtained from sources authorized by local policy. Data on LRA equipment must be scanned for malicious code on first use and at least weekly afterward. Equipment updates must be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

IdenTrust has mechanisms in place to control and monitor the configuration of its CA, CSA, CMS, and internal RA Systems. IdenTrust installs its equipment and software in a controlled environment using a documented change control process. Software, when first loaded, is verified using file checksums provided by vendors at the file or file archive level.

Change control processes consist of a change control form that is processed, logged, and tracked for any changes to CA, CSA, CMS, RA Systems, firewalls, routers, software, and other Access Controls. File modifications are controlled through the change control process. In this manner, IdenTrust can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

Hashes for CA, CSA and CMS systems files are recorded upon installation and validated weekly thereafter as explained in the *System Development Controls* Section. Host based intrusion detection is utilized to detect changes to files. Notifications are monitored and are reviewed on a daily basis.

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 the *System Development Controls* Section.

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 the *System Development Controls* Section.

IdenTrust's TAs and LRAs 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

The IdenTrust Root is kept offline and turned on under controlled conditions only when necessary for signing of Sub-Certificates, Root OCSP Responder Certificates or CRLs. Subordinate CAs are connected to one network and protected against known network attacks. IdenTrust implements a multi-tiered network utilizing the principles of defense in depth, such as multi-tiered security and redundancy. This infrastructure is comprised of firewalls, proxy servers, intrusion detection systems and other devices. All CA, CSA, CMS, RA, and Repository computer systems are located in secure facilities behind the previously mentioned multi-tiered infrastructure. Firewalls are configured with a minimum number of accounts. Only services and protocols required to support CA, CSA, CMS, and RA functions are enabled. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols, and commands required for the trustworthy provision of PKI services by such systems. IdenTrust blocks all ports and protocols by default and open only the minimum necessary ports to enable CA, CSA, CMS, and RA functions. Any network software present on firewalls is required for their functioning. Any accounts, ports, or protocols added to firewall configurations is documented, authorized, tested, and implemented in accordance with the IdenTrust System Security Plan and other IdenTrust Policies and Procedures. IdenTrust's Network Technical Architecture documents and equipment configurations are available for review on-site by its auditors and major customers upon request and under an appropriate non-disclosure agreement. RAs and LRAs external to IdenTrust are obligated by contract, this CPS and the ECA CP to implement Network Security controls consistent with this CPS and the ECA CP.

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; and
- System audit journal entries.

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

7 CERTIFICATE AND CRL PROFILES

The IdenTrust ECA Certificate profiles document contains the formats for all certificates issued under the IdenTrust DOD ECA program.

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

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 general terms in the *Certificate and CRL Formats* Section and Certificate profiles that are defined in detail the IdenTrust ECA Certificate profiles document. The Certificate profiles listed in the IdenTrust ECA Certificate profiles document conform to the Certificate profile of the ECA CP. This CPS uses and incorporates here the Certificate profile of the ECA CP. The Certificate profiles in the IdenTrust ECA Certificate profiles document and the tables in the *Name Forms* Section provide details and clarification consistent with the Certificate profiles defined in the ECA CP. Any variances from ECA CP are in accordance with the RFC 5280 and have been approved the EPMA.

- End-Entity certificates always contain the Extended Key Usage extension and that extension does not contain the anyExtendedKeyUsage {2.5.29.37.0} OID.
- Extended Key Usage OIDs are consistent with key usage bits asserted.
- End-Entity certificates shall only contain Key Usage and Extended Key Usage that are intended for the Certificate and shall not contain any other Key Usage or Extended Key Usage.
- The '*KeyUsage*' extension is the only extension in IdenTrust-issued ECA Certificates marked as critical. This *Inhibit Any Policy Extension* Section notes some implications of that fact in relation to the Certificate Policies.
- Extended Key Usage is included in the signing Certificate, the encryption Certificate, and SSL/TLS Certificate.

See the IdenTrust ECA Profile document for additional details.

7.1.3 Algorithm Object Identifiers

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

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}

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 certifies only public keys associated with the crypto-algorithms identified above, and only uses 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 one of the following based on the type of Certificate:

- *subjectAltName:RFC822Name* (for Subscribers);
- *subjectAltName:uniformResourceIdentifier*;

- *subjectAltName:dNSName*; or
- *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.
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[17] appears before the colon.[18] The disambiguating number[19] described in the *Uniqueness of Names* section 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).

[17] 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).

[18] 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.

[19] The disambiguating number is also commonly known as and interchangeable with the term *globally unique identifier* (GUID).

Identifier type:	with data content of:	Indicates:
		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 the *IETF RFC 822* (now superseded by the *IETF RFC 2822*)	An e-mail address at which the Subscriber can receive messages via SMTP. A 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 the *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 the *IETF RFC 1630*.	The URL of the component or device identified in the Certificate.
subjectAltName:dNSName (in a Component Certificate) [20]	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 the *Authentication of the Individual-Organization Affiliation* Section; 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 as per the *Authentication of Component Identities* Section.

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.

[20] 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:
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
CommonName (CN)	The words "IdenTrust ECA" or "IdenTrust ECA S2" or "IdenTrust Component S2"[21]	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 the *Document Name and Identification* Section.

7.1.7 Usage of Policy Constraints Extension

Not Present.

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.

7.1.10 Inhibit Any Policy Extension

Not Present.

[21] The value of issuer:CommonName in a Certificate issued by IdenTrust (i.e., for SHA-256 "IdenTrust ECA S[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-256 "IdenTrust ECA S2[y]").

7.2 CRL PROFILE

7.2.1 Version Numbers(S)

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 the IdenTrust ECA Certificate profiles document, which are consistent with those of the ECA CP.

7.3 OCSP PROFILE

The IdenTrust ECA Certificate profiles document contains the formats for all certificates issued under the IdenTrust DOD ECA program.

The *Certificate and CRL Formats* Section and the IdenTrust ECA Certificate profiles document 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.

IdenTrust also requires that all External RA Organizations perform an annual audit against the External RA's current, IdenTrust PMA approved RPS document. An audit report recapping the audit results and any findings resulting from the audit must be submitted to IdenTrust for evaluation. The audit report must be prepared by a representative of the entity performing the audit of the External RA Organization.

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 datacenters, personnel controls, and operational risk management. The staff must be large enough to have the necessary depth and range of expertise required to audit IdenTrust's operations 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 the *ISO 21188 Public Key Policy and Practices Framework,* WebTrust Program for Certification Authorities, FPKI Audit Guidelines and/or a SOC 2 Audit guidelines.

8.2.1 IdenTrust's External Auditor Qualifications

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

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 this CPS as well as to the WebTrust Program for Certification Authorities and FPKI Audit Guidelines. Familiarity with these 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.

8.2.2 External RA Auditor Qualifications

The auditor selected by an External RA will evaluate controls that are stated in the IdenTrust approved RPS document created by the External RA and determine whether the External RA PKI operation is operating according to the stated controls.

The auditor must possess sufficient knowledge of the PKI function and other information security technologies and their secure operation.

The auditor must be trained to a standard generally accepted in the auditing field.

8.3 Assessor's Relationship to Assessed Entity

8.3.1 IdenTrust Auditor

As noted in the *Identity/Qualifications of Assessor* Section, 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. The auditor selected will be capable of providing an unbiased, independent evaluation of IdenTrust's compliance with this CPS.

8.3.2 External RA Auditor

The auditor, individual or audit group, may be a party that is external to the External RA organization or may be a party within the External RA organization that is sufficient removed from the RA PKI operation as to be objective. The audit party must have access to and/or the ability to view documentation and procedures stated as controls in the RPS document sufficient to assess compliance with such controls.

The External RA RPS document must state the qualifications of the selected auditor and describe the relationship of the auditor to the PKI operational team.

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 (Memorandum of Agreement) 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 the ECA CP Section 8.1 – *Frequency of Audit or Assessments*.

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

CAs and RAs must have either: (1) errors & omissions insurance and an employee fidelity bond, each with coverage limits of at least $10 Million U.S. Dollars; or (2) balance sheet equity on audited financial statements sufficient to self-insure such risks. IdenTrust maintains an equal amount of errors and omissions insurance coverage for its PKI-related operations.

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 described 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 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 the *Key Escrow and Recovery* Section. Subscribers and their organizations authorize IdenTrust to manage the escrowed private keys in accordance with the *Retention Period for Archive* Section.

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 website. This CPS is subject to change in the manner set out in the *CPS Approval Procedures* and *Amendments* Sections.
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 the *Subscriber Representations and Warranties* Section 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 as described in the *Circumstances for Revocation* Section, 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 the *Publication of Certification* Section.
8. Provide Repository services: IdenTrust will provide on-line Repository services that satisfy the obligations under the ECA Section 2.2 – *Publication of Certification Information*. 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; per the *Publication of Certification Information* and *CRL Issuance Frequency* Sections. IdenTrust also publishes notices of revocation via OCSP as described in the *On-line Revocation/Status Checking Availability* Section.

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 the *Authentication of Component Identities* Section, 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 the *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 Affiliated Organizations

Affiliated Organizations shall authorize the affiliation of subscribers with that organization, and shall immediately inform the ECA of any severance of affiliation with any currently affiliated subscriber.

9.6.6 Representations and Warranties of Other Participants

9.6.6.1 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 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 TA will operate in accordance with the applicable sections of the ECA CP and this CPS.

9.6.6.2 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 the *Access Controls on Repositories* Section.

9.6.6.3 Trusted Agent Representations and Warranties

A TA shall perform Subscriber identity verification in accordance with this CPS and the ECA CP.

9.6.6.4 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:

1. Providing to the EPMA a CPS, as well as any subsequent changes, for conformance assessment;
2. Conforming to the stipulations of the ECA CP and this CPS;
3. Ensuring that Certificate and revocation information is accepted only from valid ECAs; and
4. 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 the ECA CP Section 8.5 – *Actions Taken as a Result of Deficiency*.

9.6.6.5 PKI Point of Contact Representations and Warranties

A Subscriber Organization may appoint a PKI Point of Contact (POC) (e.g., a Trusted Agent, 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.

The *Dispute Resolution Provisions* Section 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 or improper use of a recovered key, if the Certificate was issued in accordance with the ECA CP and this CPS.

9.8.2 Other Exclusions

No stipulation.

9.8.3 U.S. 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., LRAs, TAs, etc.) assume financial responsibility for improperly used Certificates or improper use of a recovered key by the Subscriber or a third party requestor.

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://www.identrust.com/support/documents/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 secured website 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 the form "IdenTrust Claim Loss Form" downloadable from which is available for download at:

https://www.identrust.com/support/documents/eca

Instructions for completion and submission of the claim are included in the claim form.

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 the *Claims and Claim Determination* 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 CPS, including suits for judicial review of claims decided according to the *Claims and Claim Determination* Section.

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. Refer to the IdenTrust ECA Certificate profiles document for all detailed profile descriptions.

None of the certificates (including Root CAs), CRL or OCSP Responses that are valid beyond 31 December 2030 shall be signed using or contain 2048 bit or lower security RSA keys.

Certificates issued using profiles specified in the previous version of this policy may be used until expired. All new certificates shall conform to these profiles.

10.1 ENCODING DATES IN CERTIFICATES AND CRLS

notBefore and *notAfter* fields in certificates; the thisUpdate and *nextUpdate* fields in CRLs; and the revocation date in CRL entries shall be encoded using the following rules:

1. Dates through 2049 shall be encoded as UTCTime; and
2. 2. Dates from 2050 onwards shall be encoded as GeneralizedTime.

Invalidity date, a CRL entry extension is always encoded as GeneralizedTime. *producedAt*, a field in OCSP response is always encoded as GeneralizedTime.

10.2 SUBJECT PUBLIC KEY INFORMATION (SPKI)

The subject public key information shall contain one of the following values: 2048, 3072 or 4096 bit RSA using rsaEncryption {1 2 840 113549 1 1 1} algorithm OID.

10.3 CERTIFICATE POLICY OIDS

CA certificates and end entity certificates other than OCSP Responder certificates contain Certificate policy OIDs using the following rules:

1. Hardware, token, software or NPE OID is determined by the type of cryptographic module in which the subscriber private key is stored.
2. SHA-384 Certificate policy OID can be asserted in a Certificate if all of the following are true:
   a) Hashing algorithm used to hash the contents of the Certificate is SHA-384
   b) CA key pair used to sign the Certificate is 3072 or 4096 bit RSA
   c) Subject public key in the Certificate is 3072 or 4096 bit RSA

A Certificate shall never contain higher assurance Certificate policy OIDs than those determined using the above rules. A Certificate may contain lower assurance Certificate policy OIDs than those determined using the above rules. In order to maximize issuance flexibility, it is recommended that a CA Certificate contain the lower assurance Certificate policy OIDs than those determined using the above rules.

10.4 SIGNATURE ALGORITHM OIDS

A Certificate or CRL shall contain one of the following values for the signature algorithm OID:

1. Certificates and CRLs signed using 2048 bit RSA CA key pair are signed using SHA-256 hash and thus assert sha256WithRSAEncryption signature algorithm OID.
2. Certificates and CRLs signed using 3072 or 4096 bit RSA CA key pair are signed using SHA-384 hash and thus assert sha384WithRSAEncryption signature algorithm OID.

10.5 CERTIFICATE PROFILES

10.5.1 ECA Root CA Self-Signed Certificate

The profile for the ECA Root Certificate is as specified in the same Section 10.5.1 of the ECA CP.

10.5.2 Subordinate CA Certificates

The profile for the Subordinate CA Certificates is as specified in the same Section 10.5.2 of the ECA CP with the exception of the Subject DN which is defined by IdenTrust. Refer to the *Names Identifying the Issuer* Section, for interpretation of the other elements of this distinguished name and the IdenTrust ECA Certificate profiles document for details.

10.5.3 signing Certificate (Identity Certificate)

Refer to the IdenTrust ECA Certificate profiles document for details.

10.5.4 encryption Certificate

Refer to the IdenTrust ECA Certificate profiles document for details.

10.5.5 Subscriber Medium Hardware PIV-I Authentication Certificate

IdenTrust does not currently offer PIV-I Certificates under the ECA program; therefore, no profile is provided.

10.5.6 Card Authentication PIV-I Certificate

IdenTrust does not currently offer PIV-I Certificates under the ECA program; therefore, no profile is provided.

10.5.7 Component Certificate

Refer to the IdenTrust ECA Certificate profiles document for details.

10.5.8 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 "*codeSigning*" value as specified in the *IETF RFC 5280*; therefore, no profile is provided

10.5.9 Group/Role Signature Certificate

IdenTrust does not currently issue Group/Role Signature Certificates; therefore, no profile is provided.

10.5.10 Group/Role encryption Certificate

IdenTrust does not currently issue Group/Role encryption Certificates; therefore, no profile is provided.

10.5.11 Content signing PIV-I Certificate

IdenTrust does not currently issue PIV-I Authentication Certificates; therefore, no PIV-I Content signing certificate profile is provided.

10.5.12 OCSP Responder Certificate

As specified in the same Section 10.5.12 of the ECA CP.

10.5.13OCSP Responder (Not Self-Signed) Certificate

The profile for an OCSP Responder Certificate that is not self-signed is defined below:

Field Name	Critical[22]	Data Content Requirements	Significance
Version	n/a	v3 only (indicated by the integer (2)	Indicates the version of the *ITU-T X.509* to which the Certificate conforms.
Serial Number	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 Signature Algorithm	n/a	The subfield *algorithmIdentifier: algorithm* must contain the object identifier (specified in the ECA CP *Section 10.4 – Signature Algorithm OIDS* and the *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 Distinguished Name	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 the *Names Identifying the Issuer* Section. [Y] = Iteration of IdenTrust ECA CA S2, starting with zero (0) (e.g., ECA S20, ECA S21, etc.)
Validity Period	n/a	The subfields *notBefore* and *notAfter* contain dates in the form specified for UTC Time in the *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 the *IETF RFC 5280*. The Certificate validity time interval may be up to, but not greater than, one month.
Subject Distinguished Name	n/a	cn=IdenTrust S2 [Y] OCSP Responder ou=IdenTrust ou=IdenTrust[23] ou= ECA o=U.S. Government c=US	As specified in the *Names Identifying the Subscriber* Section.
Subject Public Key Information	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.

[22] "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.

[23] 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[22]	Data Content Requirements	Significance
Authority Key Identifier	No	The subfield *keyIdentifier* contains the 20-byte 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.
Subject Key Identifier	No	The subfield *keyIdentifier* contains the 20-byte 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.
Key Usage	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.
Extended Key Usage	Yes	It indicates *OCSPSigning* as specified in the ECA CP Section 10.5.12 – *OCSP Responder Certificate: id-kp-OCSPSigning* {1.3.6.1.5.5.7.3.9}	The Issuer CA designates authority to sign responses to this Certificate.
Certificate Policies	No	The *PolicyInformation:policyIdentifier* subfield contains all the policy OIDs for which the OCSP Responder is authoritative. These 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 {2.16.840.1.101.3.2.1.12.10} for Medium Hardware 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 the *Document Name and dentification* Section. See also the *Certificate Usage* Section.
Subject Alternative Name	No	A subfield as specified in the *Names Identifying the Subscriber* Section;	As stated in the *Names Identifying the Subscriber* Section.
No Check	No	*Id-pkix-ocsp-nocheck* {1.3.6.1.5.5.7.48.1.5} as specified in ECA CP Section 10.5.12 – *OCSP Responder Certificate*.	The CA specifies that an OCSP client can trust this responder for the lifetime of the responder's Certificate.

Field Name	Critical[22]	Data Content Requirements	Significance
		NULL	
Authority Information Access	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 the *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 = *http://apps.identrust.com/roots/identrustecas2[Y].cer*} [2] *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}	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.)

10.6 CRL PROFILES

10.6.1 ECA Root CA CRL

As specified in Section 10.6.1 of the ECA CP.

10.6.2 Subordinate CA CRL

CRLs have the content specified in the same Section 10.6.2 of 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 the *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-256 with RSA encryption. {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	Identifies IdenTrust as issuer of the CRL; see the *Names Identifying the Issuer* Section.

Field Name	Critical	Data Content Requirements	Significance
		according to the *Names Identifying the Subscriber* Section.	
thisUpdate	n/a	A date and time specified according to Section 5.1.2.4 of the *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 the *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 anticipate issuing an update to the CRL.
Revoked certificates list	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**
Authority Key Identifier	No	The subfield *keyIdentifier* contains the 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.
CRL Number	No	An integer.	The serial number of this CRL in an incrementally increasing sequence of CRLs.

10.6.3 OCSP Request Format

Requests sent to Issuer PKI OCSP Responders are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC 6960 for detailed syntax.

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 the *IETF RFC 2560*.
Requester Name	Not required	IdenTrust ignores this field i.e., treats it as insignificant.
Requester List	One or more request subfields, each identifying a Certificate by its CertID as defined in the *IETF RFC 2560*.	Indicates the Certificate(s) for which notification of validity is requested.
Signature	Not Required	IdenTrust ignores this field and does not verify the signature if any is present.
Extension	Not Required	IdenTrust will process a nonce when provided in the request.

10.6.4 OCSP Response Format

IdenTrust supports only the *responseType* specified as *BasicOCSPResponse* in the *IETF RFC 2560*. To be succinct, some ASN.1 layers present in the response and required by the *IETF RFC 2560* do not appear in the table below:

Field Name	Data Content Requirements	Significance
Response Status	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. 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 the *IETF RFC 2560*.
Responder ID	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.
Produced At	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*.
Signature Algorithm	Value per the Signature Algorithm OIDs Section.	
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 the Key Sizes Section.
Certificates	Applicable certificates issued to the OCSP Responder.	
Extensions	Blank or unused (no value specified)	IdenTrust does not support extensions in OCSP responses.
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 the *Key Sizes* Section.
List of Responses		

Field Name	Data Content Requirements	Significance
certID	A sequence of subfields as specified in RFC 2560.	Indicates the Certificate to which the related *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 expect to update the OCSP database used in generating responses.

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 the *Authentication of Individual Identity* Section.

11.1 IDENTITY PROOFING BY U.S. CONSULAR OFFICERS AND JUDGE ADVOCATE GENERAL 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 the *Identity Proofing by Authorized DoD Employees* Section.

11.1.1 Procedures for Identity Proofing for U.S. and non-U.S. citizens in Participant Countries

IdenTrust uses the steps outlined in the *Enrollment Process and Responsibilities* Section 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 IdenTrust In-Person Identification Form 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 process outlined in the *Documentation Review* Section is augmented by having the IdenTrust LRA 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 above.

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 the ECA CP Section 11.1.3 – *Participating Countries*. 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 the ECA CP Section 11.2 – *Identity Proofing by Authorized DoD Employees*. 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 same 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 website hosted by IdenTrust. The Applicant must provide the following information:

- Name,
- Address (if necessary for sending Cryptographic Module to applicant or billing purposes)
- Email Address,
- Citizenship(s),
- Organization Name,
- An Applicant-selected Account Password and password hint, and

- A payment form (e.g., Voucher, order number[24] or credit card)

During this secured 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:

1. Make a record of the Account Number/Application ID,
2. Print out the Subscriber Agreements,
3. Take the Account Number/Application ID and Subscriber Agreement with them to the identity proofing session with the authorized 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 same ECA CP Section 11.2.2 to perform identity proofing. As part of completing the steps in the *Identity Proofing Procedures to Be Used by Authorized DoD Employees for ECA Certificates* Section, 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 LRA 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 the *Process for Authorizing Issuance of ECA Certificates When Identity Proofing Is Performed by Authorized DoD Employees outside the U.S.* Section,
- 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 the *Participating Countries* Section, 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 the following sections:
    - *Registration Processes;*

[24] 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.

- *Private Key Delivery to Subscriber*; and
- *Private Key Transfer Into or From a Cryptographic Module.*

As well as directions for retrieving the Certificate(s) using the Secure IdenTrust Retrieval website - Server-authenticated SSL/TLS secured 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 the *CA Actions During Certificate Issuance* Section.

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 the *IdenTrust's Process for DoD Approved Certificates* Section.

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 same 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:

  https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

- Department of the Treasury regulations issued pursuant to the International Emergency Economic Powers Act (IEEPA), 50 U.S. Code 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/

11.2.4.1 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 D1135970. 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 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 AGENTS (TAS)

IdenTrust uses TAs who follow the steps outlined in the *Enrollment Process and Responsibilities* Section, 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 TAs shall apply to these TAs. Additionally, the TA must be a U.S. citizen unless the identity proofing is carried out in one of the Participant Countries, in which case, the TA must either be a U.S. citizen or a citizen of the country where the identity proofing is performed.

The TA performs the steps specified in the *In-Person Registration Procedure* Section, for in-person authentication of Subscribers. Applicants must present, and TAs 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 PIV-INTEROPERABLE SMART CARD DEFINITION

IdenTrust does not currently issue PIV-I cards under the ECA program. This section is not required.

13 REFERENCES

Incorporated by reference from the ECA CP Section 13 - *References*.

14 ACRONYMS AND ABBREVIATIONS

IdenTrust incorporates the same ECA Section 14 and includes other acronyms in the CPS as follows:

ACRONYM	DESCRIPTION
ADE	Authorized DoD Employee
AES	Advanced encryption Standard
AID	Application Identifier
APL	Approved Product List
CA	Certification Authority
CMA	Certificate Management Authority
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate revocation List
CSA	Certificate Status Authority
CSOR	Computer Security Objects Registry
DES	Data encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECA	External Certification Authority
ECDSA	Elliptic Curve Digital Signature Algorithm
EPMA	ECA Policy Management Authority
EWS	Enrollment Work Station
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	(U.S.)Federal Public Key Infrastructure
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
ID	Identity (also, a credential asserting an identity)
IP	Internet Protocol
ISO	International Organization for Standards
IT	Information Technology
JAG	Judge Advocate General
KEA	Key Exchange Algorithm
KED	Key Escrow Database

ACRONYM	DESCRIPTION
KES	Key Escrow System
KRA	Key Recovery Authority
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
LRA	Local Registration Authority.
MD	Maryland
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
POC	Point of Contact
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption and digital signature algorithm)
S/MIME	Secure Multipurpose Internet Mail Extensions
SCVP	Server-based Certificate Validation Protocol
SHA	Secure Hash Algorithm
TA	Trusted Agent
TLS	Transport Layer Security
UPN	User Principal Name
US	United States
USD	United States Dollar
UUID	Universally Unique Identifier
VME	Virtual Machine Environment
WWW	World Wide Web

15 GLOSSARY

The definitions in the same ECA CP Section 15 are incorporated into this CPS, unless the CPS provides a different definition.

TERM	DEFINITION
Applicant:	An individual who applies for a Certificate. Once the Certificate application has been approved and the Certificate and keys have been retrieved the individual is referred to as a Subscriber.
Authorized DoD Employee (ADE):	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. A representative of the Defense Information Systems Agency periodically provides a list of ADEs who are eligible to perform in-person identity verification services.
Card Management System (CMS):	The Card Management System (CMS) is a hardware device and digital credential management solution that is used to issue, manage, personalize, and support cryptographic smart cards and digital certificates for identity-based applications such as physical & logical access within an organization. The CMS submits requests to the IdenTrust CA via an API. The API authenticates to the CA either through a request message that is digitally signed by the requesting CMS or by authentication of an API Key and Password. The authentication method is determined when the CMS is deployed. All communications between the CMS and the CA are secured via Server-authenticated SSL/TLS. See the definition of *Server-authenticated SSL/TLS*, for additional details regarding current methods and protocols.
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.
Certificate Lifecycle Management Tool (Tool):	This is the term used to describe the secure online tool used by LRAs to manage certificate applications, approvals, revocations, suspensions, and other lifecycle events. The Certificate Lifecycle Management Tool utilizes a Client-authenticated TLS/SSL-encrypted session to secure all communications between the Certificate Lifecycle Management Tool and the CA. Users must authenticate to the system using an IdenTrust Certificate that is pre-registered in the application. User permissions are assigned and the ability to approve certificates is only granted to individuals who are granted LRA status.
Certificate Management Authority (CMA):	A Certification Authority or a Registration Authority.
Cipher Suite:	A cipher suite is a set of algorithms that help secure a network connection that uses Transport Layer Security (TLS) or its now-deprecated predecessor Secure Socket Layer (SSL). In addition, cipher suites can include signatures and an authentication algorithm to help authenticate the server and or client. Cipher suites supported by IdenTrust at the time of this CPS publication: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) preferred • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) preferred • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) preferred

TERM	DEFINITION
	• TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) preferred • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)
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 the *Claims and Claim Determinations* Section.
Client-authenticated SSL/TLS:	Transport Layer Security v.1.2 and higher are cryptographic protocols that use PKI to secure communications transmitted over the Internet. For Client-authenticated SSL/TLS sessions described in this CPS, the IdenTrust secure server sends it is 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. All procedures defined in this ECA CPS that specify the use of Client-authenticated SSL/TLS are subject to these requirements. Cipher suites currently supported by IdenTrust can be viewed in this *Glossary* Section under the term *Cipher Suite*.
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.
CRL (Certificate revocation List):	A list of Certificates that became invalid before they expired.
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*.
Disambiguating Number:	A unique number that is included in the *subject:CommonName* of an ECA Certificate. This number is also recognized by and interchangeable with the term *globally unique identifier* (GUID).

TERM	DEFINITION
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 the *IETF RFC 5280*.
Enrollment Work Station (EWS):	An Enrollment Work Station is the customer side computer application that interfaces with the CMS to accomplish Certificate registration.
General Data Protection Regulation (GDPR):	The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas.
Head of IdenTrust Business Segment:	The individual serving in an executive position who responsible to manage the IdenTrust Business Segment operating as IdenTrust, Inc. under which the IdenTrust ECA is operated.
Head of IdenTrust Operations:	The individual serving in an executive position who is responsible to manage all Operational departments and functions of the IdenTrust ECA.
IdenTrust:	IdenTrust Services, LLC, a Delaware limited liability company.
Individual Subscriber:	See *Subscribers* section. 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.
Local Registration Authority (LRA):	A Local Registration Authority is an Individual who collects and confirms Applicant identity information and any other information provided by the Applicant for inclusion in a Certificate. Local Registration Authority is more fully defined in the *LRA* Section.
Personally Identifiable Information (PII):	Personally Identifiable Information is any data that could potentially be used to identify a particular person. Examples include a full name, Social Security number, driver's license number, bank account number, passport number, and email address.
Public Key Infrastructure (PKI):	A Framework established to issue, maintain, and revoke public key Certificates.
PKI Point of Contact (PKI POC):	An individual who is designated as the point of contact for a Subscribing Organization and may provide instructions and/or act as a reference to IdenTrust or the External RA organization with respect to Certificate lifecycle events.
PKI Sponsor:	An individual who functions in the role of a Subscriber for a non-human system component.
RA Operations:	The generic term used to describe the group of IdenTrust personnel who are involved in process certificate applications and providing technical and customer support.
RA Operations Room:	The room in which RA operations are conducted by LRA and support personnel. This room is located within the IdenTrust office space. Access to the RA Operations Room is controlled by programmable electronic badge and is limited to IdenTrust employees who have a business need to enter the restricted space.
Registration Authority:	See *Registration Authorities (RA)*.
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

TERM	DEFINITION
	Registrar may be a Local Registration Authority, Trusted Agent, an employee of IdenTrust, or a notary in some circumstances; see *Who May be a Registrar*.
Registration Practices Statement (RPS):	The Registration Practices Statement (RPS) describes the registration practices of an External Registration Authority in performance of duties and obligations to fulfil the requirements of the IdenTrust Global Common Certificate Policy.
Repository:	A system for storing and retrieving Certificates or other information relevant to Certificates.
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.
Secure Cage:	The six-sided cage located within the datacenter utilized by IdenTrust for disaster recovery. The Secure Cage encloses backup CMA equipment. Access to the Secure Cage requires that two IdenTrust employees, who have been designated by IdenTrust to act in a Trusted Role, authenticate using two-factor authentication, such as programmable electronic badge and PIN or biometric validation.
Secure IdenTrust Registration Website:	This is the term used to describe the Server-authenticated SSL/TLS secured website that is hosted by IdenTrust, where Applicants provide registration information used to apply for a digital Certificate and supply the method of payment used to purchase the Certificate. Information provided via the Secure IdenTrust Registration Website is then managed via the IdenTrust Certificate Lifecycle Management Tool. See the definition of *Server-authenticated SSL/TLS* for additional details regarding current methods and protocols.
Secure IdenTrust Retrieval Website:	This is the term used to describe the Client-authenticated secure website that is hosted by IdenTrust, where Applicants manage key generation and certificate retrieval. The Applicant must authenticate to the website using an Applicant-selected Account Password and an LRA-provided Activation Code in order to initiate the retrieval process. See the definition of *Client-authenticated SSL/TLS* for additional details regarding current methods and protocols.
Secure User Certificate Management Tool	This is the term used to describe the Client-authenticated secure website that is hosted by IdenTrust, where Subscribers can manage certain Certificate lifecycle events and maintenance tasks. Actions initiated via the Secure User Certificate Management Tool include Re-Key, revocation, Account Password Management, etc. The Subscriber must authenticate by presenting a currently valid Certificate or an Account Password to access the website. See the definition of *Client-authenticated SSL/TLS* for additional details regarding current methods and protocols.
Secure Room:	The room located in the IdenTrust primary facility in which CMA equipment is housed. Access to the Secure Room requires that two IdenTrust employees, who have been designated by IdenTrust to act in a Trusted Role, authenticate using two-factor authentication, such as programmable electronic badge and PIN or biometric validation.

TERM	DEFINITION
Server-authenticated SSL/TLS:	Transport Layer Security v.1.2 and higher are cryptographic protocols that use PKI to secure communications transmitted over the Internet. In the Server-authenticated SSL/TLS secured sessions described 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 secured session. Both the secure server and the client create a session key based on the Master Key and then begin encrypted communication. All processes defined in this ECA CPS that specify the use of Server-authenticated SSL/TLS are subject to these requirements. Cipher suites currently supported by IdenTrust can be viewed in this Section under the term *Cipher Suite*.
Subscriber:	A Subscriber is an individual who is the holder of an IdenTrust Certificate. Prior to the issuance of a Certificate, the individual is referred to as an Applicant.
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.
Subscribing Organization:	See *Subscribers*.
Trusted Agent:	See *Trusted Agents (TAs)*.
Trusted Role:	See *Trusted Roles*.
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.

16 AGREEMENTS AND FORMS

16.1 Subscriber Agreement

The most current version of the IdenTrust ECA Subscriber Agreement forms are available online at the *IdenTrust ECA Library,* under the "Forms" section.

16.2 PKI Sponsor Agreement

The most current version of the PKI Sponsor Agreement form is available online at the *IdenTrust ECA Library,* under the "Forms" section.

16.3 In-Person Identification Form (Medium Hardware Assurance)

The most current versions of the IdenTrust ECA In-Person Identifications forms for all ECA Certificate types are available online at the *IdenTrust ECA Library,* under the "Forms" section.

16.4 Part 1: Subscribing Organization Authorization Agreement

The most current version of the IdenTrust ECA Subscriber Organization Agreement forms are available online at the *IdenTrust ECA Library,* under the "Forms" section.

16.5 Trusted Agent Addendum to Subscribing Organization Authorization Agreement

The most current version of the IdenTrust ECA Trusted Agent Addendum form is available online at: the *IdenTrust ECA Library,* under the "Forms" section.