IdenTrust Global Common Certification Practice Statement

Version 1.5

August 8, 2019

Table of Contents

Revision History

Version	Date	Summary of Changes/Comments
1.0	April 30, 2013	Initial version to comply with IdenTrust Global Common Certificate Policy v1.1, dated April 19, 2013.
1.1	August 13, 2013	Updated throughout to accommodate IdenTrust Global Common Certificate Policy v1.2.1, dated August 13, 2013. Certificate Profiles previously included as Section 10 are separated out into a separate IGC Certificate Profiles document consistent with the IGC-CP. Released externally to auditors for Day 0 Audit of IGC test environment.
1.2	September 4, 2013	Changes made to Sections 4.12, 5.4.1 and 6.1.5 to bring CPS into conformance with CP after an IdenTrust internal mapping exercise. Version 1.2 provided to external auditors in conjunction with U.S. FBCA-required Day 0 compliance audit.
1.3	April 23, 2014	Final version approved by PMA for publication in conjunction with first production Certificate Issuance.
1.3.1	March 27, 2015	Minor modifications made to bring CPS into alignment with other IdenTrust CPSs allowing consistent practices. These include changes to: (a) Section 4.10.2 to specify target availability for certificate status service; (b) Section 5.3.2 to specify background check frequency; and (c) Section 6.1.3 to clarify delivery method for PKCS#10 for cross-certificate issuance.
1.3.3	July 31, 2015	Numerous modification to align CPS with IGC- CP v1.3, dated July 15, 2015. Numerous term corrections and clarifications. Additions made to several sections to allow for Issuance of DirectTrust Certificates in compliance with DirectTrust CPv1.2.1. Sentence added to Section 3.2.3.4 in support of CA/B Forum v1.2.0 requirements. Alignment with IGC-CP v1.3.1, dated July 31, 2015. Minor changes in response to DirectTrust accreditation requirements: Addition of Group Certificates for Medium Software. Removal of Group Certificates for Basic Hardware as not necessary. Recognition of DirectTrust requirements under CA warranties.
1.4	May 27, 2016	Removed the requirement for Machine Operators of Device Certificates to have an Individual Certificate. Revised identity verification requirements for Group Address Certificates.

		Increased PIV-I card lifetime to 6 years. Revised CMS-based Issuance practices for PIV-I Hardware Certificates. Revised provisions related to ECDSA Keys. Updated the Table of OIDs Added Primary Machine Operator and Secondary Machine Operator roles Revised provisions describing certificate policy OIDs Revised certificate profile attributes to align with Certificate Profiles document.
1.4.1	August 15, 2016	Updated to comply with DirectTrust 1.3 CP
1.4.2	October 12, 2016	Removed redundant OIDs for IGC Medium Software Group certificates Added OIDs for IGC Medium Hardware Group Device certificates Added new I&A requirements to confirm NPI number for DirectTrust Address certificates Added miscellaneous defined terms Clarified definition of Domain-Bound certificates
1.4.3	May 12, 2017	Updated section 5.3.2 Background Check Procedures to remove requirement for financial check for candidates in a Trusted Role (not required by IGC-CP)
1.4.4	June 16, 2017	Added support for smart card logon (SCL) to these 3 IGC non-PIV-I certificate types: Basic Hardware Medium Hardware Medium Hardware CBP
1.4.5	April 11, 2018	Add Group Organization OIDs
1.4.6	June 22, 2018	Integrated SAFE-BioPharma Bridge Certificate Authority (SBCA) cross-certification with IGC.
1.4.7	October 3, 2018	Modified language in Sections 1.1 to update policy dates and format for improved readability. Updated language in Section 4.3 to clarify options for distributing activation code via email to a verified email address or regular mail to a verified physical address.
1.4.8	November 29, 2018	Updating Section 4.3 to separate activation using hardware into two separate scenarios. Integrate DirectTrust CP V1.4 06262018 modifications. Modify Section 4.7.3 language pertaining to Re-Key to allow automated retrieval.

1.4.9	March 27, 2019	Updating Section 6.5.1 Specific Computer Security Technical Requirements to clarify language pertaining to remote access to the CA System. Updating Section 6.5.2 Computer Security Rating to align with updated IGC-CP document. Updating document to remove specific references to audits required on an annual basis and to refer to Section 8 where a table of best-practices required annual audits is recorded. This will allow one update to be made to the document when audit procedures change, instead of need to make multiple updates throughout the document. Updating format to align with RFC 3647 and the FBCA CP. Some sections were initially omitted because they pertained only to the Federal Bridge CA; however, to ensure that the document format is fully aligned, these sections have been reinserted.
1.4.10	May 29, 2019	Aligning with IGC CP v1.4.9: To remove all references to SSL certificate issuance General cosmetic and clean up to grammar, etc.
1.5	August 8, 2019	Made additional updates to remove references to SSL certificates. Additional cosmetic and formatting changes for ease of use. Adding/updating definitions for: • Reasonable Reliance • Supervised Remote Processing. Added clarifying language to address the following: • For CRL Issuance Frequency • Machine operators may request suspension through an LRA • Device certificates are dual use for signing and encryption. All other certificates are single use • Language for SAFE-BioPharma affiliated certificates to make OU required

1 INTRODUCTION

1.1 Overview

This Certification Practice Statement ("CPS") describes: the practices employed by IdenTrust Services, LLC ("IdenTrust") to operate IdenTrust Global Common Root Certification Authority ("IGC-RCA"); those employed by all Subordinate Certification Authorities ("Sub CAs") operating under IGC-RCA; and those employed by each corresponding Certificate Status Authority ("CSAs"); and by Registration Authorities ("RAs") to fulfill the requirements of the IdenTrust Global Common Certificate Policy, v1.4.9 dated May 29, 2019, (herein referred to as the "IdenTrust Global Common CP" or "IGC-CP").

1.1.1 Certificate Policy (CP)

FBCA certificates contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance established by the IGC Certificate Policy (CP) which shall be available to Relying Parties. Each certificate issued by IdenTrust under the FBCA asserts the appropriate level of assurance in the certificatePolicies extension.

1.1.2 Relationship between the FBCA CP & the FBCA CPS

The FBCA CP states what assurance can be placed in a certificate issued by the FBCA. The FBCA Certification Practices Statement (CPS) states how the FBCA establishes that assurance. The IdenTrust Global Common Certificate Policy (IGC-CP) provides policies for issuing certificates under the IGC policy and this IGC-CPS defines the practices that IdenTrust has deployed to ensure compliance with all associated CP documents. If an external RA (RA) is involved in the certificate approval process, then a Registration Practices Statement (RPS) document is created that defines the practices that the RA has deployed to ensure compliance with all associated CP and CPS documents.

1.1.3 Relationship between the FBCA CP and the Entity CP

The FPKI Policy Authority maps Entity CP(s) to one or more of the levels of assurance in the FBCA CP. The relationship between these CPs and the FBCA is asserted in CA certificates issued by the FBCA in the policyMappings extension.

1.1.4 Scope

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

This CPS also describes all practices required to fulfill the requirements of the following policies:

- DirectTrust Certificate Policy v1.4 dated June 26, 2018
- SAFE-BioPharma Bridge CA Certificate Policy v3.15 dated March 14, 2018

IdenTrust Global Common Certificate Profiles ("IGC Certificate Profiles" or "IGC Profiles") are incorporated into this CPS by reference as required by IGC-CP. At the time of publication of this CPS the current IGC Certificate Profiles version is v1.4.9 dated May 29, 2019. Future versions of IGC Profiles, as published by IdenTrust, may be implemented under this CPS without notice; PKI Participants are advised to refer to the latest IGC Profiles. All CAs operating under IGC-CP are operated in accordance with this IGC-CPS.

As described herein, IdenTrust operates its own Subordinate CA(s) ("Sub CA") and acts as an outsourced CA services provider for all Sub CAs that are owned or sponsored by non-IdenTrust entities. Specifically, IdenTrust operates all CAs subordinate to the IGC Root CA in accordance with this CPS. This CPS describes the practices followed by IdenTrust, Participant CAs, RAs and third parties in performing RA functions related to generating, issuing, managing and revoking IGC Certificates. Terms used herein have the meanings set forth in Section 1.6 below.

References and bibliography of related publications are included at the end of this document. Related publications contain information that forms the basis for PKI. A list of acronyms follows the references.

1.1.5 Interaction with PKIs External to the Federal Government

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

1.2 Document Identification

1.2.1 Alphanumeric Identifier

The alphanumeric identifier (i.e., the title) for this CPS is the "IdenTrust Global Common Certification Practice Statement v1.4.10 dated May 29, 2019".

1.2.2 Object Identifier ("OID")

IdenTrust is the owner of a numeric company identifier, (i.e., an object identifier ("OID") assigned by the American National Standards Institute). The IdenTrust OID arc for Certificates that are Issued by CAs under this CPS is 2.16.840.1.113893.0.100.

The following table defines the Certificates types and IGC-CP Assurance Levels for Issuance under this CPS.

Assurance Levels indicated for each Certificate are intended for cross-certification with the U.S. Federal Bridge Certificate Authority ("US FBCA") at the equivalent US FBCA Assurance Level and SAFE-BioPharma Bridge Certificate Authority (SBCA).

Certificates asserting an Assurance Level of Basic may be Issued to Subscribers of hardware or software Cryptomodules and are named Basic Hardware or Basic Software, respectively. Different OIDs are asserted to allow Relying Parties an ability to distinguish the Certificate storage type.

Certificates that are Issued under this CPS assert one or more of the certificate policy OIDs in Table 1, below. For each named Certificate, one or more Certificate Types may be Issued, depending the use case and Subscriber requirements. Certificate Types indicate a Certificate function such as Signing Certificate, Encryption Certificate or Card Authentication Certificate. Each individual Certificate Type asserts a unique policy in the form of a certificate policy OID under this CP.

Any Certificate issued to a Device must assert the OID or OIDs associated in Table 1 below with a single "Certificate Name" set forth in such Table and listed among the following "Certificate Names":

(i). IGC Medium Device Software;
(ii). IGC Medium Device Hardware; or
(iii). IGC PIV-I Content Signing.

All other policies defined in this CPS are reserved for Certificates not issued to Devices.

Certificates may use additional OIDs to assert affiliations, compliance with particular policies, intended usages or for other purposes. When a CA asserts OIDs indicating compliance with a particular policy, the stipulations of that policy are followed by CAs and RAs. IGC-specific certificate policy OIDs are provided in

Table 1, below; however, Participant CA-specific certificate policy OIDs are detailed and maintained in the IGC Certificate Profile. Participant CA is created and certificate policy OIDs specific to that Participant CA are to be asserted in Certificates issued under Participant CA, then such certificate policy OIDs must be defined as a part of the Certificate profiles associated with that Participant CA and included in the IGC Certificate Profile.

Unless otherwise specified, a requirement or practice specified in this CPS applies to all Certificates that are Issued under this CPS.

Unless otherwise specified, requirements or practices stated for Medium Hardware Certificates also apply to PIV-I Hardware Certificates. The PIV-I Content Signing certificate policy OID is reserved for Certificates that are Issued to a Card Management System ("CMS") for the purpose of signing PIV-I card security objects.

1.2.2.1 IGC OIDs

The following table provides all IGC OIDs:

Table 1 - IGC-CPS Certificate Names, Assurance Levels, Types and Certificate Policy OIDs

Certificate Name	Certificate Assurance Level	Certificate Type	Certificate Policy OID
IGC Basic Software	Basic	Signing Certificate – superseded 06/15/2016 Signing Certificate Encryption Certificate – superseded 06/15/2016 Encryption Certificate	2.16.840.1.113839.0.100.2.1 2.16.840.1.113839.0.100.2.3 2.16.840.1.113839.0.100.2.2 2.16.840.1.113839.0.100.2.4
IGC Basic Hardware	Basic	Signing Certificate Encryption Certificate Card Authentication Certificate Identity Certificate	2.16.840.1.113839.0.100.2.5 2.16.840.1.113839.0.100.2.6 2.16.840.1.113839.0.100.2.7 2.16.840.1.113839.0.100.2.8
IGC Medium Software	Medium Software	Signing Certificate Encryption Certificate IGC Group Organization Signing Certificate IGC Group Organization Encryption Certificate Group Address Signing Certificate Group Address Encryption Certificate	2.16.840.1.113839.0.100.3.1 2.16.840.1.113839.0.100.3.2 2.16.840.1.113839.0.100.3.3 2.16.840.1.113839.0.100.3.4 2.16.840.1.113839.0.100.3.5 2.16.840.1.113839.0.100.3.6
IGC Medium Software CBP	Medium Software CBP	Signing Certificate Encryption Certificate	2.16.840.1.113839.0.100.14.1 2.16.840.1.113839.0.100.14.2
IGC Medium Hardware	Medium Hardware	Signing Certificate Encryption Certificate Card Authentication Certificate Identity Certificate	2.16.840.1.113839.0.100.12.1 2.16.840.1.113839.0.100.12.2 2.16.840.1.113839.0.100.12.3 2.16.840.1.113839.0.100.12.4
IGC Medium Hardware CBP	Medium Hardware CBP	Signing Certificate Encryption Certificate Card Authentication Certificate Identity Certificate	2.16.840.1.113839.0.100.15.1 2.16.840.1.113839.0.100.15.2 2.16.840.1.113839.0.100.15.3 2.16.840.1.113839.0.100.15.4

Certificate Name	Certificate Assurance Level	Certificate Type	Certificate Policy OID
IGC PIV-I Hardware	PIV-I Hardware	Identity Certificate Signing Certificate Encryption Certificate	2.16.840.1.113839.0.100.18.0 2.16.840.1.113839.0.100.18.1 2.16.840.1.113839.0.100.18.2
IGC PIV-I Card Authentication	PIV-I Card Authentication	Card Authentication Certificate	2.16.840.1.113839.0.100.19.1
IGC PIV-I Content Signing	PIV-I Content Signing	PIV-I Content Signing Certificate	2.16.840.1.113839.0.100.20.1
IGC Medium Device Software	Medium Device Software	Device Certificate	2.16.840.1.113839.0.100.37.1
IGC Medium Device Software	Medium Device Software	Group Device Certificate Signing Group Device Certificate Encryption	2.16.840.1.113839.0.100.37.3 2.16.840.1.113839.0.100.37.4
IGC Medium Device Hardware	Medium Device Hardware	Device Certificate	2.16.840.1.113839.0.100.38.1

1.2.2.2 DirectTrust OIDs

The following table provides all DirectTrust OIDs as defined in the DirectTrust CP:

Table 2 – DirectTrust CP Certificate Names, Assurance Levels, Types and Certificate Policy OIDs[1]

Certificate Name	Certificate Assurance Level	Certificate Type	Certificate Policy OID
IGC Medium Software	Medium Software	Signing Certificate – Covered Entities (CE) Encryption Certificate – Covered Entities (CE)	DirectTrust CP v1.3 up to Nov 1, 2018 DirectTrust CP v1.4 from Nov 1, 2018 forward 1.3.6.1.4.1. 41179.0.1.4 (CP) 1.3.6.1.4.1.41179.1.3 (Assurance) 1.3.6.1.4.1.41179.2.1 (CE)
IGC Medium Software	Medium Software	Signing Certificate – Business Associates (BA) Encryption Certificate – Business Associates (BA)	DirectTrust CP v1.3 up to Nov 1, 2018 DirectTrust CP v1.4 from Nov 1, 2018 forward 1.3.6.1.4.1. 41179.0.1.4 (CP) 1.3.6.1.4.1.41179.1.3 (Assurance) 1.3.6.1.4.1.41179.2.2 (BA)

[1] Valid DirectTrust OIDs not currently used in IGC Certificate end-entity profiles: 1.3.6.1.4.1.41179.1.1; 1.3.6.1.4.1.41179.1.2, 1.3.6.1.4.1.41179.1.4

Certificate Name	Certificate Assurance Level	Certificate Type	Certificate Policy OID
IGC Medium Software	Medium Software	Signing Certificate – Healthcare Entities (HE) Encryption Certificate – Healthcare Entities (HE)	DirectTrust CP v1.3 up to Nov 1, 2018 DirectTrust CP v1.4 from Nov 1, 2018 forward 1.3.6.1.4.1. 41179.0.1.4 (CP) 1.3.6.1.4.1.41179.1.3 (Assurance) 1.3.6.1.4.1.41179.2.3 (HE)
IGC Medium Software	Medium Software	Signing Certificate – Non Declared Entities (ND) Encryption Certificate – Non Declared Entities (ND)	DirectTrust CP v1.3 up to Nov 1, 2018 DirectTrust CP v1.4 from Nov 1, 2018 forward 1.3.6.1.4.1.41179.0.1.4 (CP) 1.3.6.1.4.1.41179.1.3 (Assurance) 1.3.6.1.4.1.41179.2.5 (ND)
IGC Medium Software	Medium Software	Signing Certificate – Patients Encryption Certificate – Patients	DirectTrust CP v1.3 up to Nov 1, 2018 DirectTrust CP v1.4 from Nov 1, 2018 forward 1.3.6.1.4.1.41179.0.1.4 (CP) 1.3.6.1.4.1.41179.1.3 (Assurance) 1.3.6.1.4.1.41179.2.4 (Patients)

1.2.2.3 Safe-BioPharma OIDs

The following table provides all Safe-BioPharma OIDs as defined in the SBCA CP.

Table 3 – SAFE-BioPharma CP Certificate Names, Assurance Levels, Types and Certificate Policy OIDs

Certificate Name	Certificate Assurance Level	Certificate Type	Certificate Policy OID
IGC Basic Software	Basic (SBCA Basic 256)	Signing Certificate Encryption Certificate	1.3.6.1.4.1.23165.1.4 1.3.6.1.4.1.23165.1.4
IGC Basic Hardware	Basic (SBCA Basic 256)	Signing Certificate Encryption Certificate Identity Certificate	1.3.6.1.4.1.23165.1.4 1.3.6.1.4.1.23165.1.4 1.3.6.1.4.1.23165.1.4
IGC Medium Software	Medium Software (SBCA Medium SW 256)	Signing Certificate Encryption Certificate Group Signing Certificate Group Encryption Certificate	1.3.6.1.4.1.23165.1.5 1.3.6.1.4.1.23165.1.5 1.3.6.1.4.1.23165.1.8 1.3.6.1.4.1.23165.1.8
IGC Medium Software CBP	Medium Software CBP (SBCA Medium SW 256)	Signing Certificate Encryption Certificate	1.3.6.1.4.1.23165.1.5 1.3.6.1.4.1.23165.1.5
IGC Medium Hardware	Medium Hardware (SBCA Medium	Signing Certificate Encryption Certificate	1.3.6.1.4.1.23165.1.6 1.3.6.1.4.1.23165.1.6

Certificate Name	Certificate Assurance Level	Certificate Type	Certificate Policy OID
	Hardware 256)	Identity Certificate	1.3.6.1.4.1.23165.1.6
IGC Medium Hardware CBP	Medium Hardware CBP (SBCA Medium Hardware 256)	Signing Certificate Encryption Certificate Identity Certificate	1.3.6.1.4.1.23165.1.6 1.3.6.1.4.1.23165.1.6 1.3.6.1.4.1.23165.1.6
IGC Medium Device Software	Medium Device Software (SBCA Machine Medium SW 256)	Device Certificate	1.3.6.1.4.1.23165.1.27
IGC Medium Device Hardware	Medium Device Hardware (SBCA Medium Hardware 256)	Device Certificate	1.3.6.1.4.1.23165.1.28

1.3 PKI Entities

Public Key Infrastructure (A Generic Definition)

The term public key infrastructure ("PKI") is derived from Public Key cryptography, the technology on which PKI is based. Public Key cryptography is the technology behind modern Digital Signature techniques. It has unique features that make it invaluable as a basis for security functions in distributed systems.

A PKI is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on networks. PKI integrates digital Certificates, Public Key cryptography, and CAs into complete enterprise-wide network security architecture. A typical enterprise's PKI encompasses the Issuance of digital Certificates to individual users and servers; end-user enrollment software; integration with Certificate directories; tools for managing, Renewing, and Revoking Certificates; and related services and support.

The CA is the basic building block of a PKI. The CA is a collection of computer hardware, software, and the people who operate it. The CA is known by two attributes: its name and its public key. The CA performs four basic PKI functions:

1) Issues Certificates (i.e., creates and signs them);
2) Maintains Certificate status information and issues CRLs;
3) Publishes its current CRLs, so users can obtain the information they need to implement security services; and
4) Maintains archives of status information about the expired Certificates that it Issued.

A CA may Issue Certificates to users, to other CAs, or both. When a CA Issues a Certificate, it is asserting that the subject (the entity named in the Certificate) has the Private Key that corresponds to the Public Key contained in the Certificate. If the CA includes additional information in the Certificate, the CA is asserting that information corresponds to the subject as well. This additional information might be contact information (e.g., an electronic mail address), or policy information (e.g., the types of applications that can be performed with this Public Key.)

When the subject of the Certificate is another CA, the Issuer is asserting that the Certificates issued by the other CA are trustworthy.

The CA inserts its name in every Certificate (and CRL) it generates, and signs them with its Private Key. Once users establish that they trust a CA (directly, or through Certificate path discovery) they can trust Certificates that are Issued by that CA. Users can easily identify Certificates that are Issued by that CA by comparing its name. To ensure the Certificate is genuine, they verify the signature using the CA's Public Key. As a result, it is important that the CA provide adequate protection for its own Private Key.

For more information regarding PKIs generally, IdenTrust suggests reading NIST Special Publication 800-32, "Introduction to Public Key Technology and the Federal PKI Infrastructure"[2] from which the definitions above were derived.

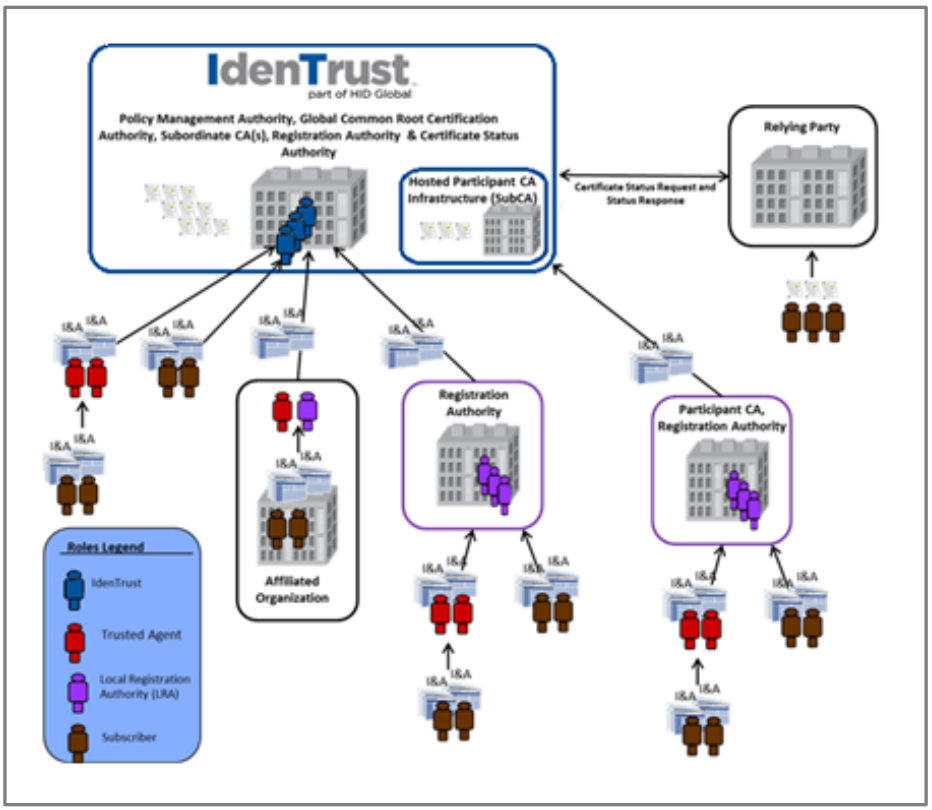
IdenTrust Global Common PKI Participants

IdenTrust operates the IGC PKI, which is a hierarchical PKI, meaning CAs are arranged hierarchically under a "Root" CA that Issues Certificates to Sub CAs. These CAs may Issue Certificates to CAs below them in the hierarchy, or to users. In a hierarchical PKI, every Relying Party knows the Public Key of the Root CA. Any Certificate may be verified by verifying the certification path of Certificates from the Root CA. The IGC PKI is used and operated by PKI Participants.

Below is Figure 1, which is an illustration of how PKI Participants are legally bound by contract. For simplicity, Figure 1 does not attempt to illustrate the contractual relationship among IdenTrust's Policy Approval Authority ("IdenTrust PAA"), the IdenTrust Policy Management Authority ("IdenTrust PMA") and certain other PKI Participants. For the same reason, it also does not attempt to illustrate the distinctions and legal relationships among Local Registration Authorities, Trusted Agents, and other PKI Participants identified in this CPS.

Figure 1: PKI Participants

[2] http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf



This CPS is an assertion of the Certification practices that IdenTrust, Participant CAs, RAs, and others implement. The rights and obligations of all PKI Participants are bound by this CPS, IGC-CP and other contractual documents between IdenTrust and other PKI Participants as described herein.

1.3.1 PKI Authorities

1.3.1.1 Federal Chief Information Officers Council

This council is established within the Federal Government and acts in accordance with the FBCA CP.

1.3.1.2 Federal PKI Policy Authority (FPKIPA)

This role is fulfilled within the Federal Government and acts in accordance with the FBCA CP.

1.3.1.3 FPKI Management Authority (FPKIMA)

This role is fulfilled with the Federal Government and acts in accordance with the FBCA CP.

1.3.1.4 FPKI Management Authority Program Manager

This role is fulfilled with the Federal Government and acts in accordance with the FBCA CP.

1.3.1.5 Entity (IdenTrust) Principal Certification Authority (CA)

IdenTrust acts as a Principal CA cross-certified under the FBCA. IdenTrust issues end-entity certificates, as well as subordinate CA certificates to other Entities and/or external party CAs.

1.3.1.6 Entity (IdenTrust) Policy Management Authority

The IdenTrust Policy Management Authority ("PMA") oversees the adoption, administration and application of IGC-CP, this CPS and any relevant Registration Practice Statement ("RPS") with CAs, RAs, Certificate Status Authorities and other PKI Participants.

The IdenTrust PMA communicates with other Policy Approval Authorities concerning the Cross-Certification existing between the IGC Root CA, Subordinate CAs and the applicable Bridge Certification Authority and conformity to the applicable CP, this CPS and other applicable requirements. The IdenTrust PMA also has charge of the future development and amendment of this CPS. Further explanation of how the IdenTrust PMA meets these responsibilities is located in the appropriate Section for that PMA responsibility (see Section 1.5.4, 8.6 or 9.12).

1.3.1.7 Federal Bridge Certification Authority (FBCA)

The FBCA is the entity operated by the FPKIMA that is authorized by the FPKIPA to create, sign, and issue public key certificates to Principal CAs. As operated by the FPKIMA, the FBCA is responsible for all aspects of the issuance and management of a certificate. This entity is fulfilled by the Federal government and acts in accordance with the FBCA CP.

1.3.1.7.1 IdenTrust Certification Authority

A Certification Authority ("CA") is an Organization that attests to the binding between an identity and cryptographic Key Pair. CA functions primarily consist of the following:

- Providing Key management functions, such as the generation of CA Key Pairs, the secure management of CA Private Keys, and the distribution of CA Public Keys;
- Binding between an identity and cryptographic Key Pair by Issuance of a Certificate;
- Issuing Certificates in response to approved Certificate applications;
- Publication of Certificates in a Repository, where Certificates are made available for potential Relying Parties;
- Initiation of Certificate Revocations, either at the Subscriber's request, the request of an Subscribing Organization; or upon the CA's own initiative; and
- Revocation of Certificates, including by such means as issuing and publishing Certificate Revocation Lists ("CRLs") or providing Revocation information via Online Certificate Status Protocol ("OCSP") or other online methods.

IdenTrust is a CA and has Issued itself the IdenTrust Global Common Root Certificate. Sub-CA Certificates are Issued by the IGC Root CA. Certificates are Issued to Subscribers by Subordinate CAs.

Sub-CA Certificates may also be Issued by the IGC Root CA to well-established, financially responsible entities that have entered into an agreement with IdenTrust, termed Participant CAs. Participant CAs are operated by IdenTrust in accordance with this CPS and IGC-CP. A Participant CA is prohibited from issuing CA Certificates to any entity other than for the purpose of Cross-certification. There shall not be more than one layer of Participant CA between Subscribers and the IGC Root CA.

IdenTrust maintains physical, administrative and operational control over the CA infrastructure for all Subordinate CAs created from the IGC Root Certificate, regardless of whether the Sub-CA Certificate has been Issued to IdenTrust or a Participant CA. In other words, the CA Private Keys of all Subordinate CAs shall be in the custody of IdenTrust. The IGC Root CA and all Subordinate CAs that are part of the IGC PKI are referred to collectively herein as CAs.

An entity that has been Issued a CA Certificate is legally responsible for Certificates that are Issued under its CA Certificate (where the entity is identified as Issuer in the Distinguished Name field of the Certificate). IdenTrust performs the CA functions on behalf of Participant CAs while they are responsible for the performance of Registration Authority functions.

As a provider of CA services, IdenTrust also ensures the availability of all Certificate management services for Certificates that are Issued under the IGC Root Certificate, including the mechanisms to Issue, Revoke and provide status information about Certificates. As the operator of each CA, IdenTrust also operates a

Certificate Status Authority for the Certificates that are Issued by each CA.

IdenTrust maintains physical, administrative and operational control over the CA infrastructure for all subordinate CAs created from the IGC Root Certificate, regardless of whether IdenTrust or a third-party is the CA. In other words, the CA Private Keys of all third-party Subordinate CAs are required to be in custody of IdenTrust on behalf of that party. The IGC Root CA and all Subordinate CAs that are part of the IGC PKI are referred to herein as Certification Authorities or "CAs."

This CPS is an assertion of the certification practices that IdenTrust implements in accordance with IGC-CP. Participant CAs and External RAs must provide an assertion of Registration practices within their RPS in accordance with this CPS and IGC-CP.

CAs, except Participant CAs, may delegate their Registration functions to RAs who meet the financial requirements of Section 9.2.

1.3.1.7.1.1 Participant CAs

IdenTrust Issues Sub-CA Certificates signed by the IdenTrust Global Common Root CA to well-established, responsible external Organizations that meet the financial requirements of Section 9.2, called Participant CAs. Participant CAs enter into an IdenTrust Participant Certification Authority Agreement ("Participant CA Agreement"), which provides that, at a minimum, IdenTrust operates the Participant's CA on behalf of Participant CA and the Participant CA agrees to perform all RA functions in a manner satisfying all RA requirements of the Participant CA's RPS, this CPS, and IGC-CP. The Participant CA Agreement provides that the Participant CA 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 Participant CA is able to demonstrate its ability to satisfy the aforementioned RA requirements and has undergone an external compliance audit in accordance with Section 8 of this CPS.

Subsequent to production operations, the Participant CA is required to undergo an annual compliance audit in accordance with Section 8 of this CPS. Such audit results must be provided by the Participant CA to IdenTrust by May 31st of each year for inclusion in IdenTrust's external compliance audit.

Participant CAs are prohibited from issuing IGC CA Certificates to any entity other than for the purpose of Cross-Certification. Any such cross-certification must be approved in advance by the IdenTrust PMA. By default, Participant IGC CA Certificates are constrained to Issuance of only end-entity Certificates. More than one layer of Participant CA between Subscribers and the IGC Root CA is prohibited.

Participant CAs are prohibited from issuing IGC SSL Certificates. Participant CA Certificates are technically constrained so as to disallow Issuance of IGC SSL Certificates.

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

Participant CAs are prohibited from contracting operation of a CMS or RA System to any entity other than IdenTrust.

A Participant CA that has been Issued a CA Certificate (where the Participant CA is identified as the Issuer in the Distinguished Name field of the Certificate) is responsible for Certificates that are Issued under its CA Certificate.

1.3.1.8 Certificate Status Servers/Authority ("CSS/CSA")

As a provider of CA services, IdenTrust also ensures the availability of all Certificate management services for Certificates that are Issued under the IGC Root Certificate, including the mechanisms to Issue, Revoke and provide status information about Certificates. As the operator of each CA, IdenTrust also operates a Certificate Status Authority for the Certificates that are Issued by Participant CAs.

IdenTrust operates a server-based Certificate Status Authority ("CSA") consisting of Online Certificate Status Protocol ("OCSP") Responder(s) for each CA to provide Revocation status information for Certificates. Certificate status for all Certificates that are Issued by CAs covered by this CPS is provided through CSAs operated by IdenTrust. OCSP Responders are Issued CA-delegated Certificates in order to ensure interoperability with cross certified partners.

IdenTrust also publishes CRLs containing Certificate status information (see Section 2.2).

1.3.2 Registration Authority ("RA")

A Registration Authority ("RA") is an entity that is responsible for collecting and confirming a Subscriber's identity and other information for inclusion 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;
- The initiation 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.

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 Section 9.2. 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 an IdenTrust SSL 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 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 Session.

1.3.2.1 External RAs

IdenTrust may delegate certain registration functions to external Organizations that meet the financial requirements of Section 9.2. Such RAs are referred to in this CPS as "External RA"s.

External RAs 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 their RPS, this CPS and IGC-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 and have undergone an external compliance audit in accordance with Section 8 of this CPS.

Subsequent to production operations, the External RA is required to undergo an annual compliance audit in accordance with Section 8 of this CPS.

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 IGC PIV-I Certificate Issuance to any entity other than IdenTrust.

1.3.3 Card Management System ("CMS")

The Card Management System ("CMS") manages smart card token content. In this context the CMS requirements are associated with the PIV-I policies only. A CMS is only deployed within IdenTrust or an authorized RA Organization. IdenTrust, as the CA, is responsible for ensuring that each CMS implementation meets the requirements described in the IGC-CP, this CPS and requirements stated in Appendix B. A CMS is never issued any certificates that express the PIV-I Hardware or PIV-I Card Authentication policy OID.

1.3.4 Subscribers

A Subscriber is an entity to whom or to which a Certificate is Issued. Subscribers are named in the Certificate subject and hold, either directly or through its designated Custodian (authorized third party), a Private Key that corresponds to the Public Key listed in the Certificate.

Subscribers include:

- Users affiliated with a legal entity requiring a Certificate for use in accordance with this CPS;
- A CA's users;
- Primary Machine Operators; or
- PKI operations personnel at IdenTrust, and Participant CAs.

Note that while CAs are sometimes considered "Subscribers" in a PKI, for the purposes of this CPS, the term "Subscriber" refers only to end-entities.

1.3.4.1 Custodian

A Custodian acts in the capacity of an agent or authorized third party of a Subscriber. The Custodian holds and manages the Private Keys of a Subscriber Certificate, on behalf of that Subscriber, in a Custodial Subscriber Key Store. The Custodial agent, who is appointed by the Custodial entity is typically referred to as the Information System Security Officer (ISSO).

1.3.5 Affiliated/Subscribing Organization

Subscriber certificates may be issued in conjunction with an organization that has a relationship with the subscriber; this is termed affiliation. The organizational affiliation will be indicated in the certificate. IdenTrust contacts the Affiliated Organizations associate with a certificate application to verify the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

1.3.5.1 Local Registration Authority ("LRA")

The Local Registration Authority ("LRA") is an Individual who collects (or receives process documentation from Trusted Agents ("TAs") and confirms each Subscriber's identity information for inclusion in the Subscriber's Certificate. (LRAs are Individuals, whereas RAs are Organizations.) The LRA and the RA Administrator are Trusted Roles held by Individuals who are subject to the requirements of Section 5.3. LRAs and RA Administrators comply with this CPS and the IGC-CP in the performance of their duties. LRA duties are similar to the duties of the RA. LRA services a limited population as authorized by the RA. LRAs collect and confirm each Subscriber's identity and information for inclusion in the Subscriber's Certificate.

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, implementation of network security controls (see Sections 5.1.1.3, 5.1.1.4, 5.1.2.3 and 5.1.2.4; 5.4, 6.5, 6.7).

1.3.5.2 Trusted Agent ("TA")

The Trusted Agent ("TA") collects information and confirms each Subscriber's identity in support of Subscriber registration. TAs are required to be bound by their respective CA or RA through written agreement to perform their duties in compliance with this CPS and the IGC-CP, which include:

- Perform in-person identification of Applicants;
- Collect copies of identification documents and declarations of identity; and
- Deliver end-user support to Applicants, Subscribers and Subscribing Organizations, such as distribution of Cryptomodules, troubleshooting, and assistance with Certificate lifecycle event requests.

TAs may be provided web pages, forms, instructions, and other resources to facilitate the work of TAs, but TAs do not have privileges within CA or RA Systems to perform Certificate lifecycle functions. They act on the behalf of a CA or RA to confirm the identity of the Subscriber as necessary for Certificate Issuance or Certificate Revocation and to deliver support to Subscribers.

IdenTrust TAs are bound through an IdenTrust Trusted Agent Agreement.

1.3.5.2.1 Internal TAs

TAs may be specified by a Subscribing Organization through written agreement between the Subscribing Organization and the contracting CA or RA as authorized to verify Applicant identity data and also authorize affiliation of Applicants and Devices to the Subscribing Organization. Such TAs are referred to in this CPS as "Internal TAs".

Contracting CAs or RAs are required to obligate both the Subscribing Organization and the Internal TA by written agreement to perform their respective duties and obligations under this CPS, and to maintain record of Internal TAs authorized by Subscribing Organizations.

The function of Internal TAs differs from that of standard TAs (those where such written authorization from a Subscribing Organization as described above does not exist) in three ways:

- Internal TAs may only conduct identity proofing for Issuance of IGC Affiliated Certificates, with such Organization affiliation required to be the same as that with which the Internal TA is affiliated;
- Internal TAs may potentially utilize an Antecedent In-Person Appearance to fulfill the requirements for in-person identity proofing (see Section 3.2.3.1.3 of this CPS for Antecedent In-Person Appearance); and
- Internal TAs may assert affiliation of Applicants for which they submit registration data, which affiliation may be relied upon by the RA or CA for Certificate Issuance.

IdenTrust Internal TAs are bound through a Subscribing Organization Agreement Trusted Agent Addendum.

1.3.5.3 Primary Machine Operator

A Primary Machine Operator is an Individual responsible for registering Devices with the LRA. The Primary Machine Operator is employed by or the authorized agent for the Subscribing Organization and expressly authorized by a Subscribing Organization to represent that Subscribing Organization with respect to the Device Certificate. The Primary Machine Operator is responsible for the operation and control of a Device and assumes the obligations of Subscriber for the Certificate associated with the Device, including but not limited to:

- A duty to protect the Private Key of the Device at all times;
- Sign and submit, or approve a Device Certificate application on behalf of the Subscribing Organization;
- Sign and submit a Subscriber Agreement on behalf of the Subscribing Organization, or, when the Organization is an affiliate of the CA, acknowledge and agree to the Certificate terms of use on behalf of the Subscribing Organization; and
- If the Primary Machine Operator desires to, designate Secondary Machine Operators.

The Primary Machine Operator must provide (a) personally identifying information and (b) evidence of affiliation with the Subscribing Organization of the Device, in each case with form and substance sufficient to sustain a verification of identity commensurate with the certificate Assurance Level of the Device Certificate being requested and in accordance with the requirements for human subscribers as detailed in section 3.2.3.1 of this CPS.

If a Primary Machine Operator designates any Secondary Machine Operators, then the Primary Machine Operator is responsible to provide the names of all such Machine Operations in the Secondary Machine Operators List which is a part of the Subscribing Organization Authorization Agreement. The Subscribing Organization is responsible for making Secondary Machine Operators aware of the limited role and scope of responsibilities of Secondary Machine Operators with respect to managing the Device Certificate.

1.3.5.4 Secondary Machine Operator

Secondary Machine Operators may be designated in relation to a given Device Certificate by the Primary Machine Operator of such Device Certificate by inclusion in the Secondary Machine Operators List included in the Subscribing Organization Authorization Agreement submitted to the CA as a part of the Registration process for the relevant Device Certificate. Verification of identity or affiliation of Secondary Machine Operators is not required during the Registration process.

The Subscribing Organization for a given Device Certificate is responsible for obtaining agreement from and compliance by Secondary Machine Operators to the same Subscriber Agreement as the Primary Machine Operator for such Device Certificate is bound.

With respect to the Device Certificate to which a given Secondary Machine Operator is identified to the IdenTrust CA, such Secondary Machine Operator may interact with the IdenTrust CA only for purposes of requesting suspension or revocation of such Device Certificate on behalf of the applicable Subscribing

Organization. Except as provided in the immediately preceding sentence, all other interactions with the IdenTrust CA by a Machine Operator relative to a Device Certificate will be the responsibility of a Primary Machine Operator of that Device Certificate.

1.3.5.5 Subscribing Organizations

Subscriber Certificates may be Issued as affiliated to a Subscribing Organization that has a relationship with the Subscriber when the Subscribing Organization has authorized such affiliation. Certificates asserting affiliation are Affiliated Certificates. Certificate is Revoked in accordance with Section 4.9.1 when affiliation is terminated.

1.3.6 Relying Parties

A Relying Party is an Organization, Subscriber, Device or any entity that relies upon the information contained within a Certificate and upon Certificate status received from a CSA. As an example, a Relying Party may use a Certificate to verify the integrity of a digitally signed message, to identify the creator of a message, to authenticate a Subscriber, or to establish encrypted communications with a Subscriber.

1.3.7 Other Participants

Not Applicable.

1.4 Certificate Usage

1.4.1 Allowed Certificate Uses

IGC Certificates that are Issued pursuant to this CPS may be used for authentication, for Access Control, to create Digital Signatures, to support verification of Digital Signatures, and to achieve confidentiality through the use of encipherment of shared secret. Extended key usages are specified in the applicable Certificate profiles found in IGC Certificate Profiles.

Signing Certificates may be used in applications where: (i) the identity of communicating parties needs to be authenticated; (ii) a message or file needs to be bound to the identity of its originator by a signature; and/or (iii) the integrity of the message or file has to be assured.

Encryption Certificates may be used in applications where a message or file needs to be protected against disclosure to anyone else except the Subscriber of the Certificate and intended recipients.

Group Certificates are primarily used for S/MIME message signature verification and S/MIME message encryption under Direct where non-repudiation of identity is not required.

The following table provides guidelines for certificate usage by assurance level:

Level	Definition
Rudimentary	This level provides the lowest degree of assurance concerning identity of the individual. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable.
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.

Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. This level of assurance includes the following certificate policies: Medium, Medium CBP, and Medium Device. The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. As such, use of certificates associated with the id-fpki-SHA1-medium, id-fpki-SHA1-medium-CBP, and id-fpki-SHA1-devices policy OIDs should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.
PIV-I	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation pin is not practical.
Medium Hardware	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk. This level of assurance includes the following certificate policies: Medium Hardware, Medium Hardware CBP, Medium Device Hardware, PIV-I Hardware, and PIV-I Content Signing. The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. As such, use of certificates associated with the id-fpki-SHA1-hardware and id-fpki-SHA1-mediumHW-CBP policy OIDs should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.
High	This level is reserved for cross-certification with government entities and is appropriate for those environments where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

1.4.2 Prohibited Certificate Uses

Certificates that are Issued under the provisions of this CPS may not be used for:

(i) any application requiring fail-safe performance such as:
- (a) the operation of nuclear power facilities,
- (b) air traffic control systems,
- (c) aircraft navigation systems,
- (d) weapons control systems, or
- (e) any other system whose failure could lead to injury, death or environmental damage; or

(ii) transactions where applicable law prohibits the use of Certificates for such transactions or where otherwise prohibited by law.

1.5 Policy Administration

1.5.1 Organization Administering this CPS

This CPS is administered by:

IdenTrust Services, LLC
5225 Wiley Post Way Suite 450
Salt Lake City, UT 84116
https://www.IdenTrust.com

1.5.2 Contact Person

Questions regarding the implementation and administration of this CPS should be directed to:

Attn: PMA Chair
IdenTrust Services, LLC
5225 Wiley Post Way Suite 450
Salt Lake City, UT 84116
Email: policy@IdenTrust.com

1.5.3 Person Determining Certificate Practices Statement Suitability for the Policy

The suitability and applicability of IGC-CP is determined by the IdenTrust PMA. The PMA determines the suitability of this CPS to the IGC-CP based on a compliance analysis performed by the PMA itself or a party independent from the CA and is not the CPS author.

1.5.4 CPS Approval Procedures

The IdenTrust PMA is responsible for approval of this CPS. All CAs operating under the IGC-CP must meet all requirements of this IGC-CPS applicable to the IGC Certificates to be Issued under the CA before commencing operations.

1.6 Definitions and Acronyms

Capitalized terms and acronyms used herein and in related agreements and other documents incorporating IGC-CP or IGC-CPS have the following meanings. Where the context and usage of a term implies that a substantive conflict occurs between the definition of a term as provided in this CPS and the definition in IGC-CP, the definition provided in IGC-CP will govern interpretation of the term.

1.6.1 Definitions

Term	Definition
Accept or Acceptance	Acceptance is a Subscriber act that triggers the Subscriber's rights and obligations with respect to the Certificate under this IGC-CP, and this CPS. Indications of Acceptance may include without limitation: (i) using the Certificate (after Issuance); (ii) failing to notify the CA or RA of any problems with the Certificate within a reasonable time after receiving it; or (iii) other manifestations of assent or Acceptance. Acceptance is further explained below in Section 4.4.
Access Controls	Access Controls are mechanisms that restrict or grant access to physical or logical resources based on predefined policies. Access Controls are discussed specifically in Section 2.4 (Access Controls on repositories), Section 5 (Facility, Management and Operational Controls) and Section 6.5 (Computer Security Controls).
Account Password	An Account Password is a value selected by an Applicant and known only to that Applicant which value is provided during the Registration process and utilized to authenticate when Retrieving a Certificate.
Activation Code	An Activation Code is a randomly generated, secret numeric code created by the CA or RA and securely delivered to the Applicant for use by the Applicant for authentication purposes.
Activation Data	Activation Data is private data used or required to access to a component or to activate KSMs (i.e., password/PIN, or a manually-held Key share used to unlock Private Keys). See Section 6.4.
Antecedent Event	An Antecedent Event is an event through which an Applicant has previously provided in-person proof of identity. As an example, an Applicant may have previously provided proof of identity to an HR Individual. See also Sponsor

Term	Definition
	Antecedent.
Applicant	An Applicant is an Individual that submits an application and identifying information to the CA or RA for the purpose of obtaining or renewing a Certificate for the Individual or, with respect to Certificates associated with a Device, for a Device.
Assurance Level	Assurance Level is the level of confidence that a Participant should have that the assertion or use of a Private/Public Key Pair or Certificate correctly references the identity, authority, or Subscribing Organization of the Subscriber, and that the Key Pair is correctly bound to the identified subject, and that the subject controls the Private Key, and that the Private Key has not been compromised.
Authorizing Official	An Authorizing Official is an Individual designated in a written agreement within a CA, or RA who can appoint and authorize other Individuals to act as LRAs or Trusted Agents for that Organization.
Business Associate	A Business Associate (BA) helps Covered Entities carry out health care activities and functions under a written business associate contract or other arrangement with the Business Associate that establishes specifically what the Business Associate has been engaged to do and requires the Business Associate to comply with the requirements to protect the privacy and security of protected health information.
CA Certificate	The CA Certificate is the Certificate containing the Public Key that corresponds to the CA Private Signing Key used by a CA to create or manage Certificates.
CA Private Signing Key	The CA Private Signing Key is the Private Key that corresponds to the CA's Public Key listed in the CA Certificate and used to sign and otherwise manage Certificates.
Card Authentication Certificate	A Card Authentication Certificate is a Certificate that is Issued to a smart card controlled by the Organization identified within the Certificate.
Card Management System	The Card Management System (“CMS”) is responsible for managing the content in smart cards. In the context of this CPS, the CMS requirements contained throughout this CPS are mandatory for the IGC PIV-I policies and optional for other Certificate policies. CAs issuing PIV-I Certificates shall ensure that all CMSs meet the requirements described in this document. The CMS shall not be Issued any Certificates that express Assurance Levels of PIV-I Hardware or PIV-I Card Authentication.
Certificate	A Certificate is a computer-based record or electronic message that: (i) identifies the CA issuing it; (ii) names or identifies its subject (see Distinguished Name); (iii) contains the Public Key of the Subject; (iv) identifies the Certificate's Validity Period; (v) is Digitally Signed by a CA; and (vi) has the meaning ascribed to it in accordance with the legal infrastructure in which the Certificate is used (e.g., the CP, contractual agreements, and other system rules governing the course of dealing, usage and trade practice). A Certificate includes not only its actual content but also all documents expressly referenced or incorporated within.
Certificate Chain	A Certificate Chain is an ordered series of Certificates connecting a Subscriber’s Certificate to the Root Certificate. Successive and superior CA and SubCA Certificates up to the Root Certificate connect superior Certificates (which may be self-signed) in a Certificate Chain. For Subscribers under this CP, a self-signed Root Certificate is Issued in compliance with this Policy.

Term	Definition
Certificate Information System ("CIS")	The Certificate Information System is a database maintained by IdenTrust that contains account information about Applicants and Subscribers.
Certificate Policy ("CP")	A Certificate Policy is a specialized form of administrative policy related to Certificate management. A CP addresses generation, production, distribution, accounting, compromise recovery and administration of Certificates. Indirectly, a CP can also govern the transactions conducted using a communications system protected by a Certificate-based Access Controls. By controlling critical Certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certificate Profile	A Certificate Profile is the format and contents of data fields in a Certificate that identify the Issuer, the Subject, the Public Key and other information about the Subject. Certificate Profiles for this CPS are specified generally in Section 7 and more specifically published as a separate document, IdenTrust Global Common Certificate Profiles ("IGC Certificate Profiles" or "IGC Profiles").
Certificate Revocation List ("CRL")	A Certificate Revocation List is a list of Certificates that have been Revoked prior to the expiration of their Validity Period.
Certificate Status Authority ("CSA")	A Certificate Status Authority is the component of a PKI that provides authoritative responses to online requests for Certificate status information, such as Certificate validity, validation of the entire Certificate Chain, and Revocation status. Certificate Status Authority is more fully defined in Section 1.3.2.1.
Certificate Type	Certificate Type defines a more granular Certificate usage or function within a particular Assurance Level. Certificate Types under this CPS are defined as: Signing Certificate; Encryption Certificate; Identity Certificate; Card Authentication Certificate; Content Signing Certificate; Device Certificate; Group Domain-Bound Certificate; and Group Address Certificate. Certificate Types are assigned unique certificate policy OIDs and are listed in Table 1 by Certificate name and Assurance Level.
Certification Authority ("CA")	A Certification Authority ("CA") is an Organization that attests to the binding between an identity and cryptographic Key Pair. Certification Authority is more fully defined in Section 1.3.2.
Certification Practice Statement ("CPS")	A Certification Practice Statement is a statement of the practices that a CA employs in creating, issuing, managing, and, revoking Certificates in conformance with a particular CP.
Client (application)	A Client is a system entity, usually a computer process acting on behalf of a human user, which makes use of a service provided by a server.
Client-authenticated SSL/TLS-Encrypted Session	A Client-authenticated SSL/TLS-Encrypted Session is a session securely communicated through use of the Secure Sockets Layer and Transport Layer cryptographic protocols. For Client-authenticated SSL/TLS-Encrypted Sessions

Term	Definition
	discussed in this CP, both the Client and the server authenticate to each other using a Certificate. Upon mutual validation of identity, the resulting session is encrypted using Public Key Cryptography.
Content Signing Certificate	A Content Signing Certificate is a Certificate that is utilized by a Card Management System to Digitally Sign content embedded in smart cards.
Covered Entity	A Covered Entity (CE) is an individual, organization, or agency that protects the privacy and security of health information and provides individuals with certain rights with respect to their health information.
Cross Certificate/Cross-certification	Cross-certification is the Issuance of a Certificate used to establish a trust relationship between two PKIs. The Cross Certificate is the Certificate Issued by one PKI to another PKI for Cross-certification.
Cryptographic Service Provider	A Cryptographic Service Provider is an independent software module or set of programs (e.g. an application program interface, or "API") used with a given Device to provide a concrete implementation of a set of cryptographic algorithms to be used for authentication, encoding, encryption and other cryptographic functions.
Cryptographic Module	A Cryptographic Module is the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Custodian	A Custodian is an organization or authorized third party that operates a Custodial Subscriber Key Store.
Custodial Subscriber Key Store	A Custodial Subscriber Key Store holds keys for a number of Subscriber Certificates in one location.
Device	A Device is a non-human Subscriber of a Certificate. Examples of Devices include but are not limited to routers, firewalls, servers, and other Devices capable of securely handling Private Keys and properly implementing PKI technologies.
Device Certificate	A Device Certificate is a Certificate Issued to a Device and can be managed by a Machine Operator, Custodian, etc.
Digital Signature/Digitally Sign	A Digital Signature is the result of or mathematical transformation of a document or message through use of cryptography. To Digitally Sign a message is the act of applying a Digital Signature. A Relying Party in receipt of a document or message with a Digital Signature can accurately determine: (i) whether the transformation was created using the Private Key corresponding to the Public Key; and (ii) whether the message or document has been altered since the transformation was made.
Direct Project	The Direct Project is an initiative from the Office of the National Coordinator (ONC) for Health Information Technology that created a set of standards and services that, with a policy framework, enables simple, routed, scalable, and secure message transport over the Internet between known participants.
Directory Information Tree	A Directory Information Tree is data represented in a hierarchical structure containing the Distinguished Names (DNs) of directory service entries.
DirectTrust	DirectTrust.org, Inc. (DirectTrust) is a non-profit and competitively neutral entity operated by and for participants in the Direct community and other communities involved in electronic health information exchange that benefit from leveraging a

Term	Definition
	healthcare-centric PKI. The Direct Project developed the original Direct Ecosystem Community Certificate Policy Version 0.9 in accordance with its consensus process.
DirectTrust Accredited Trust Anchor Bundle (ATAB)	The ATAB has as participants Health Information Service Providers (HISPs), Certificate Authorities (CAs), and Registration Authorities (RAs) that have achieved accreditation through either the DirectTrust HISP Accreditation Program for HISPs or the DirectTrust-EHNAC Trusted Agent Accreditation Program (DTAAP-CA/RA) for CA/RAs.
DirectTrust Certificates	DirectTrust Certificates are those Certificates that are Issued for use within Direct as defined in the Direct Project Applicability Statement for Secure Health Transport and more specifically by the DirectTrust Certificate Policy. DirectTrust Certificates may be Issued under this CP asserting IGC OIDs and OIDs belonging to DirectTrust, asserting compliance with DirectTrust CP.
DirectTrust Governmental Trust Anchor Bundle (GTAB)	The GTAB is to facilitate voluntary, interoperable Direct Message exchange between governmental agencies and private sector members of the DirectTrust community. The DirectTrust Governmental Trust Anchor Bundle creates a single community of trust shared by participating governmental agencies and private sector provider organizations.
Distinguished Name ("DN")	A Distinguished Name is a unique name-identifier for the Issuer or the Subject of a Certificate so that he, she or it can be located in a directory. For example, a DN might contain the following attributes: common name (cn), email address (e) or (mail), Organization name (o), Organizational unit (ou), locality (l), state (st) and/or country (c).
Domain Bound Certificate	A Domain Bound Certificate is a Certificate that contains a Health Domain Name in the form of a dNSName in the subjectCommonName and subjectAlternativeName extensions of the Certificate.
Encryption Certificate	An Encryption Certificate is a Certificate Issued to a Subscriber that can be only used for encryption services.
Enrollment Work Station ("EWS")	An Enrollment Work Station is the customer side computer application that interfaces with the CMS to accomplish Certificate registration.
Fast Healthcare Interoperability Resources (FHIR)	FHIR is a draft standard describing data formats and elements and an application programming interface for exchanging electronic health records. The standard was created by the Health Level Seven International health-care standards organization.
Group Address Certificate	A Group Address Certificate is a Group Certificate that contains a Health Endpoint Name in the Certificate subject. Group Address Certificates may be held by a third party that controls and manages access to the Private Key of the Certificate. See Section 3.2.3.3.
Group Address Encryption Certificate	A Group Address Encryption Certificate is a Group Address Certificate that can be only used for encryption services.
Group Address Signing Certificate	A Group Address Signing Certificate is a Group Address Certificate that can only be used to create a Digital Signature.
Group Certificate	A Group Certificate can be either a Group Domain-Bound Certificate or a Group Address End-Entity Certificate.
Group Domain-Bound	A Group Domain-Bound Certificate is a domain bound Device Certificate that

Term	Definition
Certificate	contains a Health Domain Name in the Certificate subject. Group Domain-Bound Certificates may be held by a third party that controls and manages access to the Private Key of the Certificate. See Section 3.2.3.3.
Group Domain-Bound Encryption Certificate	A Group Domain-Bound Encryption Certificate is a Group Domain-Bound Device Certificate that can be only used for encryption services.
Group Domain-Bound Signing Certificate	A Group Domain-Bound Signing Certificate is a Group Domain-Bound Device Certificate that can only be used to create a Digital Signature.
Government Agency	A Government Agency is an agency, unit, department, division or other subdivision of any governmental authority of any jurisdiction.
Healthcare Entity	A Healthcare Entity (HE) is an entity involved in healthcare, that has agreed to protect private and confidential patient information consistent with the requirements of HIPAA although it is not a Covered Entity or Business Associate as defined under HIPAA at 45 CFR 160.103.
Health Information Service Provider ("HISP")	A Health Information Service Provider (HISP) is an entity that processes Direct-compliant messages to and from Direct addresses, each of which is bound to a Direct-compliant X.509 digital Certificate. Acting in the capacity of an agent for the Subscriber, the HISP may hold and manage Private Keys associated with a DirectTrust Certificate on behalf of the Subscriber.
Health Domain Name	A Health Domain Name is a string conforming to the requirements of RFC 1034 and identifies the organization that assigns the Health Endpoint Names. Example: direct.sunnyfamilypractice.example.org. A Health Domain Name must be a fully qualified domain name, and should be dedicated solely to the purposes of health information exchange.
Health Endpoint Name	A Health Endpoint Name is a string conforming to the local-part requirements of RFC 5322. Health Endpoint Names express real-world origination points and endpoints of health information exchange, as vouched for by the organization managing the Health Domain Name. Example: johndoe (referring to in individual), sunnyfamilypractice, memoriallab (referring to organizational inboxes), diseaseregistry (referring to a processing queue).
ID Form	The ID Form a document incorporated into the Subscriber Agreement and is a document that, among other things (a) is used by the Applicant to provide personally identifying information as part of the Registration process, (b) must be signed by the Applicant, and (c) contains a declaration of identity by the Applicant.
Identification and Authentication ("I&A")	Identification and Authentication is the process of affirming that a claimed identity is correct by comparing the claims offered by an Applicant with previously proven information. I&A requirements for this CPS are fully described in Section 3.
Identity Certificate	An Identity Certificate is a Certificate Issued to a Subscriber that can be used to authenticate the Subscriber by a Relying Party.
IdenTrust subjectID	An IdenTrust SubjectID is included in the subjectDN field of Certificates as an (ou) attribute and, for Certificates where use includes authentication of the subject of the Certificate, is also utilized as a User Principal Name (UPN) structure in the subjectAlternativeName extension of the Certificate. The IdenTrust subjectID in any given Certificate issued by the IdenTrust CA is to be unique among IdenTrust SubjectIDs operational within the PKI.

Term	Definition
IdenTrust SubjID	Has the same meaning as IdenTrust subjectID.
Individual	An Individual is a natural person and not a juridical person or legal entity.
Issue / Issuance	To Issue, or Issuance is the act performed by a CA in creating a Certificate, listing as Issuer itself or, alternately, listing as Issuer a name which the CA has obtained a license to use for such purpose. Issuance also involves notifying the Applicant of Certificate contents, that the Certificate has been created and that the Certificate is available for Acceptance.
Issuer	An Issuer is the Organization that owns a CA Private Key used to Digitally Sign Certificates and (a) is named (or uses a name to which it owns or has licensed for such purpose) as the Issuer in the Issuer DN field in a Certificate.
Identity Verification Provider ("IVP")	An Identity Verification Provider is an Organization that provides affirmation of identity and claims made by an Applicant in support of I&A. IVPs are considered authoritative and must able to demonstrate through policy and audit that the data is accurate and maintained with appropriate integrity, privacy and confidentiality.
Information System Security Officer ("ISSO")	The Information System Security Officer is an individual who is responsible for establishing and maintaining the enterprise vision, strategy and program as it relates to information systems security, to ensure information assets are adequately protected. The ISSO will play a role in authenticating the Subscriber application when a Custodian-managed Certificate is issued under this policy.
Key	A Key is a broad term encompassing all of the defined Keys in this Section 1.6.
Key Generation	Key Generation is the process of creating a single Key (symmetric cryptography) or a Key Pair (asymmetric cryptography).
Key Pair	A Key Pair is two mathematically related Keys consisting of a Public Key and its corresponding Private Key. Key Pair properties ensure that: (i) one Key can be used to encrypt a message that can only be decrypted using the other Key; and (ii) even knowing one Key, it is computationally infeasible to discover the other Key.
Key Storage Module ("KSM")	A Key Storage Module is secure software or a hardware Cryptomodule used to store Private Keys and to perform private key operations such as Digital Signature generation. KSM is used in this policy to refer to Cryptomodules used by a Subscriber in daily operations. KSM is inclusive of software and hardware Cryptomodules as well as different form factors such as smart cards or USB tokens. See also Cryptomodule.
Licensed Notary	A Licensed Notary is an Individual commissioned by a Government Agency to perform notarial acts within that government's jurisdiction and whose commission remains in good standing. Licensed Notaries may include but are not limited to consulate officers, court clerks and may include bank officers or other Individuals.
Lightweight Directory Access Protocol ("LDAP")	Lightweight Directory Access Protocol is a protocol used by browsers and Clients to look up information in directory services based on the x.500 standard.
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 Section 1.3.4.

Term	Definition
Machine Operator	A Machine Operator may be a Primary Machine Operator or a Secondary Machine Operator.
NPI Number	A National Provider Identifier or NPI is a unique 10-digit identification number issued to health care providers in the United States by the Centers for Medicare and Medicaid Services (CMS).
Non Declared Entity	A Non Declared Entity (ND) is an entity that has not asserted it will protect personal health information with privacy and security protections that are equivalent to those required by HIPAA and is not a Patient / Consumer.
Object Identifier ("OID")	An Object Identifier is a unique numeric identifier registered under the ISO registration standard to reference a specific object or object class. OIDs are used within this CPS to uniquely identify the CP, Certificate Types, cryptographic algorithms, and other objects within the PKI.
Online Certificate Status Protocol ("OCSP")	Online Certificate Status Protocol is an internet protocol described in RFC 6960 used to obtain Revocation status of a Certificate.
OCSP Request	An OCSP Request is a message by a Relying Party to a CSA requesting the current status of a Certificate via OCSP. An OCSP Request includes but is not limited to the following data attributes: (i) date and time of the request; (ii) requester identifier (iii) Certificate serial number; (iv) Issuer DN hash; and (v) Issuer Key hash.
OCSP Response / OCSP Responder	An OCSP Response is the message sent by the CSA in response to an OCSP Request, which indicates whether the status of the Certificate in question is valid, Revoked, or unknown. The OCSP Response includes but is not limited to the following data attributes: (i) date and time of the response; (ii) Certificate serial number; (iii) Issuer DN hash; (iv) Issuer Key hash, (v) success or failure indication; and (vi) Digital Signature of the OCSP Responder.
Operational Period	An Operation Period is a Certificate's actual term of validity, beginning with the start of the Validity Period and ending on the earlier of: (i) the end of the Validity Period disclosed in the Certificate, or (ii) the Revocation of the Certificate.
Organization	An Organization is an entity legally recognized in its jurisdiction of origin, (e.g., a company, corporation, partnership, sole proprietorship, Government Agency, non-government Organization, university, trust, special interest group, or non-profit corporation).
Out-of-Band ("OOB")	Out-of-Band is communication methodology between parties utilizing a means or method to communicate that differs from another means or method of communication also used by the parties. As an example, a party could use a courier to communicate one piece of information to a party, and the internet to communicate a different piece of information.
Participants	Participants include all entities operating within an OBB PKI. Participants include but are not limited to those entities described in Section 1.3 of this CP.
Participant CA	A Participant CA is a legal entity that is Issued a Sub-CA Certificate by the IGC Root CA. A Participant CA is operated and managed by IdenTrust. The Participant enters into an Agreement with IdenTrust, which requires that IdenTrust operate the Participant CA and requires the Participant CA to follow and adhere to the provisions of this CPS and the relevant CA CPS when performing RA functions.

Term	Definition
Passphrase	A Passphrase is Activation Data created and used by the Applicant for authentication and delivered to the CIS in a secure manner. The Passphrase later presented by the Applicant for authentication to the CIS prior to performing Certificate management tasks (e.g., retrieving the Certificate).
PKI Service Providers	PKI Service Providers are CAs, RAs, CSAs, and Repositories providing services described in this CPS or within the PKI defined by this CP.
Policy Management Authority ("PMA") / Policy Approval Authority ("PAA")	A Policy Management Authority is an Organization or committee established for a PKI responsible for making recommendations or for setting, implementing, interpreting, and administering policy decisions regarding a CP and may in some instances be responsible for resolving disputes between parties subject to the CP. A Policy Approval Authority is an Organization or Committee responsible for approval of CPs, CPSs, and other policy documents related to a PKI.
Policy Qualifier	An attribute within the Certificate Policy descriptor that is included in a Certificate profile and is used to provide \additional information specific to the named Certificate Policy and certificate policy OID.
Private Key	A Private Key is the Key of a Key Pair kept secret by its holder, used to create Digital Signatures or to decrypt data encrypted with the holder's corresponding Public Key.
Public Key	A Public Key is the Key of a Key Pair publicly disclosed by the holder of the corresponding Private Key via a Certificate. The Public Key is used for Validation of a Digital Signature and encryption of data.
Public Key Cryptography	Public Key Cryptography is a type of cryptography also known as asymmetric cryptography that uses mathematical algorithms and unique Key Pairs of mathematically related numbers. The Public Key can be made available to anyone who wishes to use it, while the Private Key is kept secret by its holder. Private Key can be used to decrypt information or generate a Digital Signature; the corresponding Public Key is used to encrypt that information or verify that Digital Signature. In addition, the Public Key cannot be used to derive the Private Key without a large work factor.
Public Key Infrastructure ("PKI")	A Public Key Infrastructure is a set of policies, processes, server platforms, software and workstations used for administering Certificates and Public-Private Key Pairs, including the ability to Issue, maintain, and Revoke Certificates.
Re-Key	Re-Keying a Certificate consists of creating new Certificate with a different Public Key (and serial number) while retaining the remaining contents of the old Certificate that describe the subject. The new Certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-Key of a Certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness.
Reasonable Reliance	Reliance on a Certificate is considered Reasonable Reliance when a Relying Party has: • Agreed to be bound by the terms and conditions of the IGC-CP and this CPS; • Verified the Digital Signature and Certificate were valid at the time of reliance by using OCSP or the RFC 5280 certification path validation process as required by IGC-CP and this CPS; and • Used the Certificate for purposes appropriate under the CA'S CPS, without

Term	Definition
	knowledge of any facts that would cause a person of ordinary business prudence to refrain from relying on the Certificate, and under circumstances where reliance would be reasonable and otherwise in good faith in light of all the circumstances that were known or should have been known to the Relying Party prior to reliance.
Registrar	A Registrar the person performing the in-person confirmation of the Subscriber's identification. Some restrictions based on the specific IGC certificate Assurance Level apply to the type of Registrar who can perform identification. Registrars who are eligible to perform in-person identification under this IGC-CPS are: LRAs TAs Licensed Notary or other person certified by a Government Agency who is certified as being authorized to confirm identities (e.g., a driver's license bureau employee, a Dept. of State consular office employee, a court clerk, or a county clerk).
Registration	Registration is the process of receiving or obtaining a request for a Certificate from an Applicant, and collecting and entering the information needed from that Applicant to include in and support I&A and the Issuance of a Certificate.
Registration Agent	A Registration Agent is an Individual appointed directly by a CA or RA. A Registration Agent may also be an LRA or Trusted Agent appointed by a CA or RA or may also be a Licensed Notary or other official of a Government Agency. A Registration Agent assists CAs and RAs by providing in-person I&A in accordance with Section 3.
Registration Authority ("RA")	A Registration Authority ("RA") is an Organization that is responsible for collecting and confirming an Applicant's identity and any other information provided by Applicant for inclusion in a Certificate. Registration Authority is more fully defined in Section 1.3.3.
Registration Authority Agreement	A Registration Authority Agreement is an agreement entered into between an Organization and a CA authorizing the Organization to act as a Registration Authority for the CA, and detailing the specific duties and obligations of the RA, including but not limited to the procedures for conducting appropriate I&A on Applicants.
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 fulfill the requirements of the IdenTrust Global Common Certificate Policy.
Relying Party	A Relying Party is an Organization, Subscriber, Device or any entity that relies upon the information contained within a Certificate and upon Certificate status received from a CSA. Relying Party is more fully described in Section 1.3.8.
Repository	A Repository is an online system maintained by or on behalf of a CA for storing and retrieving Certificates and other information relevant to Certificates and Digital Signatures, including CPs, CPSs and information relating to Certificate validity or Revocation.
Requestor	A Requestor is an authorized agent of an Organization who invites an Individual to apply for an Affiliated Certificate.
Revocation or Revoke a Certificate	Revocation is the act of making a Certificate ineffective permanently from a specified time forward. Revocation is effected by notation or inclusion in a set of

Term	Definition
	Revoked Certificates (e.g., inclusion in a CRL).
Root Certificate	A Root Certificate, also known as a Trust Anchor, is a CA Certificate Issued by a CA at the top of a hierarchical PKI. For the PKI described under this CPS, The Root Certificate is the self-signed CA Certificate Issued by and to the IGC Root.
SAFE-BioPharma Bridge Certificate Authority ("SBCA")	A SAFE-BioPharma is the industry standard developed to transition the biopharmaceutical and healthcare industries to paperless environments. It mitigates legal, regulatory and business risk associated with business-to-business and business-to-regulator electronic transactions. It facilitates interoperability by providing a secure, enforceable, and regulatory-compliant way to verify identities of parties involved in electronic transactions.
Secondary Machine Operators List	The Secondary Machine Operators List is a list of individuals who are designated by a Primary Machine Operator to act in the role of Secondary Machine Operator. Initial list of individuals so designated must be made in the Subscribing Organization Authorization Agreement prior the submission of the completed and fully executed Subscribing Organization Authorization Agreement to the CA in connection with an application Registration process for the relevant Device Certificate. Then after, from time to time, the Primary Machine Operator may submit an updated list to the CA as provided in the Subscribing Organization Authorization Agreement, and each such updated list, once recorded by the CA, shall supercede the version of the list recorded by the CA prior to such updated list being recorded. The CA shall record submitted to the CA in the Subscribing Organization Authorization Agreement as part of the Registration process in the CA database. Any updated lists provided to the CA by the Primary Machine Operator as provided for in the Subscribing Organization Authorization Agreement will be recorded by the CA by adding such updated list to the archived documents associated with the relevant Device Certificate account record.
Separation-of-Duties/Multi-party Control	Separation-of-Duties or Multi-party Control are procedures or techniques whereby no single Individual possesses the equipment or authorization to view, alter, or otherwise have access to sensitive or confidential information in a particular PKI. Tasks are separated into multiple subtasks and distributed to more than one Individual, requiring the participation of two or more Individuals to complete the task. The purpose of Separation-of-Duties and Multi-party Control is to reduce risk of PKI compromise.
Server-Authenticated SSL/TLS-Encrypted Session	Server-authenticated SSL/TLS-Encrypted Sessions as discussed in the CP are those sessions in which a Subscriber or Client is directed to a specified secure URL (https://). The SSL-enabled client software confirms the identity of the IdenTrust secure server by validating the Certificate presented by the server. The subsequent session established is encrypted through use of the Secure Sockets Layer and Transport Layer Security cryptographic protocols.
Signing Certificate	A Signing Certificate is a Certificate Issued to a Subscriber that can be used to create Digital Signature to establish integrity of content.
Sponsor	A Sponsor is an Organization that authorizes Issuance of a Certificate to an Individual or a Device. (e.g., an employee's supervisor who authorizes the Issuance of a Certificate to the employee, or the head if an information systems department that authorizes Issuance of a Device Certificate to specific device). The Sponsor is responsible for either supplying or confirming Certificate attribute details to the CA or RA; and is also responsible for informing the CA or RA if the

Term	Definition
	relationship with the Subscriber or Device is terminated or has changed such that the Certificate should be Revoked or updated.
Sponsor Antecedent	A Sponsor Antecedent is an Organization that attests to the validity of an Applicant through their on-going relationship, date of Antecedent Event and provides unique Applicant identity information to the Registration Agent.
SSL / TLS Certificate	A SSL / TLS Certificate is a Certificate Issued to a Device that is utilized to establish an encrypted session between a Client and a server. SSL/TLS Certificates are not issued under the IGC policy.
Subject Name or Subject Distinguished Name	See Distinguished Name.
Subordinate CA	A Subordinate CA is an Organization Issued a Sub-CA Certificate by the IGC Root CA. All Subordinate CAs under this CPS are required to be operated and managed by IdenTrust. All Subordinate CAs are required to follow and adhere to the provisions of the IGC-CP and this CPS when performing RA functions.
Subscriber	A Subscriber is an end-entity Individual or Device to whom or to which a Certificate is Issued. Subscribers may use Certificates for purposes indicated by the Certificate Type. Where Certificates are Issued to Devices, there must be an Individual (Primary Machine Operator) who is responsible for carrying out Subscriber duties.
Subscriber Agreement	The Subscriber Agreement is a legally binding contract that provides terms and conditions applicable to a Certificate that is applied for by an Applicant and, if Issued, Issued to that Applicant as the Subscriber of that Certificate.
Subscribing Organization	A Subscribing Organization is an Organization that authorizes affiliation with Subscribers. Subscribing Organization is more fully described in Section 1.3.7.
Subscribing Organization Authorization Agreement	The Subscribing Organization Authorization Agreement is completed by and submitted in conjunction with Registration for some types of Certificates.
Supervised Remote identity Proofing	A real-time identity proofing event where the RA/Trusted Agent is not in the same physical location as the applicant/subscriber. The RA/Trusted Agent controls a device which is utilized by the applicant/subscriber in order to ensure the remote identity proofing process employs physical, technical and procedural measures to provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. Supervised Remote Identity Proofing must meet the criteria specified in NIST SP 800-63A Section 5.3.3; and must have the capacity to capture an approved biometric when utilized for PIV-I credential issuance.
Suspension or Suspend a Certificate	Suspension is the act of making a Certificate ineffective temporarily from a specified time forward. Suspension is affected by notation or inclusion in a set of Suspended Certificates (e.g., inclusion in a CRL).
System Transaction	The successful execution of all of the following components and steps: (i) Creation of a Digital Signature; (ii) Verification that the Subscriber's Digital Signature was created by the Private Key corresponding to the Public Key in the Certificate; and (iii) Verification that the Certificate was valid by using OCSP and the RFC 5280 certification path validation process as required by the IGC-CP and this CPS.
Trust Anchor	See Root Certificate.

Term	Definition
Trusted Agent	A Trusted Agent ("TA") is an Individual who acts on behalf of the CA, RA, or LRA to collect and/or confirm information regarding Applicants and/or Subscribers, and where applicable to provide support regarding those activities to the Applicants and/or Subscribers. Trusted Agents are more fully defined in Section 1.3.5.
Trusted Role	A Trusted Role is a role involving functions that may introduce security problems if not carried out properly, whether accidentally or maliciously. The functions of Trusted Roles form the basis of trust for the entire PKI.
User Principal Name ("UPN")	A User Principal Name is an attribute used in PKI, the format of such attribute being an Internet-style login name for a user based on the Internet standard RFC 822.
Virtual Machine Environment	An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine in a platform-independent environment. It consists of a host (virtual machine) and isolation kernel (hypervisor) and provides functionality needed to execute entire operating systems. At this time, allowed VMEs are limited to Hypervisor type virtual environments. Other technology, such as Docker Containers, is not permitted.
Validity Period	Validity Period is the intended term of validity of a Certificate, beginning with the notBefore date asserted in the Certificate and ending with the notAfter date asserted in the Certificate.
Zeroize	Zeroize is to erase electronically stored data by altering or deleting the contents of the data storage and overwriting with binary zeros so as to prevent the recovery of the data.

1.6.2 Acronyms

Acronym	Definition
ASN.1	Abstract Syntax Notation (version 1)
ATAB	Accredited Trust Anchor Bundle (DirectTrust)
BA	Business Associate
CA	Certification Authority
CHUID	Card Holder Unique Identifier
CE	Covered Entity
CIS	Certificate Information System
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority (interchangeable with CSS)
CSS	Certificate Status Server (interchangeable with CSA)
DN	Distinguished Name–See Subject Name/Subject Distinguished Name

Acronym	Definition
DNS	Domain Name System
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EWS	Enrollment Work Station
ECDSA	Elliptic Curve Digital Signature Algorithm
EWS	Enrollment Work Station
FASC-N	Federal Agency Smart Credential Number
FBCA	U.S. Federal Bridge Certification Authority
FHIR	Fast Healthcare Interoperability Resource
GTAB	Government Trust Anchor Bundle (DirectTrust)
HE	Healthcare Entity
HIPAA	HIPAA is the federal Health Insurance Portability and Accountability Act of 1996.
HISP	Healthcare Information Services Provider
I&A	Identification and Authentication
IGC	IdenTrust Global Common
IGC PIV-I	IdenTrust Global Common – Personal Identity Verification Interoperable
ISO	International Organization for Standardization
ISSO	Information System Security Officer
IVP	Identity Verification Provider
KSM	Key Storage Module
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
ND	Non-Declared Entity
NPI	National Provider Identifier OID
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OOB	Out-of-Band
OTC	One Time Code
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification – Interoperable
PMA/PAA	Policy Management Authority / Policy Approval Authority
RA	Registration Authority
RFC	Request for Comments
SAFE	Signatures & Authentication For Everyone

Acronym	Definition
SBCA	SAFE-BioPharma Bridge Certificate Authority
SSL/TLS	Secure Sockets Layer and Transport Layer Security
TA	Trusted Agent
UPN	User Principal Name
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
X.500	The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical
X.509, v.3	The ITU-T ("International Telecommunication Union-T") standard for Certificates adopted as ISO/IEC 9594-8 (2001). X.509, version 3, refers to Certificates containing or capable of containing extensions.
XKMS	XML Key Management Specification
XSMS	XML Subscriber Management Specification

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.1.1 FBCA Repository Obligations

The FPKIMA is responsible for all FBCA Repository Functions and Obligations.

2.1.1.1 IdenTrust Repository Obligations

IdenTrust performs the role and functions of the Repository and provides information over the Internet concerning the status of Certificates that are Issued under the IGC Root Certificate at http://validation.identrust.com/crl . The information on each site depends on the form of the information and the protocols for accessing and using it. Certificates, Certificate status information, CRLs and other relevant information is as indicated below in Section 2.2.

IdenTrust operates Repositories to support the PKI operations of IdenTrust, its CAs and all Cross-certified Relying Party populations. Mechanisms used for posting information into a Repository include:

- Hypertext Transfer Protocol (HTTP) or Directory Server Systems that provide access through the Lightweight Directory Access Protocol (LDAP);
- Availability of the information as required by the Certificate information posting and retrieval stipulations of this CPS; and
- Access Control mechanisms when needed to protect Repository availability and information as described in later Sections.

2.2 Publication of Certificate Information

2.2.1 Publication of Certificates and Certificate Status

Certificates that are Issued to Subscribers under the provisions of this CPS are created with a CRL Distribution Point ("CDP") that contains the locations where the Certificate can be validated, i.e., where Revocation can be checked by others using CRLs retrieved by using HTTP GET (and from an LDAP Directory as a secondary mechanism).

CRLs are published in DER-encoded format (binary).

The latest CRLs for end-entity Certificates are published at: http://validation.identrust.com/crl/igcca[x].crl.

[x]: Iteration of the Subordinate IGC CA.

2.2.2 Publication of CA Information

The IGC Root CA is a self-signed Certificate. Revocation information for the IDC Root CA Certificate is not published. Information regarding Certificate Issued to the IGC Root CA can be found at:

http://validation.identrust.com/roots/igcrootca[x].p7c.

IdenTrust publishes Sub-CA Certificates at:

http://validation.identrust.com/certs/igcca[x].cer.

CA Certificates can be downloaded by the following the instructions and utilizing the links found at:

https://www.identrust.com/support/documents/25.

Past and current versions of this CPS are published to a repository made accessible through links on IdenTrust's website. The complete CPS may not be publicly published; however, a redacted version of the

CPS containing information suitable for disclosure is available to Subscribers at:

https://www.identrust.com/support/documents/25.

2.2.3 Interoperability

IdenTrust provides IGC Certificate status responses via both HTTP and OCSP through a highly scalable infrastructure designed to be highly available. Certificates and status are not published via LDAP.

Directory interoperability information is provided in Section 10 below.

2.3 Frequency of Publication

All information to be published in the Repository, including this CPS and any revisions, are published promptly upon becoming available. CA Certificates are published to the Repository immediately upon Issuance. Certificates of Subscribers are not published to a publicly available Repository. CRLs are published to the locations indicated above immediately upon Issuance as specified in Section 4.9.7.

Mechanisms and procedures shall be designed to ensure CA Certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99.9% availability overall per year, and scheduled down-time not to exceed 0.5% annually.

Availability applies to the system as a whole rather than each component and excludes network outages.

2.4 Access Controls on Repositories

The IdenTrust Repository contains only the information that is intended for public dissemination described in Section 2.2. Certificates that contain a UUID in the subjectAlternativeName extension are not published to publicly accessible repositories.

IdenTrust does not impose Access Controls on the Repository for "read" operations. However, as a condition to accessing or using the Repository or other Certificate status services, the PKI Participant must Accept and agree to the terms of use for the Repository, or Certificate status services as specified at that site or as otherwise specified herein.

Administrative access to the Repository is through Access Control mechanisms requiring Individual authentication for logins. Role-based Access Controls prevent unauthorized persons from adding, deleting, or modifying Repository information. CRLs are Digitally Signed and time-stamped to detect any modification.

The Repository is physically located in the secure room in IdenTrust's primary facility and has the physical Access Controls described in Section 5.1.

See also Section 5 and Section 6 for further descriptions of the Access Controls on the Repository.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

CAs only generate and Sign Certificates that contain a non-null subject Distinguished Name ("DN") complying with the X.500 standard. Names used in Certificates are X.501 Distinguished Names ("DN"s).

3.1.1.1 Individuals

DNs include the Subscriber's common name (cn) may be expressed in one of the following formats: where cn = <firstname MI lastname> or cn= <firstname middlename lastname> or cn= <firstname middleinitial lastname> or cn= <firstname lastname>. The subjectDN contains either the value "Unaffiliated" in the organization (o) attribute or if affiliated, the Subscribing Organization's name in Organization (o) attribute. Certificates are required to contain the Subscriber's verified email address as UPN within the subjectAlternativeName extension field.

3.1.1.2 Group Certificates

Group Domain-Bound Certificates contain the domain name of the Organization in two places:

1) The subjectAltName extension formatted as a dNSName; and
2) The common name (cn) of the subjectDN.

Group Address Certificates contain the address to which the Certificate is bound in the Certificate subjectAltName extended attribute, expressed as an rfc822Name.

Group Address Certificates issued to Covered Entities (CE) contain the NPI Number named in the subjectAltName extended attribute.

3.1.1.3 Devices

Certificates that are Issued to Devices use the name of the server, service, or application, or another identifier, provided that each name or identifier is must be confirmed with the Organization in accordance with Section 4.2.2.

3.1.1.4 PIV-I Content Signing

PIV-I Content Signing Certificates indicate the Organization administering the CMS in an appropriate relative Distinguished Name attribute (e.g., Organization (o), organizational unit (ou), or domain component (dc) attribute).

3.1.1.5 Card Authentication Certificates

Basic Hardware Card Authentication Certificates, IGC Medium Hardware Card Authentication Certificates and PIV-I Card Authentication Certificates subjectDN do not contain the common name (cn) attribute. Instead, the serial number attribute in the subjectDN is populated with the UUID as described in Section 3.1.5 of this CPS. The subjectDN contains either the value "Unaffiliated" in the Organization (o) attribute or if affiliated, the Subscribing Organization's name in Organization (o) attribute.

3.1.1.6 Subordinate CAs

CA Certificates that are Issued by the IdenTrust Global Common Root CA subjectDN is "cn = IGC CA [x][3], or in

[3] [x]: Iteration of the Sub CA. (e.g., IGC CA 1, IGC CA 2, etc.)

the case of Participant CAs, cn = a unique CA name designated by the IdenTrust PMA for the Subscribing Organization. The subjectDN contains o = "IdenTrust" as the name of the Organization that owns and is legally responsible for the CA, ou = "IdenTrust Global Common" and optionally, c = country of Issuer, designated by a two-letter international country code".

3.1.1.7 Root CA

The Issuer and subjectDN for the IdenTrust Global Common Root CA is "cn = IdenTrust Global Common Root CA [x][4], o = IdenTrust, c = US."

3.1.1.8 Cross-Certifying Bridge CA

The subjectDN for the Cross Certificate Issued to cross-certifying bridges is "cn = [bridge name] CA, ou = [cross-certifying bridge ou], o = [entity legal name], and optionally, c = [Cross-Certification bridge country]".

Implementation of the above naming conventions is found in IGC Certificate Profiles.

3.1.2 Need for Names to Be Meaningful

Names used in Certificates identify Subscribers and their Organizations. Names are never to be misleading.

The Directory Information Tree will accurately reflect Organizational structures through the use of the "o" (Organization) and "ou" (organizational unit) attributes in the subjectDN.

The Access Controls for the registration system are configured such that LRAs and RA Systems are granted only Certificate lifecycle management rights for Subscribers within a certain domain or Organization namespace. These restrictions help prevent the LRA and RA System from issuing Certificates to unauthorized persons and are enforced by the CA.

When User Principal Names (UPNs) are used, they are populated with the Subscriber's verified email address ensuring uniqueness using the following structure: "unique name@Domain", where "unique name" is either a UUID or subjectID (see Section 3.1.5). Subscribing Organizations provide the Domain(s) that are to be used for those Applicants who are affiliated. The Domain(s) association is ensured based on the Subscribing Organization's obligations agreed to in accordance with Section 9.6.5.3. Only Applicant emails with authorized Domains in the system are accepted during registration. For unaffiliated Applicants the association is created based on the verification of control over the email containing the Domain. For all Applicants, affiliated and unaffiliated), the Domain is extracted from the email provided during registration.

Name uniqueness is provided by unique identifiers described in Section 3.1.5 below.

The minimum names contained within subjectDN of a Subscriber Certificate are:

- The subject:commonName field lists the legal name of the Subscriber of the Certificate as verified through the identity proofing process described in Section 3.2. The name will include first name, middle initial or name (if available, but not enforced) and last name. In the case of a Device Certificate, the subject:commonName field identifies the Device by its identifier as specified in IGC Profiles.
- The subject:organization (o) lists the name of the Subscribing Organization with which the Subscriber is affiliated.

When User Principal Names are used, they are unique within the CA namespace and accurately reflect Organizational structures.

[4] [x]: Iteration of the IdenTrust Global Common Root CA. (e.g., IdenTrust Global Common Root CA 1, IdenTrust Global Common Root CA 2, etc.)

3.1.3 Anonymity or Pseudonymity of Subscribers

All CAs are prohibited from issuing anonymous or pseudonymous Certificates.

DNs in Certificates Issued to end entities may contain a pseudonym to meet local privacy regulations as long as name space uniqueness requirements are met and the name is unique and traceable to the actual Subscriber.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in Certificates will be interpreted using the X.500 series of specifications and ASN.1 syntax. Email names in the subject AlternativeName extension field are interpreted using RFC 5322, specifying the format of Internet email messages. Email addresses and FQDNs can be resolved through DNS. RFC 5280 describes how character sets and strings are to be interpreted in Issuer, subject, and alternative name extension fields. RFC 2253 explains how an X.500 Distinguished Name in ASN.1 is translated into a UTF-8 human-readable string representation, and RFC 2616 explains how to interpret Uniform Resource Identifiers for HTTP references.

Rules for interpreting PIV-I Hardware Certificate UUID names are specified in RFC 4122.

IdenTrust as the CA shall only use valid Uniform Resource Indicators (URIs) in accordance with the applicable Internet Engineering Task Force (IETF) standards.

3.1.5 Uniqueness of Names

3.1.5.1 Subscriber Certificates

Uniqueness is ensured for the Distinguished Name or subjectDN in the Certificate through the use of subjectID or UID as described below.

3.1.5.2 Subject Identifier (subjectID)

A subjectID based on information input by the LRA or TA, may be passed into the CA through the RA System of a Subscribing Organization as a fully formed UPN with the Subscriber's verified email address. The subjectID is included in the subjectDN as an (ou) attribute and may be utilized as a UPN structure in the subjectAlternativeName extension field of Certificates intended for authentication, as defined by Certificate type in the Certificate Profiles document.

Each subjectID used by IdenTrust in Certificates that are Issued by the IdenTrust CA will be unique among subjectIDs used in Certificates that are Issued by the IdenTrust CA. The subjectID consists of three components:

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

The resulting value is expressed as a 32-character hexadecimal number and is used to distinguish Subscribers. The IdenTrust subjectID can be used by itself in which case it is populated in the subjectDN as an (ou) attribute. It can also be used in conjunction with the "@" symbol and the domain name from the Applicant's verified email address to create a UPN structure. The Subscriber's IdenTrust subjectID remains the same when an existing Certificate is used as the basis for issuing a new Certificate (e.g., issuing Encryption Certificate based on Signing Certificate). Each time the Subscriber undergoes initial identity validation as specified in Section 3.2, the Subscriber is assigned a new IdenTrust subjectID.

3.1.5.3 Unique IDentifier (UID)

For Certificates asserting an Assurance Level of PIV-I Hardware, the UID and UPN are used to ensure uniqueness.

A Unique IDentifier (UID) is generated under the parameters defined for a UUID in versions 1, 4 or 5 in RFC 4122. The resulting value is expressed as a 32-character hexadecimal number. The UID can be used by itself, in which case it will populate an OU field in the Subject extension, or it can be used in conjunction with the "@" symbol and the domain name from the Applicant's email address to create a UPN structure. In either case, the UID remains the same when an existing Certificate is used as the basis for issuing a new Certificate. Similarly, each time an existing Subscriber undergoes initial identity validation to obtain another Certificate; the Subscriber is assigned the same UID and UPN.

3.1.5.4 Device Certificates

Device Certificate uniqueness is ensured through the inclusion of the unique subjectID in an (ou) field of the subjectDN as described above. Additionally, uniqueness is ensured through inclusion of FQDNs, IP addresses, program component identifiers, serial numbers or other similar identifiers (Subject Name) expressed within the subjectCommonName (cn) of the subjectDN of the Device Certificate.

3.1.5.5 CA Certificates

The IdenTrust CA Administrator ensures name uniqueness among CAs by reviewing each CA Certificate Profile before it is implemented to ensure that no two CAs use the same name.

3.1.6 Recognition, Authentication, and Role of Trademarks

An Issuing CA shall not knowingly use trademarks in names unless the subject has the rights to use that name. Applicants are prohibited from using names or marks that infringe upon the intellectual property rights of others. An Applicant is not guaranteed that its Certificate's subjectDN will contain any requested trademark, and an Applicant requesting a specific name may be required to demonstrate the right to the use of that name. CAs and RAs may request evidence of ownership of trademarks or the findings and orders from courts or other tribunals. A Certificate will not be Revoked merely because there is another rightful owner of a name or mark when the subjectDN is sufficient for identification within the PKI and is non-infringing or otherwise not deceptive. Without incurring any liability to an Applicant or Subscriber, the CA or RA may reject any application or Revoke a Certificate because of a name or trademark dispute.

Any PKI Participant aggrieved by a decision may proceed under the Dispute Resolution Procedures outlined in Section 9.13. If appropriate, IdenTrust will coordinate with and defer to an appropriate naming authority. If it is determined that the intellectual property rights of a third party have been infringed because a Subscriber provided incorrect information in order to receive the infringing name or mark in its Certificate, that Subscriber hereby agrees to indemnify and hold IdenTrust, the CA, and the RA, harmless for any losses or damages arising out of the use of such name or mark.

3.1.6.1 Name Claim Dispute Resolution Procedure

CAs will escalate any Name Claim Disputes to the IdenTrust PMA. The IdenTrust PMA will resolve any name collisions brought to its attention that may affect interoperability.

3.2 Initial Identity Validation

The CA and RA are responsible for ensuring that proper I&A of Applicants is performed prior to the Issuance of Certificates. CAs and RAs may designate one or more employees as LRAs and may also enroll TAs to perform I&A in accordance with this Section 3.

3.2.1 Method to Prove Possession of Private Key

In all cases where the Subscriber named in a Certificate generates its own Keys, an RSA PKCS#10 Certificate signing request is used to establish that an Applicant holds the Private Key that corresponds to the Public Key included in a Certificate. The PKCS#10 is submitted by the Applicant in a secure manner and verified by the CA as part of the Certificate Issuance process as described below in Section 4.3. This occurs during a Server-Authenticated SSL/TLS Encrypted Session with the IdenTrust CA system.

Proof of possession of the Private Key is established by verifying that the Applicant's Digital Signature in the PKCS#10 was created by the Private Key corresponding to the Public Key in the PKCS#10 as described in the Issuance processes under Section 4.3.1.

For Private Keys used for Encryption Certificates, the Keys can be generated by the Applicant, RA, or the CA. Proof of possession of the Private Key for Encryption Certificates is established in the same manner as described in this Section. In the case when the Encryption Private Keys are generated by the Applicant, proof of possession of Encryption Private Key is established by verifying that the Applicant's Digital Signature in the PKCS#10 was created by the Private Key corresponding to the Public Key in the PKCS#10. The IdenTrust PMA has determined the use of Encryption Certificate Private Keys to create a Digital Signature only in a PKCS#10 for the purpose of establishing proof of possession is an acceptable use of such Private Key.

For the PIN-Protected Certificate Issuance process described in Section 4.3.1.2, an LRA generates the Keys either (1) directly on the party's Cryptomodule, or (2) in a Key generator that securely transfers the Key to the party's Cryptomodule. In this case, proof of possession is not required.

3.2.2 Authentication of Organization Identity

CAs Issue Certificates to individual Subscribers having no affiliation with an Organization or who are acting in a personal capacity and not a professional capacity. In this case, the authentication of the affiliation of the Applicant with an Organization is not required and the practices explained in this Section are not executed.

Prior to approving the inclusion of Organizational identity information in an Affiliated Certificate, the RA verifies:

1) The Organization with which the Subscriber is to be affiliated has authorized the affiliation; and
2) The Organization legally exists, inclusive of the physical address where it conducts business and the telephone number where its representatives can be contacted.

3.2.2.1 DirectTrust Group Certificates

DirectTrust Certificates are defined in IGC Profiles and will reference the DirectTrust Community X.509 Certificate Policy in the Policy Qualifier.

There are two types of DirectTrust Group Certificates:

- Group Domain-Bound Certificates: These certificates are Affiliated Device Certificates
- Group Address Certificate: These Certificates are Affiliated End-Entity Certificates

For DirectTrust Group Certificates, in addition to Organization verification, the CA or RA verifies the Applicant has represented in an agreement signed in the presence of a notary that the Organization is qualified under one of the following categories:

- A HIPAA Covered Entity;
- A HIPAA Business Associate; or

- A Healthcare-related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPAA. Each organizational certificate must represent a legally distinct entity.

3.2.2.2 Custodial Managed Certificates

Custodial Managed Certificates are Certificates that are issued to an affiliated Subscriber, but the Certificate/Private Keys are held in a Custodial Subscriber Key Store and managed by a Custodian who is designated by the Affiliated Organization. The individual physically controls the Subscriber Private Keys and the Custodial Subscriber Key Store is typically referred to as an Information Systems Security Officer (ISSO).

For Custodial Managed Certificates the procedures detailed under the following sub-sections must be executed:

- Authentication of the Individual-Organization Affiliation
- Authentication of Organization Identity

Additionally, verification that the Information Systems Security Officer (ISSO) associated with the application meets the following criteria:

- The ISSO is affiliated with the Sponsoring Organization named in the Certificate Application
- The ISSO who is authorized by the Sponsoring Organization is still active in the ISSO role

3.2.2.3 Authentication of the Individual-Organization Affiliation

CAs Issue Affiliated Certificates to Individuals affiliated to a Subscribing Organization. The Subscribing Organization need not be incorporated, but 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 a Subscribing Organization for the purposes of populating the "o" attribute with the Subscribing Organization name in the subjectDN field of the Affiliated Certificate.

If the Applicant is located outside the United States, a CA may impose through a Subscribing Organization Agreement or Subscriber Agreement additional restrictions in view of other jurisdictions' laws governing privacy, consumer protection, and other rights of Individuals. For example, if an Applicant is located within the European Community, the Subscriber Agreement may contain an additional attestation from the Applicant that the information provided shall be considered business data rather than personal data under European Directive 95/46/EC and/or that the Applicant gives his/her unambiguous consent to the processing of such data by IdenTrust.

The Applicant is affiliated with the Subscribing Organization through the Applicant's status as employee, contractor or agent of the Subscribing Organization. Because it is the Subscriber that holds the Private Key, any verifiable Digital Signature created by that Private Key is attributable to the Subscriber only, and Organizational authority cannot be inferred from IGC Certificates that are Issued under this CPS. IGC Certificates that are Issued under this CPS do not assert roles or authorizations.

In other words, Certificates that are Issued under this CPS do not imply any grant of authority by the Subscribing Organization. A Relying Party can infer from verification of a Digital Signature by reference to a valid IGC Certificate that a Digital Signature is attributable to the Individual Subscriber listed in that Certificate. A Relying Party shall not infer that the Individual Subscriber acted on behalf of the affiliated Subscribing Organization solely based on verification of a Digital Signature created by an IGC Certificate.

LRAs do not approve Issuance of a Certificate to an Individual Subscriber without first obtaining both of the following with respect to the Certificate to be Issued:

- Authorization by the Subscribing Organization with which the Applicant is to be affiliated. The Subscribing Organization may authorize affiliation in one of two ways:
    - Receipt of an attestation letter signed in ink or Digitally Signed by an authorized representative (e.g., a supervisor, administrative officer, information security officer, Authorizing Official, or Certificate coordinator of the Subscribers' Subscribing Organization), provided such letter has been verified inclusive of the authenticity of the authorizing representative and the representative's authorization to act in the name of the Organization; or
    - Receipt of an Affiliated Certificate request for an Applicant from an Internal TA, where the Internal TA has already been authorized by a Subscribing Organization through a Subscribing Organization Internal Trusted Agent Addendum to provide assertion of affiliation, where such Certificate request is for the same Organization affiliation as that of the Internal TA. Such request must be signed in ink or Digitally Signed by the Internal Trusted Agent.
- Confirmation of the existence of affiliation between the Subscribing Organization and the Applicant. This consists of confirmation of the employment, contractor or agency relationship. Confirmation of affiliation may be conducted in one of two ways:
    - Internal TAs confirm affiliation of the Applicant prior to submission of Applicant data to the CA or RA; or
    - The LRA initiates communication with the Subscribing Organization using an independently verified point of contact, i.e. LRA obtains telephone numbers for the Subscribing Organization from a trusted, independent third-party source of such information. The third party may be the Human Resources department or any Individual in a capacity within the Subscribing Organization to confirm the affiliation.

3.2.2.4 Authentication of Subscribing Organization Identity

LRAs 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;
2) Presentation to the LRA of a copy of a Governmentally Issued document attesting to the Subscribing Organization's legal existence, together with reasonable proof of the authenticity of that document. Secretaries of state in the United States generally Issue "Certificates of good standing" to the effect that the Organization in question is in existence at the time the Certificate is Issued. Such a Certificate is signed by an official representative of the secretary of state. Documents submitted for this purpose must be "fair on their face", i.e. bear no apparent indication of forgery, fraud, tampering, etc.;
3) In the case of an Organization that is not registered with a state regulatory agency (such as a partnership or unincorporated association), presentation of a copy of the partnership agreement, association rules, assumed name registration, or other document attesting to the Organization's existence;
4) Independent acquisition of (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 LRA.

RAs keep evidence of authorization of Organization affiliation and confirmation of Organization identity including legal company name, type of entity, principal address (number and street, city, ZIP or postal code), telephone number, and when deemed necessary, domain name registration, certified copy of the Certificate of registration Issued by a Government entity, date of formation, names of directors and officers, and the method(s) by which the LRA verified the Organization information.

3.2.2.5 Participant CA and Registration Authority Representatives

Authentication of identity and authority of representatives of Participant CAs and IdenTrust external RAs are performed as follows:

1) Participant CA Agreements and RA Agreements identify a Primary Authorizing Official and other Authorizing Officials. For each Authorizing Officials, his or her contact information, facsimile of the person's manual (ink) signature and the SHA-1 or SHA-2 hash of the Individual's Public Key and the SHA-1 or SHA-2 hash of the Individual's Public Key Certificate.

   Alternatively, the Secretary or Assistant Secretary of the Participant CA or RA provides IdenTrust with a signed and sealed Certificate of Incumbency that contains the manual signatures of Authorizing Officials, contact information (see previous paragraph), and a statement that such Individuals possess sufficient authority to act on behalf of and to bind the Organization with respect to the CA or RA functions to be performed.

2) Each agreement specifies that the designated Authorizing Official has authority on behalf of that party to communicate with IdenTrust regarding all matters relating to the performance of the agreement, including the authority to appoint and remove other Authorizing Officials by notifying IdenTrust in writing.
3) IdenTrust actions requiring that a request, authorization or approval be given by a representative of the other party must be in writing and Digitally Signed or signed on paper by the Authorizing Official using letterhead of that party. Digitally Signed communications are authenticated in accordance with this CPS. Paper communications are authenticated by reviewing the authenticity of the letterhead and the manual signature of the Authorizing Official.
4) Written communications of Authorizing Officials with IdenTrust are also confirmed by oral conversation via telephone with the Authorizing Official at the phone number in the Schedule attached to the agreement.
5) All oral communications are reduced to writing and with written communications are recorded as digital images and archived by the IdenTrust Operations Group in accordance with Section 5.5.

3.2.2.6 Applicable Bridge CA Representatives

Authentication of identity and authority of representatives of any applicable Bridge CA will be performed as follows:

1) The Board of Directors of the Bridge CA shall adopt a corporate resolution identifying and authorizing those Individuals authorized to act with the authority of the Bridge CA Operator regarding all matters related to Cross-Certification of the applicable Bridge CA with the IdenTrust Global Common Root CA.
2) The applicable Bridge CA shall provide IdenTrust with a copy of the resolution and minutes of the Board Meeting where such resolution was approved and contact information for each authorized representative, including name, address, phone number, and email address.

   Alternatively, the Secretary or Assistant Secretary of the Bridge CA shall provide IdenTrust with a signed and sealed Certificate of Incumbency that contains the manual signatures and contact information of the authorized representatives with a statement that such Individuals possess sufficient authority to act on behalf of and to bind Bridge CA with respect to the actions to be taken.

   In addition to providing contact information and the manual signature of such persons, the paper forms can also include the SHA-1 or SHA-2 fingerprint of each authorized representative's Public Key and the SHA-1 or SHA-2 fingerprint of each representative's Certificate.

3) CA actions require that a request, authorization or approval be given by a representative of the applicable Bridge CA in writing, either Digitally Signed or signed in ink by the authorized representative of Bridge CA on paper using letterhead of the Bridge CA. Digitally Signed communications are authenticated in accordance with this CPS. Paper communications are authenticated by reviewing the authenticity of the letterhead and the manual signature of the authorized representative.
4) Written communications from Bridge CA to IdenTrust are also confirmed by oral conversation via telephone with the authorized representative at the phone number provided to IdenTrust by Bridge CA.
5) All oral communications are reduced to writing and with written communications are recorded as digital images and archived by the IdenTrust Operations Group in accordance with Section 5.5.

LRAs record the confirmation of affiliation in an auditable log in the RA System when approving an Applicant for Issuance of a Certificate.

3.2.3 Authentication of Individual Identity

Individual identity IGC Certificates, including PIV-I Hardware Certificates are only Issued to human Subscribers. The Issuance of an IGC Certificate is based upon authenticating the identity of the Applicant as explained in the following Sections.

3.2.3.1 Authentication of Human Subscribers

The authentication process requires the collection and verification of the Applicant's information. Both, information collection and verification, may be performed either in-person or supervised remote proofing, or through automated processes. The verification process of Applicant identity information varies and is driven by the Assurance Level of the Certificate.

Applicant information is collected either from the Applicant directly, from a Subscribing Organization initiating a Certificate request on behalf of an Applicant, or through submission of Applicant data by an Internal TA. Collection of Applicant information and Certificate application is described thoroughly in Section 4 of this CPS.

For any on-line application or review of identity information prior to application submission, IdenTrust maintains a Subscriber account that is protected by an Account Password provided by the Subscriber to ensure that the verified Applicant Issued Certificate are properly bound. Upon entry of the Account Password by the Subscriber, a hash of the password is generated and stored for comparison purposes as needed for subsequent Subscriber authentication to the Subscriber account. The Subscriber Account Password is used as one of the authentication factors at time of Certificate retrieval.

Upon receipt by the CA or RA of a Certificate application, identity is established through verification of Applicant's identity as required for the IGC certificate Assurance Level by Registrars, TAs, and/or LRAs. Identity verification for the different IGC Certificate types is described in the following subsections.

3.2.3.1.1 Basic

Identity is established either in-person or supervised remote proofing, as described for Assurance Level of Medium Software below, or remotely through an automated process. Most commonly, the process is automated. No in-person identity proofing or paper forms are required of the Applicant for automated identity proofing.

For automated identity verification, the RA System performs record checks either with the applicable agency, institution, or through credit bureaus or similar databases. The RA System verifies Applicant name, address, date of birth and other information provided by Applicant for identity proofing sufficient to ensure data

provided is accurate and identifies a unique Individual.

To meet the requirements for completing the automated identity proofing algorithm, Applicant data submitted must include at least one form of identification from List 1 below:

List 1:

- Currently-valid credit card number;
- Alien Registration Number;
- Passport number; or
- Currently valid Government-Issued driver's license number or Government-Issued identification card number.

In addition to the requirements above, the Applicant must provide two or more of pieces of information from List 2 below:

List 2:

- Social Security Number;
- Date of birth;
- Place of birth;
- Current employer name; or
- Address (number and street, city, ZIP code); or
- Telephone number.

Certificate Issuance Approval

RA System identity proofing algorithms use the Applicant's data and correlate them with information collected from independent data sources for consistency. If high correlation is found, the application is approved and no additional human intervention is needed. If lower or no correlation is found instead, the application is placed into an exception process and additional information is requested from the Applicant (i.e., telephone or utility bill, notarized documentation, etc.). An LRA reviews the additional documentation and approves or disapproves the application.

The information used for the verification algorithm may change from time to time to take advantage of technology and data quality enhancements. Automated verification includes electronic verification of email as described in Section 3.2.3.1.1.

Upon Certificate approval by the automated RA System or by the LRA in the case of automated RA System exceptions, the approval date is captured by the RA System as the date identity was established and the Certificate is queued for Issuance as described in Section 4.3.1.4 of this CPS.

3.2.3.1.2 Medium (all)

Issuance requires identity to be established no more than 30 days before initial Certificate Issuance. If more than 30 days have passed since the in-person or supervised remote appearance, the system prevents the Applicant from proceeding with Key Generation and notifies them that in-person identification must be repeated.

Establishing identity requires in-person or supervised remote proofing before a Registrar (see Section 3.2.3.1.2, Who May Perform In-Person Registration). In the event a Subscribing Organization has specified an Internal TA, an Antecedent In-Person Appearance as described below in Section 3.2.3.1.3 may suffice as meeting the in-person or supervised remote identity proofing requirement.

For in-person identity or supervised remote proofing, the Applicant appears before the Registrar with a

completed ID Form and required credentials.

Credentials required are one National Government-Issued picture I.D., or one REAL ID Act compliant picture ID[5], or two Non-National Government I.D.s, one of which shall be a picture I.D. (e.g., Non-REAL ID Act compliant Driver's License). Any credentials presented must be unexpired.

Acceptable National Government-Issued picture IDs include:

- A U.S. Government or foreign National Government passport or passport card with photograph;
- A U.S. Federal or foreign National Government driver's license with photograph;
- A U.S. Federal or foreign National Government employee ID card with photograph;
- A U.S. Federal or foreign National Government military ID card with photograph;
- An Alien Registration Receipt Card with photograph;
- A Certificate of Citizenship with photograph; or
- Other similarly trustworthy and currently-valid photo ID Issued by a U.S. Federal or foreign National Government, as defined on IdenTrust-approved registration forms.

Acceptable Non-National picture IDs include:

- A state or local Government-issued driver's license with photograph;
- A state or local Government-issued ID Card with photograph; or
- A student ID from a College or University
- Other acceptable forms of ID include:
- An employer identification card;
- A social security or national health card;
- An original or certified copy of a birth Certificate;
- A voter registration card;
- A concealed weapons permit;
- A pilot's license; or
- A marriage license.

The Applicant signs the ID Form in the presence of the Registrar as a declaration of identity and indication of Acceptance of the Subscriber Agreement. The Registrar then follows instructions on the form, verifying the Applicant matches the provided credentials and signs and/or notarizes the form. Signatures made are under the format set forth at 28 U.S.C. § 1746 (declaration under penalty of perjury) or comparable format under non-US law.

Certificate Issuance Approval

Upon receipt of the ID Form, the LRA records the information set forth below for Issuance of each Certificate:

- Identity of the Registrar who performed the in-person or supervised remote identification, if applicable;
- The signed declaration by the Registrar that he or she confirmed the identity of the Applicant;
- Unique alphanumeric identifiers (e.g. driver license number, notary ID number) and Issuance and/or expiration dates collected from the credentials or IDs of the Registrar and the Applicant;
- The date and time of the confirmation; and
- The declaration of identity (ID Form) signed by the Applicant.

[5] REAL ID Act compliant IDs are identified by the presence of the DHS REAL ID star

In the event of an Antecedent In-Person Appearance, an I-9 form signed by the Applicant and provided by an Internal TA of the Applicant's Subscribing Organization may be utilized as the signed declaration of identity.

If an Applicant is unable to appear before a Registrar, the Applicant may be represented by a trusted person who is already a holder of an IGC Certificate of the same or higher Assurance Level than the Certificate being applied for by Applicant. The trusted person will present information sufficient for registration at the level of the Certificate being requested, for both himself or herself and the Applicant who the trusted person is representing. Information provided by the trusted person directly to an LRA or TA must be signed in ink if provided in paper form, or Digitally Signed with the trusted person's IGC Certificate if provided in electronic form. A trusted person may appear on behalf of an Applicant only for those severe situations where in which an Applicant cannot physically appear for in-person identification (e.g., a physically disabled Applicant). The use of a trusted person as proxy for an Applicant is not for convenience, (e.g. a spouse may not appear for an Applicant solely because the Applicant is travelling or out of country). All Certificate applications submitted by a trusted person on behalf of an Applicant must be approved by the IdenTrust Risk Management Committee prior to Certificate Issuance.

3.2.3.1.3 PIV-I Hardware

Data entered into the CMS through the EWS and certain actions and activities performed by the LRA or TA, such as capture of biometrics data and supporting documentation, as described in this section, are automatically captured by the CMS.

Certificate Issuance Approval

Access to EWS by an LRA or TA must require the LRA or TA to use a Certificate of which such LRA or TA is the Subscriber and such Certificate must be confirmed by the EWS as Valid in order for such access to occur. The Assurance Level of such Certificate must be equal to or above the Assurance Level of the PIV-I Certificates that will be issued via the EWS.

The Applicant described in this process is also defined as the Subscriber of the Certificate, if Issued, for which such Applicant applies.

Issuance requires identity of the Applicant to be established no more than 30 days before initial Certificate Issuance. If more than 30 days have passed since the in-person appearance of the Applicant for identification purposes the LRA or TA must repeat the in-person identification process before proceeding with the Certificate enrollment.

Establishing identity of the Applicant requires the Applicant to appear in-person before and present required credentials to a TA or LRA. Such TA or LRA serves as the Registrar for purposes of establishing the identity of the Applicant. The role of Registrar cannot be performed by any entity that is not a TA or LRA.

Utilization of an Antecedent In-Person Appearance is prohibited.

Credentials required to be presented by the Applicant to establish the identity of the Applicant are two identity source documents, which documents must be original documents issued by the authority responsible for issuing such documents. The documents must be of a type listed among the list of acceptable documents included in Form I-9, OMB No. 1115-0136 Employment Eligibility Verification. At least one document must be a valid form of State or Federal Government-Issued picture identification (ID).

Biometric information of the Applicant is collected during the application process. Such biometric information includes:

Two electronic versions of the Applicant's fingerprints which, upon successful completion of the Registration process, will be uploaded through the CMS to the smart card that is provided by the LRA or TA and issued to the Applicant. These electronic fingerprints will be relied upon for automated authentication during usage.

Fingerprints of the Applicant must be collected each time a smart card is Issued; and

An electronic version of the Applicant's facial image, which, upon successful completion of the Registration process, will be printed on the aforementioned smart card and uploaded through the CMS to the smart card. A facial image of the Applicant is collected each time a smart card is Issued.

Registration Forms and Agreements

For PIV-I enrollment, the LRA or TA will perform identification and authentication of the Applicant by using the EWS software to record and compile data provided by the Applicant, and to record and compile required forms and agreements necessary to the enrollment process.

The Applicant must provide information and supporting documentation to the LRA or TA sufficient to complete the enrollment process and to populate the Subscribing Organization Authorization Agreement. The Subscribing Organization Authorization Agreement may be presented and completed electronically within the EWS system or may be a presented and completed on paper.

The Subscribing Organization Authorization Agreement must be signed by the LRA or the TA, acting as the representative of the Subscribing Organization authorizing the Applicant/Subscriber to receive a PIV-I Certificate.

If the Subscribing Organization Authorization Agreement is presented electronically, the LRA or the TA may Digitally Sign the agreement where appropriate for his or her role as Registrar and using the Certificate that he or she uses to authenticate for purposes of accessing the EWS system; or

Alternatively, the LRA or TA may sign a paper copy where appropriate for his or her role as Registrar and of the Subscribing Organization Authorization Agreement in ink.

The Applicant/Subscriber must also sign a declaration of identity before a Certificate application can be approved. The Applicant/Subscriber will comply with this requirement by signing the ID Form which is included as a part of the Subscribing Organization Authorization Agreement.

If the Subscribing Organization Authorization Agreement is presented electronically, it is permissible for the Applicant to use the Private Keys of another valid Certificate that is Issued to him or her for Digital Signing, provided that such Certificate is of an Assurance Level that is equal to or higher than the Assurance Level of the PIV-I Certificate for which he or she has applied; or

As an alternative, it is also permissible for the Applicant to Digitally Sign the ID Form that is included in the Subscribing Organization Authorization Agreement using the Private Keys of the Signing Certificate that is part of the PIV-I Certificate for which he or she has applied and been Issued, provided that (a) such PIV-I Certificate is generated immediately upon authentication of the Applicant's identity made in connection therewith, and (b) such act of Digitally Signing the ID Form occurs as a part of (either integrated into or logically contiguous) the Issuance process. In the event the Applicant does not so Digitally Sign the ID Form, then the PIV-I Certificate must immediately be Revoked; or

As an alternative, the Applicant may sign a paper copy of the ID Form in ink.

A copy of the completed and fully executed Subscribing Organization Authorization Agreement that has been signed by the LRA or TA and the Applicant, and Authorizing Official of the Subscribing Organization must be retained as a part of the Applicant data record within the EWS.

Upon completion of Applicant enrollment, the LRA or TA will finalize the Applicant enrollment according to the process supported by the Subscribing Organization's EWS at which point the application is transmitted through the CMS to the CA or RA for processing.

Following CA or RA processing, the PIV-I hardware is prepared by the LRA or TA, via the CMS and distributed

to the Applicant, either immediately or on a deferred basis.

3.2.3.1.4 Appeal or Redress of Denied Application

In the event an applicant is denied a credential based on the results of the identity proofing process, IdenTrust shall provide a mechanism for appeal or redress of the decision.

When an application for a credential is declined, IdenTrust provides notification to the applicant and provides instruction for remediation of unacceptable application criteria.

3.2.3.1.5 Electronic Verification of Email and Mobile Phone

3.2.3.1.5.1 Email Verification

When a Subscriber email address is included in a Certificate or used as part of identity verification, the email address is verified.

A RA System or CMS of a Subscribing Organization may utilize a directory of email addresses maintained by the Subscribing Organization for as an authoritative source of email addresses. Where such a directory is used to verify an Applicant's email address, addition verification of the Applicant's email address is not required.

IdenTrust's online registration process verifies email addresses electronically through an automated process:

1) An automated email containing a one-time code (OTC) is sent to the Applicant's email address provided in the application by the RA System.
2) Within the automated email message there is a link that guides the Applicant to a server-authenticated SSL/TLS secured web site and instructions to the Applicant to authenticate by entering the OTC delivered in Step #1.
3) The Applicant authenticates by providing the OTC from the email message into the RA System through the SSL/TLS secured session.

Upon verification of the Account Password by the RA System, verification of email address is complete and the verification status is updated automatically by the RA System within the Applicant's application record.

3.2.3.1.5.2 Mobile Phone Verification

The registration process described in Section 4.3.1.4 for IGC Basic Software Certificates allows delivery of Activation Data via two electronic channels. In such cases where an Applicant selects this method for Activation Data delivery, the Activation Data is sent only to a mobile phone number verified to be in the Applicant's possession.

The method used to verify an Applicants mobile phone is similar to email address verification:

1) An SMS (text) message containing an OTC is sent by the RA system to the Applicant's mobile phone number as provided in the original application.
2) The Applicant authenticates the mobile phone by entering the OTC from the SMS message into the RA System through the SSL/TLS secured session.

3.2.3.1.6 Who May Perform In-Person Identification

IdenTrust uses the term "Registrar" to mean the person performing the in-person confirmation of the Subscriber's identification. Some restrictions based on the specific IGC certificate Assurance Level apply to the type of Registrar who can perform identification.

In-person identification for the Issuance of Individual Certificates may be performed by, and in the presence of one of the following kinds of Registrars:

- A LRA;
- A TA; or
- A Licensed Notary or other person certified by a Government Agency who is certified as being authorized to confirm identities (e.g., a driver's license bureau employee, a Dept. of State consular office employee, a court clerk, or a county clerk).

The Registrar or the Applicant submits the information collected from the Applicant directly to the CA or RA in a secure manner. Packages may be secured in a tamper-evident manner (e.g. sealed in an overnight delivery package commonly used by domestic and international couriers) to satisfy this requirement. The Registrar may also utilize an RA System-provided secure web interface for Digitally Signing and submitting Applicant information.

For all Assurance levels except for PIV-I Hardware, Applicant proof of identity from an Antecedent In-Person Appearance may be submitted to a CA or RA by an Internal TA, provided a relationship exists between the Subscribing Organization and the Applicant sufficient for the Internal TA to uniquely identify the Individual identity proofed the be the same Individual as the Applicant (see Section 3.2.3.1.3).

For Certificates asserting an Assurance Level of PIV-I Hardware, only LRAs and TAs may perform the in-person identification of Applicants. Identity proofing by other types of Registrars such as notaries is specifically prohibited.

3.2.3.1.7 Antecedent In-Person Identity Proofing Process

A simplified alternative in-person proofing process is possible when an Antecedent In-Person Appearance has occurred.

Utilization of an Antecedent In-Person Appearance to meet the requirement for in-person identity proofing as defined below is limited to Affiliated Certificates. The use of Antecedent In-Person Appearance for Certificates asserting an Assurance Level of IGC PIV-I Hardware is prohibited.

Only one use case is authorized for utilization of an Antecedent In-Person Appearance under this CPS, which is an Internal TA, where such Internal TA has access to identity data provided by the Applicant through an Antecedent In-Person Appearance. The Internal TA in this case is usually within the Subscribing Organization's HR department or a department head.

3.2.3.1.7.1 ID Proofing Relationships

The Subscribing Organization is required to have an established relationship with Applicant. The relationship must be sufficient enough to enable the authenticating TA to, with a high degree of certainty, verify that the Applicant is the same person that was identity proofed through the Antecedent In-Person Appearance.

3.2.3.1.7.2 Antecedent In-person Identity Proofing Event

3.2.3.1.7.2.1 Collection of Identity Data from an Antecedent In-Person Appearance

Internal TAs utilizing an Antecedent In-Person Appearance are required to:

- Utilize a specialized ID Form designed for TAs to record identity information inclusive of information from an Antecedent In-Person Appearance (if applicable);
- Record the nature of the ongoing relationship between the Subscribing Organization and the Applicant, i.e. "employee" or "contractor";
- Record the date of the Antecedent In-Person Appearance;
- Record the relationship between the Subscribing Organization and the Applicant;
- Sight the Applicant-provided I-9 form and copies of credentials provided;
- Record the date the I-9 Form was signed by the Applicant as a declaration of identity;

- Record the required identity credentials as defined in Section 3.2.3.1;
- Record the data to be used by Applicant in response to authentication questions to establish a Subscriber account and complete the application process:
    - Date of Antecedent In-Person Appearance (usually date of hire);
    - Applicant's date of birth;
    - Applicant's last 4 digits of Social Security Number;
    - Applicant's work email address (must be of the same domain as Subscribing Organization);
    - Last name of Applicant's direct manager;
    - Applicant's previous employer;
    - Applicant's home street address; and
    - Applicant's home phone number (or mobile telephone number if no home telephone number).
- Sign or Digitally Sign the ID Form and securely transmit the form to the CA or RA for verification.

3.2.3.1.7.2.2 Records Retention

While I-9s must normally be kept by employers for three (3) years after the date of hire or one (1) year after the date employment ends, I-9s used as proof of an Antecedent In-Person Appearance or as substitutes for signed declarations of identity are kept for 10.5 years as required by of Section 5.5.2.

3.2.3.1.7.3 CA/RA Verification of Applicant Data from an Antecedent In-Person Identity Proofing Event

On receipt of the ID Form from the Internal TA, a LRA verifies:

- The Internal TA submitting the ID Form has been authorized to do so through execution of a Subscribing Organization Authorization Agreement Internal Trusted Agent Addendum executed by an Authorizing Official of the Subscribing Organization to which the Applicant is to be affiliated; and
- The ID Form has been fully completed and signed in ink under penalty of perjury or Digitally Signed by the Internal TA.

The Antecedent In-Person Identity Proofing Process requires that the Certificate Validity Period not exceed nine years from the Antecedent In-Person Appearance date. To ensure that the Validity Period of a Certificate Issued on the basis of an Antecedent In-Person Appearance does not extend beyond the in-person identification limits stated above, the LRA enters the date of the Antecedent In-Person Appearance as the date of registration into the RA System. The RA System then ensures the Validity Period does not exceed nine years beyond the registration date entered as described in Section 3.3.1. In the event a requested Certificate's expiration would exceed nine years from the Antecedent In-Person Appearance, the Applicant is required to undergo new identity proofing.

If any of the above requirements are not met or there is any question by the verifying LRA as to the authenticity of the data provided by the Internal TA, the application is rejected and the Internal TA is notified to instruct the Applicant to appear for an in-person identity proofing process as defined in Section 3.2.3.1. Otherwise, the LRA enters the Applicant identity information into the RA System, creating a non-activated Subscriber Account for the Applicant.

3.2.3.1.8 Binding the Certificate Request to the Identity

The RA System sends an automated email message to the Applicant at the Applicant's work email address as provided on the Subscribing Organization Trusted Agent ID Form inviting the Applicant to complete their Certificate application. The invitation includes a web link to begin the process that is linked within the RA System to the non-activated Subscriber account. The RA System requires the Applicant to answer three questions from the list below or other information obtained during the application process, one of which

must be email address, to begin the authentication process to the RA System:

1) What is your work email address? (required);
2) What is your date of birth?;
3) What is your home address?;
4) What is your home telephone number?; or
5) Who was your previous employer?

The RA System compares the email address provided by the Applicant in response to the questions to the email address associated with the Subscriber Account referenced within the web link invitation. If a match, the RA System then verifies the remaining questions were answered correctly. If the Applicant failed to answer any question correctly, the Internal TA is notified to instruct the Applicant to appear for an in-person identity proofing event as described in Section 3.2.3.1. If the Applicant successfully answered all three questions, the RA System presents the Applicant with an additional three random questions such as those from the list below to finish the RA System authentication process:

1) Who is your direct manager?;
2) What was your date of hire?;
3) What is the number of your [ID Form 1][6] provided on your I-9 form at time of hire?;
4) What is the number of your [ID Form 2] provided on your I-9 form at date of hire?; or
5) What are the last 4 digits of your Social Security Number?

The RA System verifies the questions were answered correctly. If the Applicant failed to answer any question correctly, the Applicant is instructed to appear for an in-person identity proofing as described in Section 3.2.3.1. If the Applicant successfully answered all three questions, the RA System prompts the Applicant to enter a Subscriber Account Password, review all data for accuracy, pay for the Certificate and any related hardware (if payment is required) and Accept the Subscriber Agreement.

Upon Acceptance of the Subscriber Agreement, the Certificate is deemed approved within the RA System and the process of Issuance begins, utilizing one of the activation processes defined in Section 4.3.1, commensurate with the type of Certificate to be Issued.

3.2.3.2 Authentication of Subscribers for Role-based Certificates

Role-based Certificates are currently not Issued under this CPS.

3.2.3.3 Authentication of Subscribers for Group Certificates

A Group certificate corresponds to a credential with a Private Key that is shared by multiple Subscribers. Multiple Two different Group Certificate Types are defined for Issuance under this CPS and have differing I&A requirements:

3.2.3.3.1 Group Domain-Bound Certificates

Group Domain-Bound Certificates are Device Certificates and assert Organization name in the subjectName DN, which must be in the form of a FQDN. Group Domain-Bound Certificates are by their nature affiliated Certificates.

For Group Domain-Bound Certificates, the CA or RA verifies and records the following:

[6] The RA System requests the identifying number of the specific credential type used on the Applicant's I-9 form, as recorded by the TA from the antecedent in-person identity proofing event, ex., "What is your Passport number?", if Passport was a credential type referenced on the I-9 form.

- Organization authentication as described in Section 3.2.2;
- Authentication of a human Sponsor for the Certificate in accordance with Section 3.2.3.1 at a Medium Assurance Level;
- Verification of authorization of the Subscribing Organization with an authoritative source within the Subscribing Organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a reliable means of communication;
- The Device associated with the Group Domain-Bound Certificates according to Section 3.2.3.4 Authentication of Devices; and
- For DirectTrust Certificates, Organization HIPAA status.

3.2.3.3.2 Group Address Certificates

Group Address Certificates assert Organization and may contain an address associated with a group member (Individual acting on behalf of the Organization) in the subjectName DN. Address Certificates are Affiliated Certificates. For Group Address Certificates, the CA or RA verifies and records the following:

- Organization authentication as described in Section 3.2.3.3(1) above;
- Authentication of the Individual with whom the address is associated in accordance with Section 3.2.3.1 at a Medium Assurance Level;
- Verification of authorization of the Subscribing Organization with an authoritative source within the Subscribing Organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a reliable means of communication;
- For DirectTrust Certificates, Organization HIPAA status and membership agreement between the health information service provider (HISP) and the Subscriber; and
- For DirectTrust Group Address Certificates issued to Covered Entities (CE) confirmation of the NPI Number to be included in the Certificate subjectAltName extension in accordance with Section 3.2.3.3.1.

In addition to the above authentication requirements, the following procedures shall be performed for members of the group:

- Group Address Certificates shall not assert non-repudiation;
- The Organization responsible for management of the Group Certificate(s) shall be responsible for ensuring control of the Certificate Private Key(s), including maintaining a list of Subscribers who have access to use of the Private Key(s), and accounting for which Subscriber had control of the Key at what time;
- The subjectName DN shall not imply that the subject is a single individual, e.g. by inclusion of a human name form without also clearly indicating the group nature of its issuance;
- The list of those holding the shared Private Key shall be provided to, and retained by, the applicable CA, RA or a designated representative; and
- The procedures for issuing tokens for use in shared key applications shall comply with all other stipulations of this CP (e.g., key generation, private key protection, Subscriber obligations).

3.2.3.3.3 Custodian-managed Certificates

Custodial-managed Certificates are allowed under the IGC-CP and this CPS. In order to approve an application for an IGC Custodian-managed Certificate, the Issuer CA or RA will confirm the information identified in Section 3.2.2 Authentication of Organization Identity with respect to the authority of Information System Security Officer (ISSO) (or equivalent) and validation of the Sponsoring Organization. The CA or RA records the steps taken to verify this required information as a part of the Certificate application record.

In addition to the authentication of the Subscriber (and their organization when required), the following

procedures shall also be performed:

- The Custodian (e.g. authorized third party), ISSO or equivalent is responsible for ensuring control of the Private Key, including maintaining a list of any Users who have access to or use of the Private Key, and accounting for which User had control of the Private Key at what time.
- The subjectName DN shall not imply that the subject is a single individual, e.g. by inclusion of a human name form without also clearly indicating the group nature of its issuance; and
- The Custodian (e.g. authorized third party), ISSO or equivalent is responsible to maintain a list of those holding the shared Private Key that must be provided to, and retained by, the applicable CA or its designated representative.

NOTE: These obligations are conveyed to the ISSO or equivalent, through the Certificate registration form that is signed by the ISSO and also authorizes the Applicant to be issued a Custodian managed Certificate under the organization for which the ISSO represents. Users must be identity proofed at a level corresponding to the LoA asserted in the Certificate. If the identity proofing component is performed by the Subscriber Organization, then the compliant RA must retain documentation that the Subscriber Organization is bound through a legally binding contract with or an attestation to the RA to identity proof Users in accordance with the requirements corresponding to the LoA of the associated Certificate. This information must be made available by the Subscriber Organization to the RA upon request.

Antecedent In Person Identity Proofing Events may be used for authentication of Sponsors or Individuals for Group Certificates.

3.2.3.3.4 Verification of NPI Number

For Group Certificates issued to Covered Entities (CE) the LRA must verify that the Applicant provided NPI Number corresponds to the Applicant named in the Certificate application. The NPI Number is verified by using the NPI Registry that is available at https://npiregistry.cms.hhs.gov/, where the LRA will search by the Applicant provided NPI number and confirms that the individual's name returned in the NPI Registry search is that same as the Applicant named in the Certificate application.

3.2.3.4 Authentication of Devices

Devices (i.e., routers, firewalls and Servers) may be named as Certificate subjects. IdenTrust Issues different types of Certificates for such Devices, with the type of Certificate being dependent on the type of Device. IdenTrust verifies the type of Device during I&A according to the Assurance Level of the Certificate applied for. By following such processes IdenTrust reduces the likelihood that the identifying information contained in the Certificate is misleading.

For each Certificate with a Device named as the Certificate subject, the Device must have a human Sponsor, referred to in this CPS as a Primary Machine Operator. The Primary Machine Operator is responsible for providing the following registration information and providing supporting documentation when requested by the RA:

- Equipment identification – Subscribing Organization's registered domain name/service name (DNS name), Device serial number; FQDN(s) or public IP addresses;
- Equipment Public Keys;
- Equipment authorizations and attributes (if any are to be included in the Certificate); and/or
- Contact information to enable the RA to communicate with the Primary Machine Operator and Subscribing Organization when required.
- Designation of Secondary Machine Operators

The registration information is verified by the LRA. Acceptable methods for performing this authentication

of registration information provided by a Primary Machine Operator and ensuring the information has not been tampered with include, but are not limited to:

- Verification of Digitally Signed messages sent from the Primary Machine Operator; and/or
- Registration by the Primary Machine Operator, with the identity of the Primary Machine Operator confirmed in accordance with the requirements of Section 3.2.3 of this CPS at a level of assurance equal to or higher than that of the Device Certificate being applied for.

3.2.3.4.1 Authentication of Primary Machine Operator

As a part of the Device Registration process, the Primary Machine Operator will be named in the Subscribing Organization Authorization Agreement. Verification of the identity and affiliation of the Primary Machine Operator shall be conducted at the level commensurate with level of verification required for the Device certificate to be Issued. In addition to the responsibilities detailed in Section 3.2.3.4, the Primary Machine Operator is also responsible for the operation and control of a Device and assumes the obligations of Subscriber for the Certificate associated with the Device, including but not limited to a duty to protect the Private Key of the Device at all times and manage Device Certificate lifecycle events.

In the event that Secondary Machine Operators will be designated in conjunction with the Device, then the Primary Machine Operator is also responsible to provide an initial list of Secondary Machine Operators in the Subscribing Organization Authorization Agreement and he or she will be responsible to maintain the list of Secondary Machine Operators, accordingly.

3.2.3.4.2 Authentication of Secondary Machine Operators

Secondary Machine Operators are allowable for the purpose of managing a Device to which a Device Certificate has been Issued, and to act as back up to the Primary Machine Operator to manage certificate Suspension and/or Revocation of the Device Certificate, when needed.

During the Device Registration process, the Primary Machine Operator will designate the Secondary Machine Operator(s) by providing names and contact information for the designees in the Secondary Machine Operators List, which is a part of the Subscribing Organization Authorization Agreement, The Secondary Machine Operators List will be archived as a part of the Device Certificate account record, until and unless the list is updated by the Primary Machine Operator. A Primary Machine Operator may add or remove Secondary Machine Operators by submitting a new Secondary Machine Operators List via an email sent from the Primary Machine Operator's confirmed email address, which is provided in the Subscribing Organization Authorization Agreement. The CA will upload the new Secondary Machine Operators List into the Device Certificate account record to be referenced if an email or phone request for certificate Suspension and/or Revocation is initiated by a Secondary Machine Operator.

Confirmation of Identity and Affiliation with the Subscribing Organization is not required for Secondary Machine Operators.

3.2.3.4.3 Verification of Authorization by Subscribing Organization

Device Certificate Issuance and affiliation is authorized by submission of a Subscribing Organization Authorization Agreement, signed by a Subscribing Organization Authorizing Official.

3.2.3.4.4 Device Issuance

The Authorization Agreement specifies the authorized Primary Machine Operator, specifies any Secondary Machine Operator(s), and authorizes affiliation of the Device Certificate.

3.2.4 Non-Verified Subscriber Information

CAs are prohibited from including unconfirmed Subscriber information in Certificates. This prohibition is

enforced by IGC Certificate Profiles and procedures in this CPS, which only allow verified information to be included in Certificates.

3.2.5 Validation of Authority

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

Certificates that assert Affiliation are Issued only after verification of Applicant Affiliation with an authoritative source within the Subscribing Organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a reliable means of communication.

Once a Subscribing Organization has been authenticated (see Section 3.2.2) and has entered into a Subscribing Organization Authorization Agreement naming a Subscriber as an Authorizing Official, the Authorizing Official may appoint and remove other Authorizing Officials (or Sponsors) who are authorized to approve affiliation of Applicants and Devices, and to request Certificate lifecycle events for the Subscribing Organization, e.g., request Suspension of a Subscriber's Certificate or request Revocation of a Subscriber's Certificate in the event Organization-Individual affiliation is broken. CAs are required to maintain a list of Subscribing Organization Authorizing Officials.

CAs and RAs may rely on TAs to provide documentary proof that I&A has been performed according to Section 3.2.3. CAs and RAs may rely on Internal TAs to provide documentary proof that I&A has been performed according to Section 3.2.3, and to indicate Subscribing Organization authorization to Affiliate an Applicant or Device with the Subscribing Organization.

In the instance where an Applicant applies for an Affiliated Certificate and there is no Internal TA, the Applicant is provided a Subscribing Organization Authorization Agreement and instructed to have it signed by an officer or Individual of the Subscribing Organization able to agree to and bind the Subscribing Organization to its duties and obligations as described in the Agreement. If Organization identity has not already been established, the LRA verifies Organization identity according to the processes identified in Section 3.2.2 prior to approving Issuance of the Affiliated Certificate.

Certificates issued to Subscribers do not assert authority to act on behalf of the Subscribing Organization in any implied capacity.

3.2.6 Criteria for Interoperation

To ensure PKI interoperability, IdenTrust:

- Operates a PKI that has undergone a successful compliance audit pursuant to Section 8 of this CPS;
- Requires that all External RA organizations complete an annual audit by an independent third-party and provide audit results to IdenTrust;
- Issues Certificates compliant with the profiles described in IGC Certificate Profiles; and
- Makes IGC PKI Certificate Status information available to Relying Parties in accordance with Section 2 of this CPS.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

3.3.1.1 Subscribers – Basic and Medium

For routine Re-Key requests, identity may be established through use of a previously Issued and still valid Private Key of a Signing Certificate, except that identity shall be established through initial registration process at least once every nine years from the date identity was originally established.

To establish proof of possession, the Subscriber presents his or her Certificate to establish a Client-authenticated SSL/TLS-encrypted Session, requiring use of the Private Key. IdenTrust's RA Systems further validate the authenticity of the Certificate presented by verifying that the Certificate was Issued by the IGC PKI, 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. The RA System requires that the IGC Certificate utilized for identification be of an Assurance Level equal to or higher than 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.

3.3.1.2 Subscribers – PIV-I

I&A for Re-Key of PIV-I Certificates may be initiated by an LRA through a CMS. In such cases the Subscriber authenticates through presentation of his or her fingerprint that must match the Subscriber's fingerprint stored on the same smart card on which the Subscriber's PIV-I Certificates to be Re-Keyed are stored. Following such authentication, the CMS can write new Certificates to the smart card.

Utilization of a previous identity proofing event for routine Re-Key requires that the Subscriber not be due for new in-person identification. In the event the Subscriber is due for new in-person identification, the processes described in Section 3.2.3 of this CPS are required to re-establish identity.

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 RA 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 emails with instructions to appear in-person before an RA for identity proofing, if required, beginning 90 days prior to Certificate expiration.

3.3.1.3 LRAs

The process for Re-Keying LRAs is the same as for Subscribers.

3.3.1.4 Sub CAs, RAs and the Cross-Certifying Bridge CA

The I&A process for Re-Keying Sub CAs, RAs and Cross-Certifying Bridge CAs is the same as stated above, except that if it has been more than three years since identity was established, it must be re-established. Certificate validity is as defined in the table in Section 6.3.2.

3.3.2 Identification and Authentication for Re-Key after Revocation

Suspended, Revoked, or expired IGC Certificates cannot be Re-Keyed. Subscribers without a valid IGC Certificate will be re-authenticated by the CA or RA through a completely new IGC Certificate application.

3.4 Identification and Authentication for Revocation Request

Revocation requests authenticated on the basis of the Certificate's associated Key Pair are always accepted as valid. The identity of the person submitting a Revocation request in any other manner is authenticated in accordance with Section 4.9.3. Other Revocation request authentication mechanisms may be used as well, including a request in writing signed by the Certificate Holder and sent via U.S. Postal Service First-class mail, or UPS, FedEx, DHL, Airborne Express, TNT, Emery, etc., in a sealed, tamper-evident envelope). These authentication mechanisms balance the need to prevent unauthorized Revocation requests against the need to quickly Revoke Certificates and are explained in Section 4.9.

3.4.1 Revocation Requests Submitted by a RA

In the event a Subscribing Organization is also an RA, a revocation request for any Certificate associated with such Subscribing Organization must consist of:

- A verbal request for revocation initiated by a Subscribing Organization manager can be executed as long as a) the requesting manager is known to the LRA or can be confirmed by the LRA as a Subscribing Organization manager; and b) such manager can be authenticated as currently in that managerial role; and c) such manager has authority over the function associated with the certificate, or manages the individual named as the Subscriber of the certificate to be revoked; or
- A digitally signed email request from a Subscribing Organization manager can be executed as long as a) the requesting manager is known to the LRA or can be confirmed by the LRA as a Subscribing Organization manager; and b) such manager can be authenticated as currently in that managerial role; and c) such manager has authority over the function associated with the certificate, or manages the individual named as the Subscriber of the certificate to be revoked; or
- Receipt of a list via email from an authorized representative of that Subscribing Organization's human resources department, which list identifies terminated employees or representatives of the Subscribing Organization and a) the authorization of such authorized representative is pre-established; or b) the authorization of such authorized representative can be confirmed by the LRA via confirmation through the Subscribing Organization's human resource department; or
- A Certificate revocation request can be executed based on the removal of an individual named as the Subscriber of such Certificate from a directory used by the Subscribing Organization as an authoritative data source for information regarding employees or representatives; or
- Other methods that support a Subscribing Organization's requirements for Revocation.

4 CERTIFICATE LIFE-CYCLE

4.1 Application

IdenTrust, when operating as a CA participating in a cross-certified program (such as Federal Bridge, DirectTrust and SAFE SBCA) complies with all requirements specific to the application and acceptance of cross-certificates as specified in the governing CP document for such cross-certified policy. The IdenTrust PMA must authorize the applications for cross-certification with an external policy prior to IdenTrust personnel processing applications for cross-certificates under such program.

All communications among CAs, RAs, LRAs, TAs, Subscribers and Applicants supporting the Certificate application and Issuance process are authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the Certificates being Issued. When an IGC Certificate Private Signature Key is used to authenticate to IdenTrust systems for the purpose of Issuance of another IGC Certificate, the Certificate used must of the same or higher Assurance Level than the Certificate to be Issued. Any electronic transmission of personal information and shared secrets is encrypted using a means commensurate with the type of transmission and the sensitivity of the data.

4.1.1 Submission of Certificate Application

Who can submit a Certificate application varies with the entity to which the Certificate is Issued and whether affiliation with a Subscribing Organization is to be asserted.

4.1.1.1 Individual Unaffiliated Certificates

For Individual Unaffiliated Certificates an application may be submitted by:

- An Individual who agrees to the terms of the Subscriber Agreement; or
- An Individual who is already a Subscriber, holding a valid, unexpired IGC Certificate of the same or higher Assurance Level than the Certificate being applied for.

4.1.1.2 Individual Affiliated Certificates

For Individual Affiliated Certificates an application may be submitted by:

- An Individual who agrees to the terms of the Subscriber Agreement; or
- An Individual who is already a Subscriber, holding a valid, unexpired IGC Certificate of the same or higher Assurance Level than the Certificate being applied for;
- An Authorizing Official or Sponsor of a Subscribing Organization with which the Applicant is to be affiliated;
- An Internal TA as authorized by a Subscribing Organization in accordance with Section 3.2.5; or
- A compliant Custodian (e.g. authorized third party) creates the Certificate Signing Request based on input received from the Subscriber as validated by the RA or CA during the identity proofing process.

4.1.1.3 PIV-I Certificates

For PIV-I Certificates an application may be submitted by:

- An Individual who appears in person and agrees to the terms of the Subscriber Agreement; or
- An Individual who appears in person and is already a Subscriber, holding a valid, unexpired IGC PIV-I Certificate.

4.1.1.4 Device Certificates

For Device Certificates an application may be submitted by:

- An Individual who agrees to the terms of the Subscriber Agreement and to undergo Individual identity proofing as specified in Section 3.2.3.1;
- An Individual who is already a Subscriber, holding a valid, unexpired IGC Certificate of the same or higher Assurance Level than the Certificate being applied for;
- An Authorizing Official or Sponsor of a Subscribing Organization with which the Applicant is to be affiliated; or
- An Internal TA as authorized by a Subscribing Organization in accordance with Section 3.2.5.

4.1.1.5 LRA Certificates

For LRA Certificates an application may be submitted by:

- An employee, contractor or agent of a CA or RA who has been appointed as an LRA by an Organization Authorizing Official. Authorizing Officials for entities other than IdenTrust are specified in their relative agreements, e.g., Participant CA Agreement, RA Agreement, or in a Certificate of Incumbency.

4.1.1.6 RA Systems Certificates

For RA Systems Certificates an application may be submitted by:

- An employee, contractor or agent of a CA or RA who has been appointed as an RA Administrator by an Organization Authorizing Official. Authorizing Officials for entities other than IdenTrust are specified in their relative agreements, e.g., Participant CA Agreement, RA Agreement, or in a Certificate of Incumbency in accordance with Section 3.2.2.

4.1.1.7 Participant CA Certificates

For Participant CA Certificates an application may be submitted by:

- The authorized representative of the Participant CA who is named as such in a Participant CA Agreement or in a Certificate of Incumbency in accordance with Section 3.2.2.

4.1.1.8 Bridge CA Cross Certificates

For Bridge CA Cross Certificates an application may be submitted by:

- For a Cross-Certifying bridge, the Chief Technology Officer (CTO) and/or those persons appointed for Cross-Certification activities through a Memorandum of Agreement ("MOA") or in a Certificate of Incumbency in accordance with Section 3.2.2.
- For IdenTrust, the person(s) appointed by the IdenTrust PMA or the IdenTrust Chief Information Officer (CIO) and specified in an MOA.

4.1.2 Enrollment Process and Responsibilities

Upon initiation of a Certificate application by an authorized Individual or Organization as described above in Section 4.1.1, Applicant identity information is collected and identity established according to the processes described in Section 3.2. If the requested Certificate is Affiliated, Subscribing Organization identity and authorization for affiliation is also established in accordance with Section 3.1.

4.1.2.1 Establishment of Identity

For IGC Basic Software Certificates, identity is deemed to have been established on the day the RA System successfully completes automated identity verification, or if an in-person identity proofing process was utilized, the date the I&A information is received and entered into the system by the LRA.

For all other IGC Certificates, identity is deemed to have been established only after the I&A documentation

is reviewed by the LRA, approved by the LRA and entered by the LRA into the RA System. The date of identity establishment is deemed the date the I&A paperwork is entered into the RA System as approved by the LRA.

Upon completion of the registration process, all identity-related data for the Applicant and establishment thereof has been recorded in the RA System database.

The following Sections discuss in more detail the collection and verification of identity data, and Certificate Issuance processes.

4.1.2.2 Information Collection

During the application phase of registration, Applicant information required for identity verification is collected in one of the following manners:

- Applicants may provide registration information through an online Certificate application process via a Server-authenticated SSL/TLS secured web site hosted by IdenTrust;
- Applicants, assisted by a LRA or TA during an in-person identity proofing process may provide identity information into an EWS connected to an RA System and/or CMS;
- Internal TAs, as authorized by a Subscribing Organization in accordance with Section 3.2.5, may submit identity information for Individual Applicants or for multiple Applicants via a bulk load process as described in Section 4.1.2.2.; or
- Subscribing Organization Sponsors, as authorized by a Subscribing Organization in accordance with Section 3.2.5, may provide identity information for an Individual Applicant or multiple Applicants via an online Certificate application process over a Server-authenticated SSL/TLS secured web site or through a secure web services interface hosted by IdenTrust.

All Applicant information required for the type of Certificate to be Issued is collected through one of the above processes.

For PIV-I Hardware Certificates, the LRA or TA-assisted method through the EWS is required for collection of biometric data. The process for PIV-I data collection is more fully described in Section 4.1.2.7.

In addition to Applicant information, a hash of the Account Password selected by the Applicant is collected, which is later utilized with an Activation Code provided to the Applicant to authenticate to the RA System at the beginning of a Certificate retrieval process.

As part of the registration process, the Applicant is required to create three questions and secret answers, which together serve as a mechanism to reset their Account Password in case they forget it before they are able to download their Certificate. The reset Account Password process is activated by the Subscriber providing his or her Activation Code, which was received initially in a letter when the account was first opened and by clicking on an Account Password reset URL. This process sends an OTC and specified URL to the email address, or alternatively to the mobile phone number on file for the Subscriber. After receiving the OTC, the Subscriber must enter both the Activation Code and the OTC at the specified URL in order to gain access to the three questions that were selected during registration. (The three questions were selected by the Subscriber from a list of ten randomly selected questions that were randomly generated from a pool of password-reset questions.) If the answers are correct, the Subscriber is allowed to change the Account Password, which is immediately hashed and stored in the RA system for further use.

4.1.2.3 Information Collection via Bulk Loading by a Trusted Agent

TAs, as defined in Section 1.3.5, perform in-person identification of Applicants and collect the Applicant identity information as described in Section 3.2.3.1 of this CPS into a bulk Certificate Issuance request.

The TA views the forms of identification provided and confirms the accuracy of the photograph on the photo ID against the appearance of the Applicant. The forms of ID and identifying information for each is entered

into the bulk Certificate request for each Applicant. Internal TAs may utilize information from an Antecedent In-Person Appearance; in which case the bulk Certificate request includes the additional information normally required on an ID Form (see Section 3.2.3.1.3).

The bulk Certificate request is Digitally Signed by the TA and delivered in a secure manner to the RA so as to ensure non-repudiation of the bulk Certificate request and ensure integrity and confidentiality of data during transport. This is accomplished either through upload of the Digitally Signed bulk Certificate request through a Server-authenticated SSL/TLS secured web site, sending a Digitally Signed and encrypted email, or sending physically via courier in a sealed, tamper-proof envelope to the CA or RA.

A Subscribing Organization that is an RA may utilize a CMS to support automated batch collection of information to support Certificate Issuance from a data source maintained and kept current by that Subscribing Organization's human resources department, such as an electronic file listing those persons employed by the Subscribing Organization.

4.1.2.4 Documents Provided to Applicants

All Applicants are required to Accept a Subscriber Agreement acknowledging their duties and obligations, and to sign a declaration of identity.

Applicants utilizing an online registration process are required to Accept an online Subscriber Agreement during the registration process. Acceptance of the online Subscriber Agreement is recorded by the RA System. If the Subscriber Agreement is not Accepted, the application process is terminated.

Applicants appearing for an in-person identity proofing per Section 3.2.3.1 are provided or may download a forms package that includes:

- An In-Person Identification Form ("ID Form"), which Applicants are instructed complete and take to an approved Registrar, which may be an LRA, TA, Notary or other Individual certified for in-person identity proofing per Section 3.2.3.1.2 of this CPS. The ID Form includes a declaration of identity and Applicant Agreement to the Subscriber Agreement and is required to be signed in ink in the presence of the Registrar. It also includes Registrar instructions, and boxes or lines for the Registrar to initial or fill in when verifying the accuracy of the identifying information presented; and
- For Affiliated Certificate applications, where affiliation has not already been authorized by a Subscribing Organization or Internal TA, a Subscribing Organization Authorization Form with instructions to have the form signed by an Authorizing Official of the Applicant's Subscribing Organization. The Subscribing Organization Authorization Agreement may be signed in ink or may be Digitally Signed.

4.1.2.5 In-Person Verification of Identity Using the ID Form

The Applicant signs the ID Form in the presence of the Registrar, who then performs the following:

- Records the type, serial numbers and expiration dates for the identification documents presented by the Applicant;
- Verifies that the identification documents are protected against forgery, modification, or substitution (e.g., holograms and other security features), and 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
- Signs (or notarizes if the Registrar is a notary) the ID Form.

The Applicant's ID Form contains:

- A record of the identity of the Registrar;

- A signed declaration by the Registrar that he/she confirmed the identity of the Applicant;
- A record of the credentials used to verify the Individual's identity (e.g. ID type and number); and
- A record of the date of the in-person identity confirmation.

4.1.2.6 Verification of Identity using the ID Form for Internal Trusted Agents

Internal TAs may utilize data from an Antecedent In-Person Appearance as described in Section 3.2.3.1.3. The ID Form for Internal Trusted Agents allows the Internal TA to specify whether data collected in from an Antecedent In-Person Appearance and provide additional identity information used to authenticate the Applicant as part of the Certificate binding process. The data collected and verification process is fully described in Section 3.2.3.1.3.

The LRA enters the date of the Antecedent In-Person Appearance from the ID Form into the RA System as the date identity was established.

4.1.2.7 Submission of Forms

The ID Form and the Subscribing Organization Authorization Agreement (if required) are submitted to the CA or RA either by courier in a sealed, tamper evident envelope, Digitally Signed and submitted through a Server-authenticated SSL/TLS secured web site, or sent in a Digitally Signed and encrypted email.

In the case in which the Registrar is other than a LRA or TA, the Applicant submits all the application information directly to the applicable CA or RA by courier in a sealed, tamper evident envelope.

In the case in which the Registrar is a TA or LRA, the Applicant, TA or LRA may submit the information either by courier in a sealed, tamper evident envelope. To reduce processing time, the LRA or TA may Digitally Sign and submit the information through a Server-authenticated SSL/TLS secured web site, or in a Digitally Signed and encrypted email.

For the purposes of electronic submission, ID Forms may be scanned and sent by LRAs and TAs, provided the scan is in full color and of suitable quality for viewing by the LRA, and provided the submission is Digitally Signed by the LRA or TA.

Digitally Signed Subscribing Organization Authorization Agreements may be submitted via email by the Applicant, an Authorizing Official of the Subscribing Organization, a RA or a TA.

4.1.2.8 In-Person Verification of Identity for IGC PIV-I Hardware Certificates

For PIV-I Hardware Certificates, verification of identity is required to be conducted in-person, by a LRA or TA. Other Registrars such as Notaries are not permitted. The identity proofing session is conducted utilizing an EWS securely connected to the CMS that steps the LRA or TA through the registration process with the Applicant. Forms of ID may be captured through entry of identity document data into the CMS directly by the LRA or TA or through the use of ID Forms.

The LRA or TA assists the Applicant through an online registration process, collecting from the Applicant any required information not already supplied by a Subscribing Organization Sponsor. The LRA or TA physically reviews, records identity document description and numbers, and enters the information into the CMS. In such cases where a paper ID Form is utilized, the ID form is scanned and uploaded into the CMS. Use of Antecedent In-Person Appearance data for PIV-I identity verification is not permitted.

The LRA or TA captures and ensures successful recording of both a facial image and fingerprint utilizing biometric capture devices connected to the EWS.

Upon Acceptance of the Subscriber Agreement by the Applicant, the Certificate application is queued in the CMS for review and verification.

4.1.2.9 RA Administrator and LRA Access to RA System Functions

All access to RA Systems, inclusive of a CMS, is authenticated through use of a Private Key corresponding to the LRA or RA Administrator's IGC Certificate.

RA Administrators must be holders of and authenticate with an IGC Certificate of the highest Assurance Level as Issued by the CA in connection with the RA. A LRA must be a holder of and authenticate with an IGC Certificate with an Assurance Level equal to or higher than the Assurance Level of the Certificates on which they will be performing LRA duties. Additionally, the authority of the person to act as LRA or RA Administrator must be confirmed by an Authorizing Official of the RA through submission of an Authorization Form signed or Digitally Signed by an Authorizing Official. Upon receipt of a properly completed Authorization Form and approval by the applicable CA or RA, the ACL is updated to reflect authorization to use the RA System.

During this same process, access is granted to the RA Administrator or LRA for only those domains or Subscribing Organization name spaces (see Section 3.1.2) that the RA is authorized by the CA or RA to administer.

4.1.2.10 Participant CAs

Prior to the Key Generation process discussed in the Section 6.1.1, the Applicant for a Participant CA Certificate must first enter into a Participant CA Agreement with IdenTrust. During this contracting process, personnel authorized to act on the Applicant's behalf for purposes of Key Generation and Certificate Issuance are identified. If necessary for confirmation of identity during an in-person visit to IdenTrust by such authorized representative, IdenTrust may request, review, and obtain a copy of the representative's Government-Issued Photo ID.

4.1.2.11 Bridge Cross-Certificate

Authorized representatives of Cross-Certifying bridges are identified in accordance with Section 3.2.2. If necessary to confirm the identity of the authorized representative during an in-person visit to IdenTrust, IdenTrust may request, review, and obtain a copy of the representative's Government-Issued Photo ID.

4.2 Certificate Application Processing

Information in Certificate applications must be verified as accurate before Certificates are issued. The following procedures are to be used in verifying information in Certificate applications.

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 Individuals and Devices

Identity of Applicants is established according to the procedures defined in Sections following the procedures defined in Section 3.2.3.1.

For Certificates asserting Assurance Level of Basic, when performance of I&A is an automated function and there is no in-person identity proofing.

For IGC PIV-I Certificates, the LRA or TA utilizes the EWS connected to the CMS to guide the Applicant through the Applicant enrollment process, including capture of the Applicant's identity source documents, collection of biometric data, Applicant's entry of a Subscriber's Account Password, and Acceptance by the Applicant of the Subscriber Agreement within the EWS as well as execution by the Applicant of a declaration of identity, in each case as provided for in Section 3.2.3.1.

For all other Certificates that are Issued to Individuals, and Certificates asserting Assurance Level of Basic where an in-person identity proofing process has been used, the Registrar examines the identification documents for the Applicant as specified in Section 3.2.3.1. The Applicant, in the presence of the Registrar,

signs the ID Form, which includes a declaration of identity. Upon successful verification of identity, the Registrar signs (or notarizes, if a notary) the ID Form.

When a Certificate can be Issued immediately after the Registrar collects and examines the Subscriber's information, the Registrar can sign the ID form and then the Applicant can Digitally Sign the declaration of identity with the newly Issued Certificate.

In the case of Certificates asserting PIV-I Hardware Assurance Level requiring the collection of biometric data (e.g., fingerprints and facial image), these data are also collected and examined by the TA or LRA along with the other documentation described above.

4.2.1.2 Local Registration Authorities

Local Registration Authorities are identified and Issued Certificates as Individuals. (Based on the Public Key and a Certificate thumbprint added to the ACL, the LRA is granted rights to perform RA functions). Prior to updating the ACL for RA functions, an IdenTrust LRA Authorization Form signed by the RA's Authorizing Official is submitted to IdenTrust and reviewed by an IdenTrust LRA to confirm the LRA's appointment by the RA. The LRA is granted Certificate management rights only for those domains or namespaces that the LRA has been authorized to administer.

4.2.1.3 Representatives of RAs, Participant CAs and the Bridge CAs

Representatives of RAs, Participant CAs and the Bridge(s) CA(s) are identified through ordinary business processes that include confirming position, title and chain-of-command through correspondence on official letterhead, Digitally Signed e-mail, by telephone, through the contract negotiation process and by the execution of written contracts, which designate authorized representatives, as described in Section 3.2.2. If necessary to confirm the identity of an authorized representative during an in-person visit to IdenTrust, IdenTrust may request, review, and obtain a copy of the representative's Government-Issued Photo ID.

4.2.2 Approval or Rejection

Guidelines for Approval or Rejection of Certificate Applications are provided in the following sub-sections.

4.2.2.1 By Certificate Assurance Level

4.2.2.1.1 Basic Assurance

For Certificates asserting an Assurance Level of Basic for which automated identity proofing has been successfully completed, approval or rejection is an automated process as described in Section 3.2.3.1. Where automated identity proofing has been utilized, the RA System records the date of approval as the date identity was established.

4.2.2.1.2 Medium Assurance

For Medium Assurance certificates, an authorized LRA is responsible for the approval or rejection of an application. The LRA must be an Individual different from any Registrar used for collection of Applicant information, i.e. an LRA involved in the process of collecting information for a given Applicant is prohibited from approving that Applicant's Certificate application to maintain Multi-Person control.

IdenTrust maintains a list of Public Keys and Certificate thumbprints of LRAs that are authorized to submit Certificate approvals, and the RA system restricts LRAs to those domains or namespaces for which the LRA is authorized to approve.

To approve or reject non-PIV-I Certificate applications, the LRA accesses the web-based Certificate management interface of the RA System via a Client-Authenticated SSL/TLS-Encrypted Session, authenticated through use of the LRA's Medium Hardware or PIV-I Hardware Signing Certificate Private Key, whose

corresponding Public Key has been registered in the RA System's ACL.

If necessary, the LRA uploads into the system the application that has been verified or will be verified. For Certificate applications that are submitted using an electronic registration process, the LRA does not have to upload the information in the system but is required to compare the information in the applications with the information in the database. The LRA verifies the completeness of the application, the completion of all required forms, and ensures all information used to identify the individual has been adequately verified. Any information not already verified, e.g. identity of Subscribing Organization, is verified by the LRA. The LRA then approves or rejects the application, and if approved the Certificate is queued by the RA System for Issuance. The LRA records the date of the in-person identity proofing into the RA System as the date identity was established.

4.2.2.1.3 PIV-I Assurance

For Certificates asserting Assurance Level of PIV-I Hardware, a CMS is used to manage the Certificate approval process. The CMS maintains an ACL of the PIV-I Certificate thumbprints and Public Keys of LRAs authorized to approve PIV-I Certificate applications. The CMS restricts LRAs to those domains or namespaces for which the LRA is authorized to approve.

For Certificate applications where a LRA or TA conducts an assisted enrollment of the Applicant through an EWS, the LRA does not have to upload any additional information, but is required to ensure the completeness of the application, that required Applicant and biometric data has been collected, that the Subscriber Agreement was electronically Accepted within the EWS by the Subscriber, and that that the application was Digitally Signed by the LRA or TA within the EWS. Verification is conducted through the CMS, which programmatically ensures each of the required steps is completed and allows the LRA to view all application data. The LRA then approves or rejects the application, and if approved the Certificate is queued by the RA System for Issuance. The LRA records the date of the in-person identity proofing into the RA System as the date that identity was established.

4.2.2.2 Binding the Applicant to the Certificate

Binding between the Applicant and the information provided in the application is conducted in an automated manner for email addresses and/or mobile phone numbers as described in Section 3.2.3.1.1. This binding also serves as a methodology to deliver Activation Data in the form of an OTC to the Applicant as part of the registration process.

Binding between the Applicant and the approved application in the RA System or CMS is maintained in one or more of the three following ways:

1) For the applications based on information submitted online (see processes described on 4.3.1.3 and 4.3.1.4), 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 Data to the Applicant using a verified piece of information from the application as an OOB 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;

2) For applications based on information that the Registrar submits directly to the RA System (see processes described in Sections 4.3.1.1 and 4.3.1.2), the LRA manually approves the application prior to submitting the information to the system, ensuring the binding between the Applicant database record and the verified Applicant. Then, when using the RA System, the LRA provides Activation Data to the Applicant using a verified piece of information from the application as an OOB delivery method (e.g., physical address, email address or mobile phone). In order to retrieve the Certificate, the Applicant must provide the Activation Data provided by the LRA; or
3) For PIV-I Hardware Certificates, binding between the Applicant, the registration process and the Certificate is through Applicant use of biometric data at time of card and Certificate activation. This is accomplished through the EWS, whereby biometric data (Applicant/Subscriber fingerprints and facial image) is provided at the time of Certificate activation, and compared to the biometric data collected during the application process and stored in the CMS. Such comparison of biometric data must be successful in order for the activation process to be initiated.

The binding processes between Subscriber, Certificate and Cryptomodule are more fully described in Section 4.3.1.

4.2.2.2.1 Individuals

The LRA reviews the identity confirmation forms, authorization forms, and any other supporting documentation submitted by Applicants, Subscribing Organizations or Registrars (e.g., photocopies of identity documents and biometric data) to determine for each Applicant that the identifying information is (i) internally consistent, and (ii) consistent with the information contained in the application for the Certificate.

For all applications received, the LRA ensures the following minimum information is recorded in the RA System or CMS:

- Applicant's name as it appears in the Applicant's request for a Certificate;
- Method of application (i.e., on-line or in-person) for each data element accepted for proofing, including electronic forms;
- Name of document(s) presented for identity proofing, including:
  - Issuing authority;
  - Date of Issuance;
  - Date of expiration; and
  - All fields verified;
- Source of verification (i.e., which databases used for cross-checks);
- Method of verification (i.e., on-line, in-person) ;
- Date/time of verification as the date identity was established;
- Names of Subscribing Organizations or IVPs providing identification services, if any;
- Fields that failed verification, if any;
- Status of current registration process (Suspended or ended);
- All identity verification data;
- All associated error messages and codes, if any; and
- Date/time of process completion or Suspension.

An LRA may approve Certificate Issuance if:

- All steps in Section 3.2 required for the type of Certificate to be issued have successfully been completed; and
- The Certificate fee has been paid (or other satisfactory payment arrangements exist).

The LRA will reject a Certificate application if:

- A required step in Section 3.2 cannot be successfully completed;
- The Applicant fails to respond or does not provide requested documentation within a reasonable timeframe;
- More than 30 days have elapsed since the date identity was established (for all Certificates except IGC Basic);
- The biometric data does not seem to correspond to the Applicant or is not complete;
- Payment has not been received or other satisfactory payment arrangements have not been made; or
- The LRA reasonably believes that Issuance of the Certificate may create an unnecessary risk to the reputation of a PKI Participant.

Upon approval of the Certificate by the LRA, the Certificate is queued for Issuance as described in Section 4.3.

4.2.2.2.2 Devices

Approval or rejection of Device Certificate applications is fully described in Section 3.2.3 of this CPS, Authentication of Devices. Upon completion of the processes described in Section 3.2.3, the Device Certificate application is queued for Issuance as described in Section 4.3 of this CPS.

4.2.2.2.3 LRAs

An application for a Certificate by an LRA is approved or rejected in the same manner as other Subscribers.

4.2.2.2.4 RAs

Registration Authority applications are reviewed by the CA's PMA and approved or rejected based on whether the Organization meets requirements found in the RA Agreement, including financial responsibility (Section 9.2 of this CPS).

4.2.2.2.5 Participant CAs

Applications for Participant CA Certificate Issuance are reviewed by the IdenTrust PMA and approved or rejected based on whether the Organization meets requirements found in the Participant CA Agreement and Section 9.2 (Financial responsibility) of this CPS.

4.2.2.2.6 Bridge CA

An application for a Cross-Certificate to be Issued to a Bridge CA will be reviewed by the IdenTrust PMA and approved or rejected based on the criteria and process in Section 3.2.6 and those agreed upon with the Applicant Bridge CA.

4.2.2.3 Time to Process Certificate Applications

4.2.2.3.1 Individual and Devices

LRAs and TAs will respond promptly to all Certificate applications. This is especially important for Certificates that must be retrieved within 30 days of the date identity was established (all except IGC Basic Software).

Certificates are made available for retrieval by the Applicant following completion of the steps listed in this Section 4.2 and provided that the Public Key has been properly delivered and all other technical prerequisites for Certificate Issuance have been met.

4.2.2.3.2 All Other Certificates

No stipulation.

4.3 Issuance

The process to begin Issuance of a Certificate begins once an IGC Certificate has been approved. Upon Certificate approval, identity proofing is deemed complete and the Applicant becomes a Subscriber in the RA system.

4.3.1 CA Actions During Certificate Issuance

The Issuance processes in this Section are designed to ensure Certificates and their Private Keys are securely bound to the Applicant's registration and the Subscriber. Issuance processes are performed by actors associated with the CA or the RA as identified. Upon Issuance of a Certificate, CA, RA and Subscriber warranties as described in Sections 9.6.1, 9.6.2 and 9.6.3 of this CPS become effective.

An RA may use one or more of the following processes to initiate retrieval of a Certificate that has been approved for issuance as defined in Sections 4.3.1.1 through 4.3.1.6.

4.3.1.1 Activation Code-Account Password Process with Automated I&A

This process is applicable only to IGC Basic Software Individual Subscriber Certificates.

This process uses one Activation Code. In all cases where only one Activation Code is delivered to the Applicant, the Activation Code may be delivered via an email to the Applicant's confirmed email account (see section 3.2.3.1.1) or alternatively the Activation Code may be delivered via a blind mailer (PIN mailer) to the applicant provided and confirmed physical mail address (see section 3.2.3.1)

NOTE: Activation codes cannot be used to retrieve an approved certificate without being used in conjunction with a validated Account Password, which is known only to the Applicant. The Account Password is provided by the Applicant during the registration phase of the application process.

For this scenario, the Certificate Issuance process requires initial online enrollment by the Applicant with Applicant identification conducted in an automated manner as described in Section 3.2.3.1.

1) As one of the initial registration steps, the Applicant is directed to a specified secure enrollment site (https://) and initiates a Server-Authenticated SSL/TLS-Encrypted Session. During this online enrollment session, the Applicant creates a profile with the Applicant's name, email address, Organization name and other necessary information. The Applicant also creates an Account Password to be used later during Certificate retrieval. A hash of the Account Password is submitted to the RA System.
2) Also during the initial online enrollment session, the Applicant's email address is automatically verified through delivery of an OTC needed to further progress the registration via an OOB method as described in Section 3.2.3.1.1.
3) After the RA System successfully completes automated I&A, an Activation Code is randomly generated by the system and emailed to the Applicant's verified email address. Alternatively, the Activation Code may be mailed to the Applicant's confirmed mail address in a PIN-mailer or in a tamper-evident envelope.
4) The Applicant is instructed to access a specified secure retrieval site (https://), that is either hosted by the RA System where a Server-Authenticated SSL/TLS-Encrypted Session is initiated. For authentication purposes, the Applicant enters the Account Password and Activation Code to proceed.[7] The Applicant is presented with the Subscriber Agreement and must Accept it to continue.

[7] For all Certificates except IGC Basic Software, a 30 day period is calculated based from the date identity was established. The 30 day period begins from the date the I&A is approved by the LRA and entered by the LRA into the RA System. If more

5) The Applicant continues with the Key Generation, Certificate generation[8], and Certificate loading process during which the Certificate Issuance system ensures that the appropriate Cryptomodule and Key lengths are being used. To ensure that Keys are properly generated and stored in Cryptomodule that meet the requirements of Section 6.2.1, programs are run that enforce restrictions on the Cryptographic Service Providers that can be used by the Applicant. If the required Cryptographic Service Provider is not found, the Applicant receives an error message.
6) The Applicant generates a Key Pair within the boundaries of the Cryptomodule and uses the Private Key to sign the Public Key in an RSA PKCS #10 Certificate request. During this same SSL/TLS session, additional scripts are run by the Certificate Issuance system to ensure that the Key length meets minimum requirements and that the PKCS#10 is valid. Upon verification of the Applicant's Digital Signature on the RSA PKCS #10 Certificate signing request (using the algorithm specified in the request), the requested Certificate is generated by the CA and delivered to the Applicant during this same SSL/TLS session.
7) If there is no requirement for Encryption Key escrow, a second Private Key for an Encryption Certificate is generated using the same method explained in step (6). If there is a requirement for escrow of the Encryption Key, Encryption Keys are created and delivered as explained in Section 6.1.2.

If the Key Generation, Certificate generation, and Certificate loading processes are successful, the Applicant is notified of Certificate Issuance as described below in Section 4.3.2.

4.3.1.2 Activation Code Used in Conjunction with an Account Password following Completion of I&A Processes

This process uses one Activation Code. In all cases where only one Activation Code is delivered to the Applicant, the Activation Code may be delivered via an email to the Applicant's confirmed email account (see section 3.2.3.1.1) or alternatively the Activation Code may be delivered via a blind mailer (PIN mailer) to the applicant provided and mailed to the address provided by the applicant.

NOTE: Activation codes cannot be used to retrieve an approved certificate without being used in conjunction with a validated Account Password, which is known only to the Applicant. The Account Password is provided by the Applicant during the registration phase of the application process.

This scenario requires initial online enrollment by the Applicant where some Applicant data may be submitted by a sponsoring Subscribing Organization or by a Trusted Agent. The Applicant completes the online registration process, which includes review of any Applicant data that has been prepopulated by the RA System and completion of any missing data.

1) As one of the initial registration steps, the Applicant is directed to a specified secure enrollment site (https://) and initiates a Server-Authenticated SSL/TLS-Encrypted Session. During this online enrollment session, the Applicant creates a profile with the Applicant's name, email address, Organization name and other necessary information. The Applicant also creates an Account Password to be used later during Certificate retrieval. A hash of the Account Password is submitted to the RA System.

---

than 30 days have passed since the date identity was established, the system prevents the Applicant from proceeding with Key Generation and notifies them that in-person identification must be repeated.

[8] The Certificate's Subject Distinguished Name (DN) is assembled at this point. All information used in the DN is taken from the verified application data provided to the CA system by the LRA. The Common Name and Organization fields are populated with exactly the same information entered in the application. The Country field is optionally populated with the ISO 3166 standard 2-character code that represents the country in the application. The Organization Unit is populated with a unique ID generated as explained in section 3.1.5.

2) Also during the initial online enrollment session, the Applicant's email address is automatically verified through delivery of an OTC (Activation Data) needed to further progress the registration via an OOB method as described in Section 3.2.3.1.1.
3) After the LRA approves Certificate Issuance (via Client-Authenticated SSL/TLS-Encrypted Session), an Activation Code is randomly generated by the system and is either emailed to the verified email account or alternatively the Activation Code may be mailed to the address provided by the applicant.
4) The Applicant is also instructed to access a specified secure retrieval site (https://), that is either hosted by the RA System where a Server-Authenticated SSL/TLS-Encrypted Session is initiated. For authentication purposes, the Applicant enters the Account Password and Activation Code to proceed. The Applicant is presented with the Subscriber Agreement and must Accept it to continue.
5) The Applicant continues[9] with the Key Generation, Certificate generation[10], and Certificate loading process during which the Certificate Issuance system ensures that the appropriate Cryptomodule and Key lengths are being used. To ensure that Keys are properly Generated and stored in Cryptomodule that meet the requirements of Section 6.2.1, programs are run that enforce restrictions on the Cryptographic Service Providers that can be used by the Applicant. If the required Cryptographic Service Provider is not found, the Applicant receives an error message.
6) The Applicant generates a Key Pair within the boundaries of the Cryptomodule and uses the Private Key to sign the Public Key in an RSA PKCS #10 Certificate request. During this same SSL/TLS session, additional scripts are run by the Certificate Issuance system to ensure that the Key length meets minimum requirements and that the PKCS#10 is valid. Upon verification of the Applicant's Digital Signature on the RSA PKCS #10 Certificate signing request (using the algorithm specified in the request), the requested Certificate is generated by the CA and delivered to the Applicant during this same SSL/TLS session.
7) If there is no requirement for Encryption Key escrow, a second Private Key for an Encryption Certificate is generated using the same method explained in step (6). If there is a requirement for escrow of the Encryption Key, Encryption Keys are created and delivered as explained in Section 6.1.2.

4.3.1.3 Activation Code Delivered via Hardware Installation Kit

For Certificates stored on hardware, a Cryptomodule installation kit may be sent to either an Applicant or the TA. The Cryptomodule installation kit contains the Cryptomodule and Cryptomodule interface device (e.g. card reader), software drivers for the Cryptomodule (which includes the Cryptographic Service Provider necessary to operate the Cryptomodule), and instructions for the Applicant to follow to activate the Cryptomodule. Only when two Activation Codes are sent to the Applicant may an Activation Code also be sent with the Cryptomodule Installation Kit so that in any case, at least one Activation Code is delivered directly to the Applicant in a channel that is separate from the delivery of the Cryptomodule.

4.3.1.4 PIN-Protected-Cryptomodule Process

This method is available only for IGC Certificates retrieved to hardware Cryptomodules prior to sending to

[9] For all Certificates except IGC Basic Software, a 30 day period is calculated based from the date identity was established. The 30 day period begins from the date the I&A is approved by the LRA and entered by the LRA into the RA System. If more than 30 days have passed since the date identity was established, the system prevents the Applicant from proceeding with Key Generation and notifies them that in-person identification must be repeated.

[10] The Certificate's Subject Distinguished Name (DN) is assembled at this point. All information used in the DN is taken from the verified application data provided to the CA system by the LRA. The Common Name and Organization fields are populated with exactly the same information entered in the application. The Country field is optionally populated with the ISO 3166 standard 2-character code that represents the country in the application. The Organization Unit is populated with a unique ID generated as explained in section 3.1.5.

the Subscriber

After approval of Certificate Issuance by the LRA (during a Client-Authenticated SSL/TLS-Encrypted Session), a Key Pair and Certificate are generated and installed on the Subscriber's Cryptomodule by an LRA. The Cryptomodule is immediately protected with an Activation Code generated by the RA System. The Activation Code and Cryptomodule Installation Kit are sent by the LRA through separate channels to the Applicant. To enforce principles of Separation-of-Duties/Multi-party Control, two LRAs (LRA-1 and LRA-2) are involved in the Certificate Issuance process. An RA System (described in Section 1.3.3) is located in a secure room at an RA site (see Sections 5.1.1.3 and 5.1.1.4). LRA-1 generates[11] the Signing Key Pair for the Subscriber within the boundaries of an approved Cryptomodule while the Cryptomodule is connected to the RA System. The Private Key is used to sign the Public Key in an RSA PKCS #10 Certificate signing request. In a Server-authenticated SSL/TLS-encrypted session (see Definitions), the PKCS#10 is transmitted to the CA within a Digitally Signed data structure (e.g., XKMS/XSMS). The CA system verifies the Digital Signature of the RA System on the data structure. The PKCS#10 is processed to confirm that the request was signed with the Private Key corresponding to the Public Key contained in the request. Upon verification of the Digital Signature on the PKCS#10 Certificate signing request (using the algorithm specified in the request), the requested Certificate is generated[12] by the CA, returned to the RA System, and installed on the Cryptomodule in a PKCS#7 format by the RA System. Depending on whether the Encryption Keys are escrowed or not, the Private Keys will be generated as explained above for non-escrowed Key; or, for escrowed Keys, they are created and delivered as explained in Section 6.1.2.

1) The Cryptomodule is protected by an Activation Code that is randomly generated by the RA System and delivered to LRA-2 in a sealed PIN-mailer, or is immediately sealed by LRA-2 in a tamper-evident envelope. LRA-2 sends the Activation Code to the Applicant separately by mail or courier in a tamper evident envelope. As part of system configuration and the assignment of access rights, separate role-based privileges are designated for LRA-1 and LRA-2 so that one role can only generate the Key Pairs and the other can only generate the Activation Code, as described above. Alternatively, the Activation Code may be sent to the Applicant's verified email address.
2) Immediately after installing the Certificate on the Cryptomodule, LRA-1 attaches the Subscriber's name to the Cryptomodule, places the Cryptomodule in an Installation Kit and marks the kit for delivery purposes with the name and address of the Applicant (or the name and address of the Trusted Agent). The Cryptomodule Installation Kit is sent through a separate channel to the Applicant or TA.

Later when the Applicant has received the Activation Code and the Cryptomodule Installation Kit, the Applicant is instructed to activate the Cryptomodule and immediately replace the initial Activation Code with personally chosen Activation Data. Using his or her Certificate, the Subscriber is instructed to Digitally Sign the Subscriber Agreement and an acknowledgement of receipt of the Cryptomodule using the associated Private Key and to send them to the Registration Authority for record keeping and archival.

[11] For all Certificates except IGC Basic Software, a 30 day period is calculated based from the date identity was established. The 30 day period begins from the date the I&A is approved by the LRA and entered by the LRA into the RA System. If more than 30 days have passed since the date identity was established, the system prevents the Applicant from proceeding with Key Generation and notifies them that in-person identification must be repeated.

[12] The Certificate's Subject Distinguished Name (DN) is assembled at this point. All information used in the DN is taken from the verified application data provided to the CA system by the LRA. The Common Name and Organization fields are populated with exactly the same information entered in the application. The Country field is optionally populated with the ISO 3166 standard 2-character code that represents the country in the application. The Organization Unit is populated with a unique ID generated as explained in section 3.1.5.

4.3.1.5 Activation Code Not Required due to In Person Activation (PIV-I)

For IGC PIV-I Hardware Certificates, the smart card is sent to the RA in advance. At the time of smart card personalization, the EWS interacts with and authenticates the smart card through use of a factory-set key used for initial card communication. The factory-set key is replaced with a diversified key by the CMS as part of the personalization process.

This method is available only for IGC PIV-I Assurance Certificates.

After the Issuance of a Certificate has been approved by the LRA, a TA or a different LRA provides the smart card to the Applicant in order to download Certificates and signed biometric data as part of an assisted card personalization process requiring the Applicant to authenticate using biometrics collected during the registration process.

In the event cards are loaded and personalized using a batch process, each card is locked until the applicable Applicant is available for card Activation. The Applicant authenticates during the Activation process by using biometrics collected during the certificate application process (Applicant/Subscriber fingerprints and facial image), which are compared to the fingerprint and facial biometrics collected during the Activation process. Upon successful activation the card PIN is changed by the Applicant and the card is activated.

After the LRA approves Certificate Issuance, the Applicant appears in-person before the TA or LRA different than the Certificate approving LRA, who authenticates the Applicant based on previously collected biometric data.

1) The smart card is placed in the personalization station where the facial image is printed on it. Subsequently, the station connects to the CMS and all the Certificates and signed biometric data are transferred into the smart card securely.[13]
2) The TA or LRA different then the Certificate approving LRA instructs the Applicant to change the PIN in the smart card and through the personalization workstation authorizes the CMS to set to an Applicant-selected PIN and activate the smart card.

The Subscriber uses the newly issued Certificate Private Signing Key to formally acknowledge the receipt of the smart card with all Certificates and to Digitally Sign the Subscriber Agreement that contains a declaration of identity.

4.3.1.6 Activation Code Delivered via CMS and EWS Directly

An alternate acceptable process requires an Activation Code that is managed by the CMS and the EWS directly and is changed in the smart card by the Applicant when the Certificates are Issued. The process of Key and Certificate generation; the biometric data collection, signature and store in the smart card are performed in the presence of the Applicant.

4.3.1.7 Two-Activation-Code Process

After the Issuance of a Certificate has been approved by the LRA (via Client-authenticated SSL/TLS-encrypted Session[14]), two (2) Activation Codes are generated by the RA System, and are sent by two LRAs through

[13] For all Certificates except IGC Basic Software, a 30 day period is calculated based from the date identity was established. The 30 day period begins from the date the I&A is approved by the LRA and entered by the LRA into the RA System. If more than 30 days have passed since the date identity was established, the system prevents the Applicant from proceeding with Key Generation and notifies them that in-person identification must be repeated.

[14] Unless otherwise indicated, in this Section 4.3, all communications between LRAs and the CA system are via Client-Authenticated SSL/TLS-Encrypted Session using an IGC Medium Hardware Assurance or IGC PIV-I hardware Assurance

separate channels to the Applicant.

To enforce principles of Separation-of-Duties/Multi-party Control, two LRAs (LRA-1 and LRA-2) are involved in this process. As part of system configuration and the assignment of access rights, separate role-based privileges are designated for LRA-1 and LRA-2 so that each role can only receive one of the two Activation Codes[15], as described in the process below.

1) LRA-1 assembles the Cryptomodule Installation Kit and places the first Activation Code in a sealed envelope and ships it with the Installation Kit either to the TA or the Applicant.
2) LRA-2 sends the second Activation Code by mail or email to the Applicant using information contained in the Applicant's Profile.
3) Following the instructions provided with the Installation Kit (or downloaded from the registration system), the Applicant installs any necessary drivers and/or Cryptographic Service Providers onto the system where the Cryptomodule interface device is connected.
4) The Applicant then accesses a specified secure retrieval page (https://) hosted by the RA System and initiates a Server-Authenticated SSL/TLS-Encrypted Session. For authentication purposes, the Applicant enters both Activation Codes provided during the registration and approval process. The Applicant is presented with the Subscriber Agreement and must Accept it to continue.
5) The Applicant continues with Key Generation16, Certificate generation17, and Certificate loading process during which the Certificate Issuance system ensures that the appropriate Cryptomodule and Key lengths are being used. To ensure that Keys are properly Generated and stored in Cryptomodules that meet the requirements of Section 6.2.1, programs are run that enforce restrictions on the Cryptographic Service Providers that can be used by the Applicant. If the required Cryptographic Service Provider is not found, the Applicant receives an error message.
6) The Applicant generates a Key Pair within the boundaries of the Cryptomodule and uses the Private Key to sign the Public Key in an RSA PKCS #10 Certificate request. During this same SSL/TLS session, additional scripts are run by the Certificate Issuance system to ensure that Key lengths meet minimum requirements and that the PKCS#10 is valid. Upon verification of the Applicant's Digital Signature on the RSA PKCS #10 Certificate signing request (using the algorithm specified in the request), the requested Certificate is generated by the CA and delivered to the Applicant's Cryptomodule during this same SSL/TLS session.

Certificate Issued to the LRA and a valid SSL Server Certificate that chains to one of IdenTrust's Root Certificates (e.g., DST Root CA X3 or IGC Global Common Root).

[15] The Activation Code one is a 10-digit number and the Activation Code two is 9-digit number. Both Activations Codes are generated using a 48-bit seed, which is modified using a linear congruential formula. The numbers are compared against all previous numbers to ensure they have not previously generated. If the number has previously been used, the process is repeated until an ungenerated number is created.

[16] For all Certificates except IGC Basic Software, a 30 day period is calculated based from the date identity was established. The 30 day period begins from the date the I&A is approved by the LRA and entered by the LRA into the RA System. If more than 30 days have passed since the date identity was established, the system prevents the Applicant from proceeding with Key Generation and notifies them that in-person identification must be repeated.

[17] The Certificate's Subject Distinguished Name (DN) is assembled at this point. All information used in the DN is taken from the verified application data provided to the CA system by the LRA. The Common Name and Organization fields are populated with exactly the same information entered in the application. The Country field is optionally populated with the ISO 3166 standard 2-character code that represents the country in the application. The Organization Unit is populated with a unique ID generated as explained in section 3.1.5.

7) If there is no requirement for Encryption Key escrow, a second Private Key for an Encryption Certificate is generated using the same method explained in step (6). If there is a requirement for escrow of the Encryption Key, Encryption Keys are created and delivered as explained in Section 6.1.2.

4.3.1.8 Manual PKCS#10 Process

Some devices are not capable of submitting a PKCS#10 during an interactive web-based session described in the processes outlined above. In that case, the Applicant is instructed to create the Key Pair according to the manufacturer's or system developer's instructions and to create and submit a PKCS#10 Certificate signing request.

1) The Applicant generates the Key Pair and exports the PKCS#10 Certificate signing request in base-64 encoded format.
2) The Applicant is directed to a specified secure enrollment site (https://) and initiates a Server-Authenticated SSL/TLS-Encrypted Session. During this online enrollment session, the Applicant creates a profile with Subscriber name, email address, Organization name and other necessary information. The Applicant also creates an Account Password to be used later during Certificate retrieval. A hash of the Account Password is submitted to the CA. The Applicant pastes the base-64 encoded PKCS#10 into a web form and submits it to the CA. The PKCS#10 is verified to ensure proper Key lengths are used and that the information in the PKCS#10 matches the information provided by the Applicant in the profile (e.g., the FQDN or identifier of the Device). The Digital Signature on the PKCS#10 request is verified by the CA to establish proof of possession. The Applicant is then instructed that he or she will be notified when the Certificate has been approved.
3) When the Certificate is approved, an Activation Code is generated and sent to the Applicant through a digitally signed and encrypted email, in a PIN-mailer or in a sealed, tamper-evident envelope. Following instructions provided in the envelope (or downloaded from the registration system), the Applicant is directed to a specified secure retrieval site and a Server-Authenticated SSL/TLS-Encrypted Session is initiated.
4) In the event a digitally signed and encrypted email is used to transmit the Activation Code, the Applicant must already be (a) a Subscriber of an Individual Certificate at an assurance level equal to or higher than the assurance level of the Device Certificate being applied for and (b) affiliated with the same Subscribing Organization as the Device Certificate being applied for.
5) For authentication purposes, the Applicant enters the Account Password and Activation Code to access the retrieval page.[18] The Applicant is presented with the Subscriber Agreement and must Accept it to continue. The Certificate is generated and downloaded to the Applicant's Device where it is installed on the hardware according the manufacturer's or system developer's instructions.

The Applicant confirms completion of the activation process by testing the newly installed Certificate.

4.3.1.9 Certificate Issuance to CAs, CSAs and the Cross-Certifying Bridge CA

Certificate signing for CAs and Cross-Certifying Bridge CAs requires approval from IdenTrust senior management. The Certificate signing ceremony for CAs, CSAs, CMSs and Bridge CAs is performed in the secure room described in Section 5.1.2.1. The ceremony is scripted, videotaped and witnessed. Pursuant to Sections 3.2.2 and 3.2.5, the CA Administrator reviews the documentation provided by the entity applying

[18] For all Certificates except IGC Basic Software, a 30 day period is calculated based from the date identity was established. The 30 day period is calculated based on the in-person identification date value entered into the RA System by the LRA (based on the review of the ID Form as described in section 4.1.2.4 and 4.1.2.5). If more than 30 days have passed since the in-person appearance, the system prevents the Applicant from proceeding with Key Generation and notifies them that in-person identification must be repeated.

for the CA, CSA or CMS Certificate to validate the request (e.g., reviews authorizing signatures, authorizations, and accompanying Certificate request identifiers) and to ensure that the Certificate and Key Pair are bound to the party making the request.

Pursuant to Section 3.2.1, the CA system also verifies the Digital Signature on the PKCS#10 Certificate signing request to establish proof of possession. In order to prevent collisions among the Certificates that are Issued by the IdenTrust Global Common Root CA, the IdenTrust CA signing product ensures uniqueness of the Certificate serial number.

The Certificate signing ceremony is performed and the Certificate is signed using the CA Private Signing Key and the PIN Entry Device ("PED") and associated PED key(s) for authentication to the CA Cryptomodule via Separation-of-Duties/Multi-party Control (see Sections 6.2.2 and 6.2.8).

4.3.2 Notification to Subscriber of Certificate Issuance

Notification of Certificate issuance is provided according to the following procedures.

4.3.2.1 Notification to Subscribers

Notification of Certificate Issuance is provided to a Subscriber during the secure online Certificate Retrieval process. The Subscriber is led through a series of interactive screens that assist the user in retrieving, testing and confirming the Certificate. Activation material provided by IdenTrust, in conjunction with user provided confirmation information is required during the process as described in Section 4.3.1.

A follow-up email is also sent to the Subscriber as notification that the Certificate has been generated and delivered.

4.3.2.2 Notification to RAs, CAs and Cross-Certifying Bridge CAs

4.3.2.2 Notification to RAs, CAs and Cross-Certifying Bridge CAs IdenTrust notifies the designated representative of the RA, CA or the Cross-Certifying Bridge CAs when it has Issued the Certificate to the RA, CA or Cross-Certifying Bridge CA.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following sub-sections define conduct constituting Certificate Acceptance.

4.4.1.1 Certificate Acceptance by Subscribers

During the Certificate Retrieval process the Subscriber must acknowledge acceptance of the Certificate.

Subscriber Agreements also set forth additional, alternative conduct that constitutes Acceptance by the Subscriber, including but not limited to:

- Failing to notify the CA or RA of any problems or errors with the Certificate within a reasonable time of downloading or retrieving it; and
- By using a Certificate, a Subscriber Accepts the Certificate, warrants the accuracy of its contents and agrees to the obligations, representations and warranties of Section 9.6.3 and to the terms and conditions of the Subscriber Agreement.

4.4.1.2 Certificate Acceptance by Participant CAs and Cross-Certifying Bridge CA

Issuance and publication of a Sub CA Certificate or Cross-Certificate constitutes Acceptance unless the CA or the Bridge CA notifies IdenTrust that it does not Accept the Certificate and requests that it be Revoked.

4.4.2 Publication of the Certificate by the CA

Subordinate CA Certificates are published in the Repository upon Issuance.

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

IdenTrust notifies the Cross-Certifying Bridge PAAs and personnel of the Bridge CAs when it has Issued any CA Certificate that chains to the IGC Root CA.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers or Custodian (e.g. authorized third party) are notified of their obligation to protect their Private Keys from access by other parties. Subscribers are required by agreement to use Private Keys only in accordance with the usages listed in the key usage extension and extended key usage extension of the Certificate and for purposes allowed by Subscriber Agreement, the IGC-CP and Section 1.4 of this CPS. Furthermore, a Subscriber is required by agreement to not use the Private Signing Key after the Certificate has been Revoked or has expired.

Key usage by CAs, CSAs and RAs is discussed below in Section 6.1.7.

4.5.1.1 RA and LRA Private Key Usage

LRAs using the RA System web interface may use their Keys to Digitally Sign Certificate management transactions and to authenticate via Client-Authenticated SSL/TLS-Encrypted Session. When an RA hosts its own Certificate registration and approval system, LRAs will use their Keys to Digitally Sign Certificate management transactions and to authenticate via Client-Authenticated SSL/TLS-Encrypted Sessions. The RA System connects via Server-Authenticated SSL/TLS, its Keys are used to Digitally Sign Certificate management transactions submitted to the CA system, and the RA Administrator is responsible for ensuring proper Private Key usage.

4.5.2 Relying Party Public Key and Certificate Usage

Certificates that are Issued pursuant to this CPS conform to IGC Profiles. Public Keys, information contained in Certificates, and related information stored in the Repository may be used only in accordance with the usages listed in the key usage extension and extended key usage extension of the Certificate. Such information may not be used other than as allowed by the IGC-CP or as allowed herein. The use of such information for any unauthorized purpose, such as for sending unsolicited commercial mass messages (junk email, spam, and the like) is expressly forbidden.

Relying Parties may use or otherwise rely on Certificates that are Issued pursuant to this CPS on the following terms and conditions. Relying Parties shall:

- Be held responsible to understand the proper use of Public Key Cryptography and Certificates;
- Verify Certificates that are Issued hereunder, through the use of Certificate Chains, OCSP and CRLs in accordance with X.509, v.3;
- Trust and make use of a Certificate only if such Certificate has not expired or been Revoked and only if the Certification Path can be verified to the IGC Root Certificate and/or the US Federal Common Root Certificate using RFC 5280 Certification Path validation rules;
- Comply with all laws and regulations that might be applicable to the Relying Party's export, import, or use of the Certificate and related information;

- Make their own judgment and rely on the Certificate only if the same constitutes Reasonable Reliance in the circumstances, including determining whether a particular type of Certificate is appropriate for the purpose or transaction contemplated and also taking into consideration the following additional factors:
    - Any legal requirements for the identification of a party, the protection of the confidentiality or privacy of information, or the legal enforceability of Digital Signatures in accordance with any laws that may apply;
    - All facts listed in the Certificate, or of which the Relying Party has or should have notice, including this CPS and the IGC-CP;
    - The economic value of the transaction or communication, if applicable;
    - The potential losses or damage which might be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction or communication;
    - The applicability of the laws of a particular jurisdiction, including the jurisdiction specified by the IGC-CP or this CPS;
    - The Relying Party's previous course of dealing with the Subscriber, if any;
    - Usage of trade, including experience with computer-based methods of trade; and
    - Any other indicia of reliability or unreliability, or other facts of which the Relying Party knows or has notice, pertaining to the Subscriber and/or the application, communication or transaction.

Additional Relying Party obligations are found in Sections 1.3.8, 4.9.6 and 9.6.4 and elsewhere in this CPS.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

Certificate Renewal is not supported for Subscribers. Subscriber subscription renewal results in a Certificate Re-Key (see Section 4.7).

CSA OCSP Responder Certificates are Renewed on a monthly basis as long as use of the corresponding Key Pair has not extended its usage period (see Section 6.3.2).

Cross-Certificates are renewed more frequently than the corresponding CA in consistency with the Certificate lifespan outlined in IGC Certificate Profiles as long as the Key Pair usage period has not been exhausted in accordance with Section 6.3.2 parameters.

4.6.2 Who May Request Renewal

Renewal requests are initiated differently based on the type of certificate renewal as defined in the following sub-sections.

4.6.2.1 Who May Request Device Renewals

The designated Machine Operator may request renewal of a Device Certificate.

4.6.2.2 Who May Request OCSP Renewals

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

4.6.2.3 Who May Request a Cross-Certificate Renewals

For the Cross-Certifying Bridge CA, those persons identified pursuant to Section 3.2.2.

4.6.3 Processing Certificate Renewal Requests

Renewal requests are processed by type according to the details provided in the following sub-sections:

4.6.3.1 Processing Device Renewal Requests

In advance of the certificate expiration an automated emailed notification is sent to the individual who is designated in the Certificate as the Machine Operator. The Machine Operator may request renewal via the IdenTrust online Certificate management system. All renewals are processed according to the Initial Registration process as described in Section 3.2.

4.6.3.2 Processing OCSP Renewal Requests

Prior to expiration of each OCSP Responder Certificate, the CSA Signing Key is re-signed during a Certificate renewal ceremony performed in the secure room under 2-person control where the ceremony is scripted, witnessed and video-taped. The prior OCSP Responder Certificate is not used as basis for the renewal and is left to expire.

4.6.3.3 Processing CA Renewal Requests

For Cross-Certification, the CA and the Cross-Certifying Bridge CA should be renewed and ready for Cross-Certification three months prior to the scheduled expiration of the Cross-Certificate. The prior cross-Certificate is not used as basis for the renewal and is allowed to expire unless the Bridge CA requires Revocation which, if required, is executed in a subsequent ceremony.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification of new Certificate Issuance for Renewals are made according to the type of Certificate as described in the following sub-sections:

4.6.4.1 Notification for Device Certificates

Notifications for Renewed Device Certificates are processed according to the Initial Registration Certificate notification process as described in Section 4.3.2.1.

4.6.4.2 Notification for OCSP Certificates

The CA Administrator is present and needs no notice of OCSP Responder Certificate Issuance.

4.6.4.3 Notifications for CA Certificates

For the Cross-Certifying Bridge CA, see Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Acceptance of Renewal Certificates are processed by type according to the details provided in the following sub-sections:

4.6.5.1 Acceptance of a Renewal Device Certificate

Acceptance of Renewal Device Certificates are processed according to the Initial Registration Certificate Acceptance process as described in Section 4.4.1.1.

4.6.5.2 Acceptance of a Renewal OCSP 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.

4.6.5.3 Acceptance of a Renewal CA Certificate

For the Cross-Certifying Bridge CA, see Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

Renewal OCSP Responder Certificates are published in the 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.

For the Cross-Certifying Bridge CA, see Section 4.4.3.

4.7 Certificate Re-Key

Re-keying a Certificate consists of creating new Certificates with a different Public Key (and serial number) while retaining the remaining contents of the old Certificate that describes the subject. The new Certificate may be assigned a different Validity Period, Key identifiers, specify a different CRL distribution point, and/or be signed with a different Key. Re-Key of a Certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness. Certificate Replacements are allowed under certain circumstances. See sub-section heading Certificate Replacements below for specific details.

After Certificate Re-Key, the old Certificate may or may not be Revoked, but must not be further re-keyed, renewed, or modified.

Certificate Replacements

Dependent on Certificate type, IdenTrust provides for the replacement of Certificates when the Subscriber's Private Key has not been compromised and there are no changes to the Certificate. In the case where a non-escrowed Private Key is lost or damaged, including in the event the Subscriber has lost control of a software or hardware Cryptomodule on which the Certificate is stored, the Certificate cannot be replaced, and the identity of the Subscriber must be established through the initial registration process described in Section 3.2.

The most common reason for Certificate replacement is a forgotten Certificate PIN or password. Upon receiving an authenticated request to replace an IGC Basic Certificate from a Subscriber, the RA records the following Certificate replacement transaction data:

- Certificate serial number;
- Certificate common name;
- Certificate policy OID;
- Date/time of completion of replacement process;
- Name of Subscriber; and
- All associated replacement data.

In the event of replacement, the LRA Revokes the previously issued Certificate.

Certificates asserting an Assurance Level of Basic do not require retrieval within the thirty day period of the date identity is established. For such Certificates, the Certificate may be replaced based on original establishment of identity provided the Certificate Validity Period does not exceed nine years from the date identity was established.

IGC Medium Software Certificates may be replaced according to the processes above provided the Certificate is retrieved within 30 days from the date identity was established. If more than 30 days have passed since the in-person appearance, the system prevents the Applicant from proceeding with Key Generation and

notifies them that in-person identification must be repeated.

For all other IGC Certificates, replacement is not permitted under any circumstance.

4.7.1 Circumstances for Certificate Re-Key

Subscribers and other PKI Participants should plan on Re-Keying well in advance of the time when a Key Pair or Certificate is scheduled to expire. Creating a new Key Pair and obtaining a new Certificate prevents a disruption in signing activities that would be caused if the Certificate were allowed to expire before attempting to Re-Key.

4.7.1.1 Re-Key by Subscribers and LRAs

End-entity Certificates are Issued with one, two or three year validity. At least three months prior to validity expiration, the CA, RA System or CMS may automatically notify the Subscriber that he or she must Re-Key and re-establish identity through the process described in Section 3.3.1.

For PIV-I end entity Certificates, Re-Key is allowed provided the validity of the new Certificate does not exceed the lifetime of the PIV smart card on which the Certificate is stored. In the event Re-Key would extend beyond card validity, Issuance of a new PIV smart card is required.

For Device Certificates, the Machine Sponsor is required to follow the same steps to re-establish identity for Certificate Re-Key as would a normal Subscriber, described in Section 3.3.1. Primary Machine Operators may also opt to add, remove or edit subject names during Re-Key. If the contents of a Device (e.g., the Organization information), the LRA will request verification information in accordance with the verification processes set forth in Section 3.2.3.4 of this CPS before the Re-Key process can be completed.

4.7.1.2 Re-Key for RAs

For RA Systems, IdenTrust will contact the RA Administrator to schedule Re-Keying at least three months prior to the scheduled expiration. The prior Certificate is not used as basis for the Re-Key and is allowed to expire.

4.7.1.3 Re-Key for CSAs and Cross-Certifying Bridge CAs

CSA Re-Keying consists of a Key Generation Ceremony performed in accordance with Section 6.1.1. For Cross-Certification, the CA and the Cross-Certifying Bridge CA should be Re-Keyed and ready for Cross-Certification three months prior to the scheduled expiration of the Cross-Certificate. Neither the prior Certificate in the CSA nor the Cross-Certificate is used as basis for the Re-Key and is allowed to expire. For the cross-Certificate, if the Bridge CA requires Revocation, such Revocation is executed in a subsequent ceremony.

4.7.2 Who May Request Certification of a New Public Key

Authorized requesters for Re-Key depends on the type of Certificate. See sub-sections for specific details.

4.7.2.1 Re-Key Requests for Subscribers and LRAs

For Subscribers and LRAs, see Section 3.2.3 (Identification and authentication) and Section 4.1.1 (Who can submit a Certificate application).

4.7.2.2 Re-Key Requests for RAs

For RAs, those persons identified pursuant to Section 3.2.2.

4.7.2.3 Re-Key Requests for CSAs ad Cross-Certifying Bridge CAs

For CSAs and the Cross-Certifying Bridge CA, those persons identified pursuant to Section 3.2.2.

4.7.3 Processing Certificate Re-Keying Requests

Certificate Re-Key requests are processed according to certificate type. See sub-sections below for specific details.

4.7.3.1 Processing Re-Key Request for Subscribers and LRAs

During re-keying, the Subscriber must present his or her currently valid IdenTrust-issued IGC Certificate to establish a Client-authenticated SSL/TLS-encrypted session via the IdenTrust Certificate management application. The Certificate management application validates the authenticity of the Certificate presented by verifying that a) it was issued by IdenTrust; b) by comparing the status of the Certificate in the relational database to confirm it is not revoked; and c) that the Certificate is still valid (not expired). The database utilized for this process is the same one used to issue the CRLs and provides a real-time check of the Certificate status to verify its validity (see definition of "Client-authenticated SSL/TLS" in Section 1.6.1 Definitions.)

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

If the Subscriber successfully uses his or her Certificate to enter the Certificate management application interface, the Subscriber will complete the re-key online through an automated process. The Subscriber is eligible for immediate retrieval of the rekeyed Certificate if the following criteria is met:

- The maximum Validity Period for Key Pair Usage as defined in Section 6.3.2 Certificate Operational Periods and Key Pair Usage Periods has not been exceeded;
- The Subscriber confirms that no information in the Certificate has changed;
- The Subscriber reviews and accepts the terms of the Subscriber Agreement; and
- The Subscriber provides payment for the new Certificate.

If the Subscriber changes any information during the process, the re-key application will be referred to an RA Operator for manual review. If it is determined that the Subscriber has changed their name, affiliation, or any data contained in the Certificate, the RA will notify the Subscriber that he or she is not eligible for re-key and will need to apply for a new certificate and must appear for in-person identity proofing.

If the modified information is not information that is included in the Certificate, (such as a telephone number), the RA Operator will approve the re-key request and send a notification via courier or U.S. mail first class including the retrieval instructions for the re-keyed Certificate.

If the Subscriber cannot present their Certificate or changes specific information, related to verification (personal information, organization affiliation, etc.) he or she is not eligible for re-key and must apply for a new certificate and appear for in-person identity proofing.

4.7.3.2 Processing Re-Key Request for RAs

Re-Key for RAs is performed in the same manner as Initial Certificate Issuance. See Section 4.2.2.

4.7.3.3 Processing Re-Key Requests for CSAs and Cross-Certifying Bridge CAs

Re-Key for CSAs and Cross-Certifying CAs is performed in the same manner as Initial Certificate Issuance. See Section 4.2.2

4.7.4 Notification of New Certificate Issuance to Subscriber

Notifications for Certificate Re-Key is performed in the same manner as initial Certificate Issuance. See

Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting Acceptance of a Certificate Re-Key is performed in the same manner as initial Certificate Issuance. See Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Publication of the Re-Keyed Certificate by the CA is performed in the same manner as initial Certificate Issuance. See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of Certificate Issuance for a Re-Keyed Certificate is performed in the same manner as initial Certificate Issuance. See Section 4.4.3.

4.8 Modification

Certificate modification, sometimes called Certificate update, is not supported for Subscribers and LRAs. See the Re-Keying process described above in Section 4.7.

4.8.1 Circumstance for Certificate Modification

CAs may request Certificate modification for any reason, provided they address interoperability concerns as described in Section 4.8.3 below. CA Certificate modification requires approval in writing by the IdenTrust PMA.

4.8.2 Who May Request Certificate Modification

A CA may only request a modification of its own CA Certificate(s).

Subscribers must request a modification via the secure IdenTrust online certificate management system. The subscriber must authenticate through the presentment of his or her active Certificate or by providing the account number and account password associated with the Certificate.

4.8.3 Processing Certificate Modification Requests

Modification requests are processed by type according to the details provided in the following sub-sections:

4.8.3.1 Processing Modification Requests for Subscriber Certificates

IdenTrust will process the modification application according to the procedures pertaining to new Certificate issuance and in accordance with Section 3.2.2.

4.8.3.2 Processing Modification Requests for Sub-CA Certificates

Modification of a CA Certificate requires that the CA making the request enter into a written agreement with the IdenTrust PMA, other Bridge PAA as appropriate, and any affected CAs to address interoperability concerns. Proposals to modify CA Certificates are processed as follows:

The CA seeking modification will survey any associated CAs to determine potential effect on relying applications and whether the proposed modification creates interoperability concerns. Any concerns raised by a CA should be addressed. If there are no remaining concerns, the Root CA may re-Issue a Sub CA Certificate with the requested modifications. The old CA Certificate will not be Revoked unless all Issues related to the transition from the old CA Certificate to the new CA Certificate have been resolved. The Public Key for the modified CA Certificate will remain the same. Otherwise, Key changeover processes of Section 5.6 will be implemented for Certificate modification.

The new CA Certificate is provided to, and must be Accepted by, the CA prior to distribution.

4.8.3.3 Processing Modification Requests for CA Cross- Certificates

Assuming all applicable Cross-Certification requirements are met, the Cross-Certifying CA(s) will re-sign the Subject CA's Public Key obtained from the previously Issued Cross-Certificate. The Subject CA's Public Key may be verified by comparing the two Public Keys. The Cross-Certifying CA will re-certify the Subject CA's Public Key with the Modified Certificate contents. The new Cross Certificate is provided to, and must be Accepted by, the Subject of the Cross Certificate prior to distribution. The Modified Cross-Certificate will be distributed to all PKI Participants, including vendor partners who create IGC Certificate enabled applications using one or all of the procedures listed in Section 6.1.4.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.8.3 above.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.8.3.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Notice of CA Certificate modification will be provided to all PKI Participants as outlined in Section 4.4.3.

4.9 Certificate Revocation and Suspension

All Certificate Revocations are authenticated according to the procedures described in this section.

4.9.1 Circumstances for Revocation

Certificate Revocations are processed according to Certificate type as described in the following sub-sections.

Revoked Certificates are included on all new publications of the CRL until the Certificates expire. All Revoked Certificates are published to at least one CRL.

4.9.1.1 Circumstances for Revocation for Individual and Device Certificates

Subscriber Certificates are Revoked under the following circumstances:

- Subscriber or other authorized agent requests Revocation;
- Identifying information or affiliation components of any names in the Certificate become invalid;
- An Organization terminates its relationship with the CA such that it no longer provides affiliation information;
- Subject can be shown to have violated the stipulations of its respective Subscriber Agreement or the stipulations of this CPS or the IGC-CP;
- Private Key has been compromised or is suspected of being compromised;
- The Issuing CA obtains evidence that the Certificate was misused;
- The Issuing CA is made aware of a material change in the information contained in the Certificate;
- The IdenTrust Risk Management Committee is made aware of a possible compromise of the Private Key of the Issuing Sub CA Certificate and reaches a determination Revocation is in the best interest of the PKI (see Section 5.7.3);
- The PMA or Issuing CA suspects or determines that Revocation of a Certificate is in the best interest of the integrity of the PKI;

- The Issuing CA is made aware a Subscriber no longer has an affiliation with the Subscribing Organization or is no longer authorized to hold the Certificate;
- The Issuing CA is made aware that information included in the subjectDN of a Device Certificate no longer accurately represents the Subscribing Organization, or Device;
- The Applicant rejects a newly Issued Certificate (see Section 4.4);
- The Issuing CA determines Issuance of the Certificate did not follow necessary procedures specified by this CPS or information in the Certificate is inaccurate, false, deceptive or misleading;
- The Subscriber fails to meet contractual obligations;
- The Issuing CA or Issuing CA of the Sub CA Certificate ceases operations for any reason and has not made arrangements for another CA to provide Revocation support for the Certificate;
- The Issuing CA's right to Issue under this CPS is Revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- The technical content or format of the Certificate is deemed by the IdenTrust Risk Management Committee to present an unacceptable risk to PKI Participants;
- Termination of the service agreement held between the Subscriber and the Custodian that holds the Private Key ends; or
- The Subscriber, Custodian (e.g. authorized third party) or RA requests Certification revocation.

4.9.1.2 Circumstances for Revocation for CA

CA Certificates are Revoked under the following circumstances:

- The IdenTrust Risk Management Committee determines the CA fails or has failed to meet contractual obligations;
- The Sub CA requests Revocation in writing;
- The Sub CA notifies IdenTrust that the original Certificate request was not authorized and does not retroactively grant authorization;
- IdenTrust Risk Management Committee is made aware of compromise or suspected compromise of Sub CA Private Keys and reaches a determination Revocation is in the best interest of the PKI (see Section 5.7.3);
- For IGC SSL Certificates, the IdenTrust Risk Management Committee determines the Sub CA has not complied with CA/B Forum Requirements or this CPS;
- The IdenTrust Risk Management Committee obtains evidence that the Sub CA Certificate was misused;
- The IdenTrust Risk Management Committee determines that any of the information appearing in the Sub CA Certificate is inaccurate or misleading;
- The Issuing CA or Sub CA ceases operations for any reason and has not made arrangements for another CA to provide Revocation support for the Certificate;
- The IdenTrust Risk Management Committee determines technical content or format of the Certificate presents an unacceptable risk to PKI Participants; or
- CA termination pursuant to Section 5.8.

4.9.1.3 Circumstances for Revocation for All Certificates

The IdenTrust Risk Management Committee may require Revocation of any IGC Certificate if it is determined Revocation is in the best interest of the PKI.

4.9.1.4 Certificate Problem Reporting

IdenTrust provides Subscribers, Relying Parties, Subscribing Organizations, application software suppliers and other third parties with clear instructions and contact information for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any

other matter related to utilization of and reliance upon Certificates. These instructions are available online at the IdenTrust website in the support section at www.IdenTrust.com. This page lists a telephone number to contact help desk representatives during business hours and an email contact to ensure reporting will be received 24/7.

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

- Account number;
- Name and Contact Information of the Individual/Organization Reporting the Certificate;
- Subscriber, Organization, Domain and/or PKI Sponsor name;
- Nature of the Issue (illegal activity, Private Key Compromise, etc.); and
- When the issue was discovered.

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

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

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

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

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

CAs and External RAs are required to provide Subscribers, Relying Parties, Subscribing Organizations, application software suppliers and other third parties with clear instructions and contact information for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to utilization of and reliance upon IGC Certificates.

CAs and External RAs are required to contact IdenTrust in the event of any Certificate problems or suspected compromise as outlined in this Section 4.9.

4.9.2 Who Can Request Revocation

Various individuals are authorized to request Revocation of a Certificate, depending on the type of Certificate to be Revoked, as follows:

- A Subscriber may request Revocation of his or her own Certificate at any time for any reason.

- A Sponsor or an Authorizing Official of a Subscribing Organization may request Revocation of a Subscriber Certificate with affiliation to that same Subscribing Organization. As an example, a Sponsor may request Revocation of a Certificate held by a Subscriber no longer employed by the Subscribing Organization and no longer affiliated to the Subscribing Organization.
- A Primary Machine Operator or Secondary Machine Operator of a Device may request the Revocation of its Certificate.
- An RA Administrator or an Authorizing Official may request Revocation of a Certificate used by an RA System.
- An Authorizing Official of a CA may request Revocation of their CA Certificate. A CA may Revoke a Certificate that it Issued to an Individual or Device. A CA may also identify other entities authorized to submit Certificate Revocation requests.
- An operator of a CMS may request Revocation of a CMS Certificate or Content Signing Certificate.
- A RA or TA may request the Revocation of a Subscriber's Certificate on behalf of the Subscriber and the Subscribing Organization. The Subscribing Organization, through its Authorizing Officials, may appoint other Individuals (e.g., HR personnel, Security Officers, Officers of the Organization, Purchasing agents, etc.) to request Revocation in their Subscribing Organization Agreement with the relevant CA.
- A CA may summarily Revoke Certificates that it has Issued.
- An RA's Authorizing Official may request Revocation of any Certificates held by an LRA, RA Administrator and TA to whom the RA sponsored the Issuance of a Certificate.
- The IdenTrust Risk Management Committee may request Revocation of a CA Certificate, CMS Certificate, PIV-I Content Signing Certificate or RA System Certificate when the CA or RA fails to comply with obligations in its agreement with IdenTrust or with requirements in the IGC-CP, this CPS or the entity's RPS.
- The IdenTrust Risk Management Committee or the PMA may require Revocation of any IGC Certificate if it is determined Revocation is in the best interest of the PKI.

4.9.3 Procedure for Revocation Request

Revocation requests are processed according to the type of Certificate for which Revocation has been requested and by whom the Revocation request has been made. These procedures, by Certificate type and requester are described in the following sub-sections.

4.9.3.1 Procedure for Revocation Request of Subscriber Certificate by Subscriber, Subscribing Sponsor Organization or Machine Operator

A Subscriber's Certificate may be Revoked either by sending a Digitally Signed Revocation request to the RA, by establishing a Client-Authenticated SSL/TLS Encrypted Session (using the Signing Key Pair associated with the Certificate being Revoked) with the RA System described in Section 1.3.3, or by contacting the RA's LRA or TA on the phone to place the request stating the reason for Revocation. The Subscriber, Sponsor, or the Primary Machine Operator or Secondary Machine Operator is required to indicate the Subject of the Certificate to be Revoked, the reason for the Revocation request, and the LRA or TA, when the request is submitted via email or phone, will document the reason for the request and archive this documentation. Reason codes are included in the CRLs Issued by IdenTrust, including the reason code of Revocation because of Key compromise.

Additionally, Device Certificates may be Revoked by the Primary Machine Operator or a Secondary Machine Operator who authenticates and requests Revocation using a Server-Authenticated SSL/TLS Encrypted Session and the account number and Account Password used by the Primary Machine Operator or Secondary Machine Operator during initial registration.

If the Primary Machine Operator or a Secondary Machine Operator no longer has the account number or cannot remember the Account Password, then identifying information of the Primary Machine Operator or a Secondary Machine Operator obtained during registration may be used to authenticate the Primary Machine Operator or a Secondary Machine Operator's request (e.g. the Primary Machine Operator or a Secondary Machine Operator can be called at the phone number previously established for the Primary Machine Operator as discussed in Section 3.2.3.4.)

The authority of the requesting Primary Machine Operator can be made by accessing the Subscribing Organization Authorization Agreement which is archived as a document included in the Device Certificate account record that is associated with the Revocation request, and confirming that the requesting individual is designated as the Primary Machine Operator.

In the case of a phone request for Certificate Revocation made by a Secondary Machine Operator, confirmation of the request is made by confirming that the requesting individual is included on the current Secondary Machine Operators list, which can be accessed through the Device Certificate account record that is associated with the Device Certificate to be revoked.

If the requester is not designated as the Primary Machine Operator or identified as a Secondary Machine Operator by inclusion in the archived documents mentioned above, then the request for Suspension will be denied.

In addition, a Digitally Signed request from the Primary Machine Operator that enables the LRA to verify association of the Primary Machine Operator with the Device Certificate using the electronic records in the RA System is considered valid.

If the Revocation request cannot be authenticated by the Private Key or the Account Password for the Device Certificate to be Revoked, then the Subscriber, Subscribing Organization Sponsor or Primary Machine Operator may be authenticated by in-person appearance before the LRA or TA, or alternatively, on the phone by providing three (3) pieces of information previously collected as part of the identity proofing process (e.g., ID number, ID Issuance place, DOB, etc.). The Subscriber, Subscribing Organization Sponsor or Primary Machine Operator should first attempt to contact the LRA or TA who was involved during the Issuance of the Certificate or the TA of their Subscribing Organization.

When a TA intermediates a Revocation request, the LRA will authenticate TA Digitally Signed Revocation request emails by verifying (i) the TA has a valid Certificate of commensurate Assurance Level of the Certificate to be Revoked; and (ii) the authority to request actions on behalf to the Subscribing Organization. The authority to request is validated based on lists put together by LRA based on the paperwork that nominates the TA. The list will contain identifiers that uniquely identify the TA (i.e., Name, Certificate's thumbprint / fingerprint / serial number).

The Subscriber or Primary Machine Operator is required to present an acceptable form of photo identification (see Section 3.2.3.1), which the LRA or TA reviews to identify and authenticate the Subscriber or Primary Machine Operator making the Revocation request. TAs must notify the LRA immediately upon validating the Revocation request and request that the LRA Revoke the Certificate.

A Subscriber ceasing its relationship with the Subscribing Organization must, prior to departure, Revoke the Certificate and should surrender to the LRA or TA any Hardware Cryptomodule that was Issued to the Subscriber. The Subscribing Organization Sponsor should be involved in proactively informing the TA or LRA about the departure in order for the LRA and TA to collect the Cryptomodule. If not already Revoked by the Subscriber, the LRA or TA Revokes the Subscriber's Certificate. LRAs and TAs are provided with instruction about their obligation to store the Cryptomodule securely to protect it from malicious use between surrender and Zeroization (see Section 6.2.10).

If the Cryptomodule cannot be obtained from the Subscriber, then the Subscriber's Certificate(s) will be immediately Revoked, expressing the reason code as "Key compromise." Promptly following Revocation, IdenTrust updates the Certificate status in the Repository and updates the CRL. Alternatively, a Subscribing Organization may opt for not collecting any Cryptomodules due to logistical difficulties (e.g., Subscriber is terminated under unfriendly conditions, Subscriber in a remote location, etc.) and instead always request Revocation of the Certificates as if the Cryptomodule was not obtained from the Subscriber. In these cases, the Revocation request will always result in a "Key compromise" code.

The CA will make a centralized location available to the Subscriber and Subscribing Organization for Cryptomodule destruction. Cryptomodules received in this location will be Zeroized or otherwise physically destroyed. A record in the form of an inventory of all Zeroized/destroyed Cryptomodules will be kept that shows at a minimum the sender, model and, if possible, serial number of the Zeroized/destroyed Cryptomodules.

4.9.3.2 Procedure for Revocation Request of Subscriber Certificate by Other PKI Participants

When a request for Revocation does not originate from the Subscriber, it must be made by an authorized person who meets the requirements of Section 4.9.2, and it must be accompanied by adequate proof of identity and authority. LRAs and TAs are provided with instructional material on methods to authenticate Revocation requests made by third parties.

The LRA or TAs validate the credentials of the requesting party and determine if the Revocation request meets the requirements of Section 4.9.1. It is the responsibility of the LRA or TA to investigate the alleged reason for Revocation and to determine whether Revocation is appropriate. If Revocation is appropriate, the LRA or TA documents information concerning the identification of the requestor and the reason for the request. TAs will forward the Revocation request via Digitally Signed email and mail the documentation supporting the request to the LRA for archival.

Requests for Revocation of all other Certificates is done either with a Digitally Signed request using the Private Key corresponding to the Certificate being Revoked, or by the authenticated request of an authorized representative of the RA, CA or CBCA, who are identified and authenticated in accordance with Sections 3.2.2 and 3.2.5.

4.9.3.3 Procedure for Revocation by LRA

Account restrictions exist in the CA and RA Systems that prevent an LRA from requesting or approving the Revocation of Certificates of Subscribers who are not within their own Organization, domain, Subscriber community, etc. The LRA's Certificate is compared against the ACL and, if authorized for that domain or namespace, the LRA submits the request for Revocation.

The LRA will Revoke the Certificate through a Client-Authenticated SSL/TLS-Encrypted Session with the CA System. Alternatively, the LRA can Revoke the Certificate through an RA System that submits the Revocation to the CA via a Server-Authenticated SSL/TLS-Encrypted Session using a Digitally Signed data structure (ASN.1 or XKMS/XSMS). The CA will change the Certificate status in the Repository from valid to Revoked. Revocation occurs when the serial number and other identifying information for the Certificate is published in a CRL. In any event, all Certificate Revocation requests should be promptly communicated to the CA.

It is not required to send Subscribers notice of Revocation. In the event Revocation notice is desired, it is the LRA's responsibility to send the Subscriber an email notice with brief explanation of the reasons for Revocation and to archive such notice. CA and RA Systems may be configured to automatically send Revocation notification emails to Subscribers.

4.9.3.4 Procedure for Revocation by Non-Authorized Requestors

Any Certificate Revocation requests from other, non-authorized requesters must be submitted to IdenTrust, not the CA. If IdenTrust determines that Revocation is appropriate, it will submit a Revocation request to the CA as specified below.

4.9.3.5 Procedure for Revocation by IdenTrust

Authorized representatives of IdenTrust may communicate Revocation requests and Revocation determinations to CAs or RAs by Digitally Signed email. The LRA will validate the request by verifying the signature on the Digitally Signed message and confirming that the representative has appropriate authority. The LRA will effect the Revocation and will send the Subscriber an email notice and brief explanation of the reasons for Revocation and will archive the notice with the identifying information for the IdenTrust representative and the reason for making the Revocation request.

4.9.3.6 Procedure for Revocation of CA or CSA Certificates

IdenTrust will Revoke the CA and CSA Certificates it has Issued to a CA in breach of its contractual obligations or if the Private Key corresponding to the Public Key in the Certificate has been or is suspected to have been compromised. In any event, prior to taking such action, the IdenTrust CIO will convene a meeting of management representatives (including representatives of the CA, RA and IdenTrust PMA) to assess the situation and make an appropriate decision concerning a course of action (see Section 5.7.3).

4.9.3.7 Procedure for Revocation of CMS, RA and IGC PIV-I Content Signing Certificates

IdenTrust will Revoke the CMS, RA and PIV-I Content Signing Certificate it has Issued to a CA or RA in breach of its contractual obligations or if the Private Key corresponding to the Public Key in the Certificate has been or is suspected to have been compromised. In any event, prior to taking such action, the IdenTrust CIO will convene a meeting of management representatives (including representatives of the CA, RA, and IdenTrust PMA) to assess the situation and make an appropriate decision concerning a course of action (see Section 5.7.3).

4.9.3.8 Procedure for Revocation of Cross-Certified Bridge CA Certificates

IdenTrust will Revoke the Cross-Certificates it has Issued if the subject of the Certificate is in breach of its contractual obligations or if the Private Key corresponding to the Public Key in the Certificate has been or is suspected to have been compromised. In any event, prior to taking such action, the IdenTrust CIO will convene a meeting of management representatives (including representatives of CAs, the IdenTrust PMA, and the Cross-certified Bridge PAAs to assess the situation and make an appropriate decision concerning a course of action (see Section 5.7.3).

4.9.3.9 General Guidance for All Situations not Specifically Addressed

Persons authenticating Revocation requests must balance the risk of an unauthorized request and the potential harm caused by Revoking the Certificate against the harm caused by not Revoking the Certificate.

TAs and LRAs are trained to expedite authentication and authorization checks on Revocation requests and to submit them to the CA as soon as possible.

4.9.4 Revocation Request Grace Period

There is no Revocation grace period. All PKI Participants are required to communicate a Certificate Revocation request as soon as it comes to their attention.

4.9.5 Time Within Which CA Must Process the Revocation Request

Certificates are Revoked and the CRL is published within one (1) hour of positively authenticating the request.

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

The frequency of CRL issuance depends on the type of CRL as defined in the following sub-sections.

4.9.7.1 CRL Issuance Frequency for CAs

The CRL Format for Certificates that are Issued by Subordinate CAs is found in IGC Certificate Profiles. It states that the value for the nextUpdate field in CRLs for CAs is 24 hours. However, as a certification practice, IdenTrust Issues and publishes CRLs on a 12-hour basis, even if there are no changes or updates to be made (Periodic CRLs). CRLs may be Issued more frequently (Interim CRLs) if a Revocation occurs. The superseded CRL is then removed from the directory system and replaced with a new CRL.

4.9.7.2 CRL Issuance Frequency for Root CAs

IdenTrust Issues and publishes the CRL for Certificates that are Issued by the IdenTrust Root CA at least every 31 days. In the case of CA compromise or Key compromise, IdenTrust Issues an emergency CRL within 18 hours of notification. The superseded CRL is then removed from the directory system and replaced with a new CRL.

4.9.7.3 CRL Issuance Frequency for All CAs

IdenTrust publishes a new CRL prior to the time specified in the Next Update field of the active CRL. Upon publishing of a new CRL, the Root CA and Participant CA any and all old CRLs published in the Repository are removed.

4.9.8 Maximum Latency of CRLs

IdenTrust publishes an Interim CRL within one hour of receiving a properly authenticated Revocation request.

4.9.9 Online Revocation / Status Checking Availability

The IdenTrust Certificate Status Authority ("CSA") supports OCSP and provides online Certificate status information in Digitally Signed OCSP Responses for Certificates that are Issued by CAs that are indicated in OCSP Requests submitted by Relying Parties. The CSA service is optional for Certificates that do not assert an Assurance Level of PIV-I hardware. The CAs that opt to implement it will be Issued Certificates that include a pointer to the OCSP Responder in the Certificate authority information access extension. For Certificates asserting an Assurance Level of PIV-I Hardware, the CSA service is provided via CA-delegated trust model OCSP as specified in RFC 6960.

Each OSCP Responder is Issued a Certificate signed by the same CA Private Key that signed the Certificates that will be validated by the OCSP Responder. Many applications will not validate properly unless the same

IdenTrust OCSP Responders are based on CRLs that are consistent with the specifications outlined in Section 4.9.7 in regards to latency.

4.9.10 Online Revocation Checking Requirements

See Sections 4.9.6, 4.9.9, and 7.3.

4.9.11 Other Forms of Revocation Advertisements Available

A CA may also use additional methods to publicize the Certificates it has Revoked. IdenTrust does not support any other method for obtaining Certificate status information than those described in Sections 4.9.7 and 4.9.9.

4.9.12 Special Requirements Related to Key Compromise

IdenTrust will notify potential Relying Parties if it discovers or suspects that a CA's Private Key has been compromised by publishing updated Certificate status in a CRL as described in Sections 4.9.3 and 4.9.7.

4.9.13 Circumstances for Suspension

A Certificate may be placed on Suspension upon a Revocation request of the Subscriber or a Subscriber's Subscribing Organization. A Certificate may be placed on Suspension in the event of an unsigned Revocation request or Revocation request pending authorization. Certificates can be placed on Suspension upon any other reason deemed acceptable by the CA or when the Subscriber requests this service due to lack of access to the Cryptomodule holding the Certificate.

4.9.14 Who Can Request Suspension

Certificate Suspension can be requested by various individuals depending on the type and ownership of the Certificate, as follows:

- A Subscriber may request Suspension of his or her own Certificate at any time for any reason.
- The Primary Machine Operator or a Secondary Machine Operator of a Device may request the Suspension of its Certificate.
- LRAs of a CA may request the Suspension of a Certificate that it authorized to be Issued to an Individual or Device.
- An Authorizing Official or Subscribing Organization Sponsor of a Subscribing Organization may request the Suspension of a Certificate that it authorized to be Issued to an Individual or Device.
- A LRA or TA may request the Suspension of a Subscriber's Certificate on behalf of the Subscriber and the Subscribing Organization.
- The IdenTrust Risk Management Committee may request suspension of any Certificate.

4.9.15 Procedure for Suspension Request

Procedures for processing Certificate Suspension varies based on the type of certificate and the party requesting suspension, as detailed in the following sub-sections.

4.9.15.1 Procedure for Suspension Request of Subscriber Certificate by Subscriber

A Subscriber's Certificate may be Suspended by sending a Digitally Signed Suspension request to the RA's LRA or TA or by establishing a Client-Authenticated SSL/TLS Encrypted Session with the RA System to place the request (using the Signing Key Pair associated with the Certificate being suspended) stating the reason for Suspension. The Subscriber or the Primary Machine Operator or a Secondary Machine Operator is required

to indicate the reason for the Suspension request, and the LRA or TA will document the reason for the request, when the request is submitted via email.

If the Suspension request cannot be authenticated through a Digital Signature of the Certificate to be Suspended, then the Subscriber or Machine Operator may be authenticated by in-person appearance before the LRA or TA in accordance with guidelines in Section 3.2.3.1.

4.9.15.2 Procedure for Suspension Request of Subscriber Certificate by Subscriber Sponsoring Organization

An authorized individual from the Subscriber Sponsoring Organization may request the suspension of a Subscriber Certificate. This may be necessary if a Sponsoring Organization believes that a Subscriber's Private Key may be compromised or the Sponsoring Organization suspects that the Subscriber is not in compliance with the Subscriber Agreement. A Certificate may be suspended while an investigation can be performed. The authorized individual from the Subscriber Sponsoring Organization may request Suspension from an LRA or directly from IdenTrust. Once determination has been achieved, the Suspension should be removed or a Revocation of the Certificate should be initiated.

4.9.15.3 Procedure for Suspension Request of Subscriber Certificate by Machine Operator

If the Primary Machine Operator or the Secondary Machine Operator requests Suspension via a phone call, confirmation of the authority of a Primary Machine Operator or Secondary Machine Operator must be made.

The authority of the requesting Primary Machine Operator can be made by viewing the Subscribing Organization Authorization form which is archived as a document included in the Device Certificate account record that is associated with the Suspension request, and confirming that the requesting individual is designated as the Primary Machine Operator.

In the case of a phone request for Certificate Suspension made by a Secondary Machine Operator, confirmation of the request is made by confirming that the requesting individual is included on the current Secondary Machine Operators List, which can be accessed through the Device Certificate account record that is associated with the Device Certificate to be Suspended.

If the requester is not designated as the Primary Machine Operator or identified as a Secondary Machine Operator by inclusion in the archived documents described above, then the request for Suspension will be denied.

If the Suspension request cannot be authenticated through a Digital Signature of the Certificate to be Suspended, or by confirming the identity of a Primary Machine Operator or a Secondary Machine Operator by reviewing the current version of the Secondary Machine Operators List, which is archived as part of the Device Certificate account record that is associated with the Suspension request, then the Subscriber or Machine Operator may be authenticated by in-person appearance before the LRA or TA in accordance with guidelines in Section 3.2.3.1.

4.9.15.4 Procedure for Suspension Request of Subscriber Certificate by Other PKI Participants

When a request for Suspension does not originate from the Subscriber, it must be made in person by an authorized person who meets the requirements of Section 4.9.14, and it must be accompanied by adequate proof of identity and authority. LRAs and TAs are provided with instructional material on methods to authenticate Suspension requests made by third parties.

When a Suspension request has been validated, the LRA or TA will document information concerning the identification of the requestor and the reason for the request. TAs will forward the Suspension request via signed email and mail the documentation supporting the request to the LRA for archival.

4.9.15.5 Procedure for Suspension Request Executed by LRA

The LRA will suspend the Certificate through a Client-Authenticated SSL/TLS-Encrypted Session with the CA System. Alternatively, the LRA may Suspend the Certificate through an RA System that submits the Suspension to the CA via a Server-Authenticated SSL/TLS-Encrypted Session using a Digitally Signed data structure (ASN.1 or XKMS/XSMS). The CA will change the Certificate status in the Repository from valid to Suspended (i.e., reason code CertificateHold). Suspension occurs when the serial number and other identifying information for the Certificate is published in a CRL associated to a reason code of "Certificate Hold".

A Suspension status is resolved either by removing the Certificate from the CRL or by assigning the KeyCompromise Revocation reason code under the conditions described in Section 4.9.16 below.

4.9.16 Limits on Suspension Period

There is no stipulation with respect to limits on Suspension period; however, the LRA or TA who assists with a Certificate Suspension should take care to monitor the Suspension until the Certificate is either Revoked or the Suspension is removed.

In order for a Certificate to be removed from Suspension status, the Subscriber must submit a request for removal of the Suspension status. The request may consists of:

- A Digitally Signed communication or an online request via a Client-Authenticated SSL/TLS Encrypted Session using a Certificate delivered to a hardware Cryptomodule, other than the Suspended Certificate, Issued to the Subscriber of the Suspended Certificate; or,
- A phone call from an authorized primary or secondary Machine Operation, who can be authenticated in accordance with the guidelines in Section 4.9.15; or
- In-person request after the Subscriber has been authenticated in accordance with the guidelines in Section 3.2.3.1.

4.10 Certificate Status Services

IdenTrust supports both CRL and OCSP validation.

4.10.1 Operational Characteristics

Specifics on how to obtain status information via CRL or OCSP are located in Sections 7 of this CPS.

4.10.2 Service Availability

Certificate Status Services shall be available on a 24x7 basis, with a minimum of 99.9% availability overall per year and a scheduled downtime not to exceed 0.5% annually. IdenTrust accomplishes this by operating a fully redundant architecture at the primary location, as well as having tertiary devices at the disaster recovery location for critical services including the repository and all components needed to perform validation.

4.10.3 Optional Features

Operational features of CRL and OCSP services are located in Section 7 of this CPS.

4.11 End of Subscription

End of a subscription varies based on the type of certificate as detailed in the following sub-sections.

4.11.1 End of Subscription for Subscribers

A Subscriber may terminate its subscription to Certificate services by allowing the term of a Certificate or applicable agreement to expire without renewal.

Subscribers may also voluntarily Revoke their Certificate as explained in Section 4.9.3. If a Subscriber terminates subscription during a Certificate's Validity Period, the Certificate is Revoked.

Prior to the end of subscription, the CA or RA will send the Subscriber notice of pending Certificate expiration at least 30 day intervals beginning 90 days before the expiration date of the Subscriber's Certificate.

4.11.2 End of Subscription for Sub-CAs

Beginning at least three years and six months prior to the expiration date of the Certificate of an IdenTrust Sub CA, IdenTrust will meet to determine the strategy to be used for Key changeover (see Section 5.6). Beginning at least three years and six months prior to the expiration date of the Certificate of a Participant CA, IdenTrust and the Participant CA will meet to determine the strategy to be used for Key changeover (see Section 5.6) and to ascertain whether to continue operating under the Participant CA Agreement as then existing, or to enter into negotiations to revise the arrangement and, depending on the outcome of such negotiations, execute a new agreement or a replacement CA to address business continuity for the Participant's Subscribers. If an IdenTrust Participant CA notifies IdenTrust that it does not intend to continue providing CA services and that there will be no replacement CA to take over operation of the Sub CA, then the CA Certificate is Revoked.

4.11.3 End of Subscription for Cross-Certified PKI Bridge CAs

End of subscription period processes for Cross-Certification with other Bridge CAs are specified in the specific policies. Pursuant to those policies, at least 180 days prior to the expiration date of the Cross-Certification agreement, the parties shall ascertain whether there is interest in renewing the Cross-Certification arrangement as then existing, or to enter into negotiations to revise the Cross-Certification arrangement and, depending on the outcome of the negotiations, execute a new Cross-Certification arrangement.

4.12 Key Escrow

Key escrow and key recovery practices are defined within the IGC-CP and IGC-CPS documents. IdenTrust does not maintain a separate Key Recovery Policy or Key Recovery Practices Statement.

4.12.1 Key Escrow and Recovery Practices

CA, CSA, RA and CMS Private Keys are not escrowed. Subscriber Private Signing Keys are not escrowed.

4.12.1.1 Key Escrow for Subscribers

IdenTrust Issuing CAs escrow Subscriber Private Encryption Keys when such Keys are delivered to hardware Cryptomodules to provide key recovery services. Subscribers are notified of escrow in the Subscriber Agreement. Escrowed Private Keys are encrypted and protected with at least the level of security used to generate and deliver the Private Key. Controls are in place to prevent unauthorized access to escrowed Private Keys.

4.12.1.2 Key Escrow for CMS

IdenTrust may escrow Private Keys within a Key escrow database on the premise of a third party RA operating a CMS. In such cases escrowed Private Keys are encrypted and protected on the RA system first with a symmetric Key, then using an asymmetric Key Pair where the Private Key is held by IdenTrust. Multi-party controls required for Key recovery are an inherent function of a FIPS 201 compliant CMS. Recovery requests through the CMS to the IdenTrust CA require the Private Key held by IdenTrust to be active.

In cases where a Participant CA or External RA escrows Private Keys of Encryption Certificates on their premise through use of a CMS, escrowed Private Keys are encrypted and protected on the RA system first through the use of a symmetric encryption key, and then additionally through encryption of the symmetric

key with an asymmetric Key Pair where the Private Key is held by IdenTrust. Only the encrypted symmetric key is delivered to IdenTrust.

RAs are required to describe, in the organization's RPS document, how CMS workstations are protected to ensure that only authorized LRAs are able to access the CMS for certificate issuance requests and/or key recovery.

4.12.1.3 Circumstances for Key Recovery

Subscribers and Subscribing Organizations may request recovery of an escrowed Private Key. Key recovery requests can only be made for one of the following reasons:

- The Subscriber is requesting recovery of their own escrowed Private Key(s);
- The Subscriber is no longer part of the organization to which affiliation is asserted in the Subscriber's escrowed Certificate;
- The escrowed Private Key is part of a required investigation or audit;
- The requester has authorization from a competent legal authority to access the communication that is encrypted using the key;
- Key recovery is required by law or governmental regulation; or
- The Subscribing Organization asserted in the Subscriber's escrowed Certificate indicates that key recovery is mission critical or required for business continuity.

4.12.1.4 Controls for Key Recovery

Key Recovery in currently only available for Certificates requested via the CMS. A Subscriber may request Key recovery via a secure online certificate management system hosted by IdenTrust. Multi-party controls are required for Key recovery requested by a subscriber. See section 4.12.1.5

Multi-party controls required for Key recovery are an inherent part of FIPS 201 approved CMSs. Recovery requests through the CMS to the IdenTrust CA require the RA System Private Key issued to the CMS be active, ensuring involvement of the CA in all recovery operations.

4.12.1.5 Key Recovery for Subscribers

Upon receipt of a recovery request for an escrowed Key, IdenTrust:

- Verifies the request meets one of the required conditions above;
- Verifies the authority of the individual making the request, i.e. the Subscriber, Subscribing Organization Authorizing Official;
- Under multi-party control an IdenTrust LRA recovers the Certificate with Private Key to a FIPS 140-2 Level hardware Cryptomodule in a PKCS#12 format;
- Securely delivers the Cryptomodule to the requestor; and
- Separate from the Cryptomodule, communicates the password for the Cryptomodule to the requestor.

4.12.1.6 Key Recovery via CMS

There are two (2) models for Key recovery via the CMS.

1) Keys are generated by the CMS at issuance, encrypted and stored on locally on the CMS workstation. When key recovery is required, the CMS initiates a request to the CA for the recovery key to unlock the escrowed encryption key for recovery.

2) Keys are escrowed at issuance, then encrypted and stored in the IdenTrust database. Key recovery is only available via a request from the RA local CMS station, via a secure channel to IdenTrust where the encrypted key is recovered and sent back through the same channel to the CMS.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Session Key encapsulation services are not provided.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

In the event a Participant CA or External RA operates an RA System or CMS external to IdenTrust, the Participant CA or External RA is required by contract to facility, management and operational controls equivalent to those implemented by IdenTrust for protection of such systems. Evaluation of Participant CA and External RA controls is required as a part of the compliance audit prior to IdenTrust providing authority to operate and part of the annual compliance audit requirement (see Section 8.0 Compliance Audits and Other Assessment: **Table - Required Best-Practices Annual Audits** which includes specific criteria that each audit satisfies).

IdenTrust's implementation of facility, management and operation controls is described in this Section 5.

5.1 Physical Controls

IdenTrust requires that equipment for CMS, RA Systems and LRA workstations located outside of IdenTrust's physical control be protected from unauthorized access. Operators of such equipment are obligated by contract, this CPS and the IGC-CP to implement physical Access Controls to reduce the risk of equipment tampering even when the Cryptomodule is not installed and activated. These security mechanisms are commensurate with the level of threat in the CMS, RA System or LRA environment and IdenTrust's procedures.

IdenTrust dedicates computer systems specifically to its PKI operations including the CA, CSA, CMS and RA functions as well as databases, networking and physical housing. These systems may be shared among IGC and other PKIs. IdenTrust CA, CSA, CMS and RA operations are serviced by trusted IdenTrust personnel. All trusted IdenTrust personnel meet the requirements of the IGC- CP for Trusted Roles.

Subscribers and Relying Parties do not have access to the PKI-specific CA, CSA, CMS, RA and LRA platforms. Logs, lists of Certificates that are Issued and Revoked, and the directory tree are located on a dedicated certification system, where they are not accessible for modification by anyone other than IdenTrust trusted 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.

IdenTrust's CA, CSA, CMS and RA equipment, including all Cryptomodules, are located in states which have statutes against computer trespass and intrusion. In addition, federal computer security legislation applies. Together, those laws generally forbid unauthorized use and access to IdenTrust computer equipment; however, legal advice should be obtained in specific cases.

5.1.1 Site Location and Construction

IdenTrust has two facilities dedicated to host CA, CSA, CMS and RA equipment. In selecting the appropriate facilities, risk management techniques have been used and controls have been designed to mitigate specific risks.

IdenTrust's CA, CSA, CMS and RA equipment are hosted in a primary facility that provides the highest-risk protection. For purposes of disaster recovery, a second facility in a geographically-diverse location has been selected and provides risk protection on par with the primary facility. Physical security controls protecting the certification platform and Cryptomodules[19] are described in the remainder of this Section. These physical security controls are intended as protection against theft, loss and unauthorized use.

[19] Cryptomodule Private Key storage practices are discussed in Section 6.2.7

In cases that IdenTrust may provide LRA equipment and services, the LRA equipment is hosted in a high-risk protection facility different from the primary and disaster recovery facilities where the CA, CSA and RA are located.

5.1.1.1 IdenTrust's Primary Facility for CA, CSA and RA Operations

IdenTrust's primary facility for CA, CSA, CMS and RA equipment is located in Utah, in the United States. It is housed in an unmarked building; the site is not identified as housing IdenTrust equipment in any 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, and contains a rigid exterior steel-braced frame and heavy concrete floor slabs; all are designed to minimize motion in case of an earthquake. The building has ready access to reliable sources of public power, backed up by a UPS and generator system as described in Section 5.1.3.1, and provides increased layers of security as an Individual moves closer to the critical assets and computer systems in the secure room. Roof access is through an internal stairwell in a mantrap, and its door is kept locked.

The data center is located on the second floor of the building and resides within an area with no windows. The secure room, where CA, CSA, CMS and RA equipment is hosted, is built within the data center. The secure room has only one access point, which is restricted as described below. Access through the ceiling and floor is prevented by the use of chain link fencing and metal cross rails. Multiple layers of security surround the CA, CSA, CMS, and RA equipment. These include exterior barriers requiring programmable electronic badges; mantraps; further barriers protecting various interior sections of the building; dual-factor authentication for entry into the data center areas; and two-person, dual-factor authentication including biometrics for entry into the secure room itself. The equipment is further protected from physical access by locked cabinets, to which only authorized persons possess the keys. The exterior and public interior areas of the building (e.g., halls) are under continuous recorded video surveillance by the building security staff; further recorded video surveillance within the secure room is provided by a second video system under the ownership and control of IdenTrust. No cameras are placed in such a way that sensitive data can be captured.

The secure room is also protected by motion sensors within the room, above the ceiling, and below the raised floor.

5.1.1.2 IdenTrust's Disaster Recovery Facility

IdenTrust's disaster recovery data center is located in Colorado, in the United States. This area is not prone to such environmental hazards as tornadoes, earthquakes, hurricanes, forest fires etc. The data center is housed in an unmarked concrete building; the site is not identified as housing IdenTrust equipment in any way. The data center is located on a raised level, at least 24 inches above the normal first-floor level, in an area with no windows. The secure cage is near the center of the data center room.

Multiple layers of security protect sensitive information and equipment, including trees, berms, and other natural barriers to external entry; controlled front-door access, requiring programmable electronic badges; restricted access to various sections of the building; dual-factor authentication for entry into the data center areas; and dual-factor authentication including biometrics for entry into and exit from the IdenTrust secure cage.

The IdenTrust secure cage uses chain-link metal caging material for the walls and ceiling, and has additional barriers to prevent access from under the floor. The area is surveilled 24x7 by both building cameras and IdenTrust's own camera system, which system can be monitored in real time, searched for past events, or logged if necessary, by the Security Office in Salt Lake City. No cameras are placed in such a way that on-

screen data could be captured. The secure cage is also protected by motion sensors.

5.1.1.3 IdenTrust's LRA Site

LRA equipment is located in a building geographically separated from the CA, CSA and RA site. The site is not identified as housing IdenTrust equipment in a publicly visible way. LRA equipment is located in an isolated and restricted-access room on an upper floor of the building.

The multiple layers of security surround the LRA equipment, including external building doors with security patrols and restricted access during nonbusiness hours, internal suite door with restricted access and 24x7x365 recorded video surveillance and, LRA room door with further restricted access.

5.1.1.4 External RA and LRA Sites

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.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

See details provided in the following sub-sections.

5.1.2.1.1 IdenTrust's Primary Facility for CA, CSA and RA Operations

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

The staff members from the hosting facility perform checks of the facility at least once per shift (at least three times daily), covering the facility's access points, cameras, and other aspects of a physical walk-through. Additionally, IdenTrust's Security Office performs a weekly check and review of the physical security integrity of the facility to ensure that alarms, access points, biometric readers to access the secure room, safes containing Cryptomodules and activation materials, video cameras, storage containers, access logging equipment, and other items, are 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 and reviewed with external auditors annually as part of audits as described in Section 8 (see Section 8.0 Compliance Audits and Other Assessment: **Table - Required Best-Practices Annual Audits** which includes specific criteria that each audit satisfies).

Programmable electronic badges for IdenTrust personnel working in the building are granted only upon authorization from the IdenTrust Security Office. Badges are programmed so that all building occupants have access only to their own authorized areas and data rooms.

Employees are prohibited from permitting unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas when accessing the facilities. Authorization for any persons, including vendors, repair persons, or visitors, to enter the IdenTrust portion of the facility must be obtained in advance from the Security Office or Operations Management.

Visitors to IdenTrust are allowed within the fence only with prior authorization from IdenTrust. Visitors must also properly identify themselves to the building personnel, as well as their purposes and the persons they will visit before being allowed on site. Visitors are allowed access IdenTrust offices only after their identities have been verified, they have signed an entry log, and at least one IdenTrust employee escorts them in all non-public areas of the building.

The secure room is physically secured and requires two-person, dual-authentication including biometrics for entry. The room is also surveilled with a 24x7x365 camera system whose output is maintained and reviewed by the Security Office. Only Trusted Role employees who have a clear need for access to the secure room are granted authorization by the CIO or Security Office for such access.

The secure room is required to be under 2-of-M person control at all times when Individuals are 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 provisions, as well as the access system described previously. At no time is any Individual left alone in the secure room. Two approved Trusted Role employees accompany any additional personnel or contractors at all times.

Access to storage safes located inside the IdenTrust secure room is controlled through Separation-of-Duties/Multi-party Control. The safes require two persons, each with an authenticator, for access. No single employee has access to both authenticators for any safe. Authenticator types are assigned based on Trusted Role, so that one Trust Role group has one type of authenticator and another group has another type. Once a safe is opened, all access to material inside it is documented through an access log and is signed for by two Trusted Role employees.

In addition to the electronic entry and exit logs generated by the access-control system, each entry into, and exit from, the secure room is logged manually with the respective persons, dates, times, and reasons for access. Prior to signing out and departing the secure room, IdenTrust personnel accessing the secure room are required by policy to check that all physical protection is in place, that all sensitive materials are securely stored, and that the alarms are properly armed.

CA, CSA, CMS and RA 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, CSA and CMS Cryptomodules are secured in the locked computer cabinets within the IdenTrust secure room when in use. When not in use the Cryptomodules and activation materials are stored in separate safe boxes within the secure room, or in the secure off-site facility as described in Section 5.1.6. The Security Office reviews 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 the Security Office.

5.1.2.1.2 Disaster Recovery Facility

The staff of the data center facility performs checks of the facility at least once a day, covering the facility's access points, cameras, and other aspects of a physical walk-through. A record is kept that describes the types of checks performed, the time, and the person who performed them. Records are kept for not less than one year and reviewed with external auditors on an annual basis as part audits performed according to Section 8 (see Section 8.0 Compliance Audits and Other Assessment: **Table - Required Best-Practices Annual Audits** which includes specific criteria that each audit satisfies).

IdenTrust personnel require programmable electronic passcards to access the building, and to enter IdenTrust areas within the building. Programmable electronic passcards for IdenTrust-related personnel working in the building are granted upon prior authorization from the IdenTrust Security Office. If access is required for someone not previously so authorized, that person may enter the building upon presenting appropriate identification to the building security staff, and while in the company of an IdenTrust Trusted Role employee.

Access to the area where the secure cage is located requires two-person, dual-factor authentication including biometrics. The cage is equipped with an IdenTrust-owned 24x7x365 camera system that can be monitored, searched, and logged by the IdenTrust Security Office in Salt Lake City. The area surrounding the IdenTrust secure cage is also surveilled by building cameras that are constantly monitored by building security staff, with video recordings retained for at least 90 days. Only authorized IdenTrust Trusted Role employees or their authorized and identified visitors are granted access to the secure cage.

CA equipment is located inside locked computer cabinets within the IdenTrust secure cage. Cabinet keys are maintained by the same number of Trusted Role employees who have access to the secure cage.

5.1.2.1.3 IdenTrust's LRA Site and Room

The IdenTrust office, entries, and the room where the LRA equipment is located are video-recorded. The IdenTrust Security Office performs periodic checks and reviews of the security integrity of the facilities to ensure that alarms, access points, video cameras, storage containers, access logging, etc., are operational and/or functioning correctly. A record is kept that describes the types of checks performed, the times, and the persons who performed them. Records are kept for no less than one year and reviewed with external auditors as a part of the audits described in Section 8 (see Section 8.0 Compliance Audits and Other Assessment: **Table - Required Best-Practices Annual Audits** which includes specific criteria that each audit satisfies).

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

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

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

5.1.2.2 Physical Access for RA Equipment

See details provided in the following sub-sections.

5.1.2.2.1 External RA and LRA Equipment

In cases where RAs are external to IdenTrust, RAs and LRAs are obligated by contract, the IGC-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.

5.1.2.3 Physical Access for CSS Equipment

See Section 5.1.2.1

5.1.2.4 Physical Access for CMS Equipment

See Section 5.1.2.1

5.1.3 Power and Air Conditioning

See details provided in the following sub-sections.

5.1.3.1 Primary Facility

The facility housing the IdenTrust CA, CSA, CMS, RA and Repository 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. Site power is supplied by a generating plant approximately three-tenths of a mile away, through a substation that is approximately two-tenths of a mile away, along power lines that cross private property only and are not located near public throughways. 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. A robust uninterruptible power supply (UPS) provides temporary power for the facility and automatically activates the generator when a power failure is detected. The fuel tank can be refueled on the go for continuous service, with priority-refill contracts in place. This system is tested weekly, and under load at least annually. The secure room (where the IdenTrust CA, CSA, CMS, RA and Repository systems are located) is controlled for humidity and temperature 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, CMS, RA and Repository equipment is supplied with air conditioning and power that is sufficient to provide a reliable operating environment. In the event of a major power outage the data center is equipped with a UPS system that is adequate to provide power until the multiple onsite generators are delivering power. The generators can be refueled on the go for continuous service, and priority-refill contracts are in place. The data center where the secure cage is located contains 10 HVAC units that control temperature, keeping it within 2 degrees of 70 F. Relative humidity is maintained within 2% of 40%.

5.1.4 Water Exposures

See details provided in the following sub-sections.

5.1.4.1 Primary Facility

To mitigate the risks of water damage, multi-user computers and communications facilities for the CA, CSA, CMS and RA Systems are housed on the second floor. Equipment sits on a raised floor approximately 18" above the concrete flooring. No water lines exist within the ceiling or overhead in any way. All environmental equipment, such as cooling equipment, is located around the outside perimeter of the data center. Restroom facilities are not located directly above the areas hosting the systems. A braided cable is located below the floor and is capable of detecting even minute amounts of water and alerting the data center operations staff. The IdenTrust secure room fire suppression provides non-liquid oxygen evacuation to stifle combustion. The only water threat to systems is humidity control equipment that employs a water-based environmental maintenance system. The water leads and piping for this equipment are below the raised floor and behind a 4-inch concrete barrier, thus isolating under-floor wiring from potential plumbing hazards.

5.1.4.2 Disaster Recovery Facility

In the disaster recovery facility, equipment sits on a raised antistatic flooring approximately 24" above the concrete floor. All HVAC equipment is located at the perimeter of the data room, and adjacent areas are monitored with moisture sensors. Braided moisture sensing cable is installed in areas that may be exposed to a potential moisture risk.

5.1.5 Fire Prevention and Protection

See details provided in the following sub-sections.

5.1.5.1 Primary Facility

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

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

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

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

5.1.5.2 Disaster Recovery Facility

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

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

5.1.6 Media Storage

Sensitive CA, CSA,CMS and RA information (including audit and archive data) written to magnetic tape, Cryptomodules, or other storage media, is stored one of two locations: (1) within dual-control safes inside the secure room, or (2) at an offsite storage facility. Certain CA, CSA, CMS and RA sensitive information, such as security audit logs, is written to non-rewriteable media (e.g., CD-ROM or DVD-ROM) and is placed within tamper evident bags that are tracked via custody matrix.

Within the secure room, backup copies of PKI materials, including CA, CSA and CMS Cryptomodules and activation materials, are stored within the safes using the controls described in Section 5.1.2.1. All additions to or removals from the safes are tracked with logs that require two Trusted Role employees to sign them acknowledging such actions. Cryptographic materials and activation materials are contained in separate safes.

The offsite storage facility is used for backup tapes and related materials, and also for tertiary copies of CA, CSA, and CMS Cryptomodules and activation materials.

This facility is situated inside a solid granite mountain a sufficient distance away from the primary data center to ensure that both sites are not likely to be impacted by the same natural or manmade event. The facility was constructed for and is dedicated to vital records and information protection. The vault is designed to be unaffected as a result of floods, earthquakes, fires, and manmade disasters.

The storage vault is constructed of cement and steel, surrounded by 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 and fire extinguishers and independent power sources. Thus, records are maintained in a temperature and humidity controlled environment that meets or exceeds all federal requirements for archival storage.

The vault entrance is protected by three separate security gates and a 12,000 pound vault door.

Only one point of ingress and egress exists for the facility and for the vault itself. Any attempt to use explosives or other force on the gates and vault door would be detected by heat, motion, and/or seismic sensors that trigger an alarm system. Mantraps and sign-in logs are utilized for physical Access Control and auditing.

The vault is under 24-hour electronic surveillance, and it is regularly patrolled by local law enforcement during nonbusiness hours. During business hours, an armed guard escorts all persons entering the facility and the vault area proper. All access to the vault requires at least 24-hour advance notice.

Because both backup tapes and tertiary copies of CA, CSA, and CMS Cryptomodules and activation materials are stored in this offsite location, IdenTrust has established procedures to ensure segregation between the two types of materials:

- Backup tapes are transported in metal boxes with no outside hinges, and with padlocks to which only IdenTrust has the keys;
- CA, CSA, and CMS materials are transported in minisafes for which only IdenTrust has the combinations. Both combinations and keys are stored securely within the secure room;
- Neither the boxes nor the safes have external markings indicating their IdenTrust ownership or their contents;
- At the offsite facility, the backup tapes are stored in a separate location from the CA, CSA, and CMS materials; and
- At the offsite facility, the minisafes are stored within a separate vault inside the facility's main vault. Only the storage facility personnel have the combination to the separate vault, and only IdenTrust personnel have the combinations to the minisafes.

Shipment to and from the off-site location is conducted via bonded couriers who are employees of the storage facility. By policy and practice, visitors to the vault may not deposit or remove any materials directly; all materials must be transported by the facility's couriers to and from predefined destinations.

Within its office spaces, IdenTrust adheres to a strict "clean desk" policy by which all hardcopy sensitive information not in use is locked in file cabinets, desks, safes, or other furniture. Likewise, all computer media (such as tapes, CD-ROMs, DVD-ROMs) containing sensitive information is locked in similar enclosures when not in use or when not in a clearly visible and attended area.

5.1.7 Waste Disposal

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

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

When electronic media such as hard drives that have stored sensitive CA information reach their end of life, the data is erased, if possible, by using a secure multi-pass procedure. The media is then physically destroyed by degaussing, followed by shredding or other physical destruction approved by the Security Office. No end-of-life media that has contained sensitive information leaves IdenTrust premises intact.

The Security Office is contacted for assistance in disposing of media and equipment no longer being used by the CA, CSA and RA Systems. Such media and equipment are stored at a level of security appropriate to the level of sensitivity of information contained in the media and equipment until they can be effectively sanitized or destroyed.

Prior to destruction, Cryptomodules remain in locked safes within the secure room; sensitive backup tapes remain in the offsite secure location's vault. All Cryptomodules are Zeroized after the Keys on them are no longer needed. If Zeroization procedures fail, then they are physically destroyed.

5.1.8 Off-site Backup

The CA systems are backed up at the primary facility in Utah to a local backup server. Data is also replicated in near real time to the system at the disaster recovery site. These system backups provide the capability to recover from a system failure. Incremental backups are performed daily. Full system backups are performed every week. Backups are sent to the offsite, hardened, secure mountain storage vault described in Section 5.1.6 at least twice a week.

At least annually, backup tapes are consolidated and archive media is identified and stored in the off-site storage vault to satisfy IdenTrust's 10.5 year data retention schedule.

Components needed to restore the CA, CSA, CMS and RA Systems are stored in separate areas of the off-site secure vault facility (see Section 5.1.6). The most sensitive material, including Cryptomodules, Activation Keys, and password copies, are stored within locked mini-vaults and their combinations are under IdenTrust control. Other material is 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 so as not to reveal IdenTrust ownership or their content.

Only those IdenTrust employees in Trusted Roles, and only with a need-to-know status, as authorized by the CIO or the Security Office are authorized access to the off-site storage facility. In cases where a request is made to deliver backup material to IdenTrust facilities, the request is made by a Trusted Role employee who has been previously identified to the offsite facility as one who has authority to make such a request. The offsite facility then verifies the request with a second Trusted Role employee who has been identified previously to the offsite facility as having verification authority.

5.2 Procedural Controls

5.2.1 Trusted Roles

All employees, contractors, and consultants of IdenTrust, CAs, RAs and LRAs who have access to or control over cryptographic operations that may materially affect the Issuance, use, Suspension, or Revocation of Certificates, including access to restricted operations of IdenTrust's CA, CSA, CMS, RA, LRA Systems and Repository are, for purposes of this CPS, considered as serving in a Trusted Role. Such personnel include, but are not limited to system administration personnel, system operators, engineering personnel, and operations managers who oversee CA, RA or LRA operations. The functions and duties performed by these persons are also separated and distributed so that one person alone cannot circumvent security measures or subvert the

security and trustworthiness of the PKI (see Section 5.2.4). Oversight of IdenTrust's Trusted Roles is performed by the Risk Management Committee, Operations Management, the Human Resources Department, and Executive Management.

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

The following table maps the IGC-CP Trusted Roles to IdenTrust-internally-defined roles in Sections 5.2.1.1-5.2.1.10. Two roles, TA and Machine Operator, do not necessarily need to be Trusted Roles, but are included here for role clarity.

IdenTrust Trusted Role Matrix

	IdenTrust Internally Defined Role							
IGC-CP Role	**CA Administrator**	**LRA**	**System Administrator**	**Security Officer**	**External RA Administrator**	**Trusted Agent**	**Machine Operator**	**PKI Consultant**
CA Administrator	X							
CA Agent		X						
CA Auditor				X				
CA Operator			X					
CSA Administrator	X							
CSA Auditor				X				
CMS Administrator	X							
CMS Operator			X					
CMS Auditor				X				
RA Administrator		X			X			X
Other Role						X	X	

5.2.1.1 Certification Authority (CA) Roles

All Certificates that are Issued under the IGC Root Certificate are Issued under the control of IdenTrust Operations Management as operator of the IGC Root CA or as the CA services provider for the IGC PKI. The responsibilities for CA functions are carried out by IdenTrust employees acting in their Trusted Roles and include administration and operation tasks described in the IGC-CP.

5.2.1.1.1 CA Administrator

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

- Installation and configuration of the CA software;

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

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

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

CA Administrators do not Issue to Subscribers.

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

5.2.1.1.2 CA Agent

Within IdenTrust, the CA Agent responsibilities are performed by an LRA (see Section 5.2.1.5). CA Certificates generation responsibility is also shared by Help Desk Representatives (see Section 5.2.1.11).

5.2.1.1.3 CA Operator

Within IdenTrust, the CA Operator functions are divided between the CA Administrator and the System Administrator. See Section 5.2.1.8 for details on CA Operator's tasks performed by the System Administrator.

5.2.1.1.4 CA Auditor

Within IdenTrust, the CA Auditor functions are performed by the IdenTrust Security Office with oversight by the IdenTrust Security Officer (see Section 5.2.1.10).

5.2.1.2 Certification Status Authority ("CSA") Roles

The responsibilities for CSA functions are carried out by IdenTrust employees acting in their Trusted Roles and include administration and operation tasks described in the IGC-CP.

5.2.1.2.1 CSA Administrator

Within IdenTrust, CA Administrators also carry out the responsibilities of the CSA Administrator. The CSA Administrator responsibilities and operating procedures performed by IdenTrust CA Administrators, as they relate to CSA Operation, are as follows:

- Installation, configuration, and maintenance of the CSA software;
- Generating and backing up CSA Keys (performed under two person control);
- Management of CSA Key and Certificate lifecycle, including renewal of OCSP Responder Certificates (performed under two person control);

- Establishing and maintaining system accounts and configuring audit parameters; and
- Operation of the CSA equipment.

5.2.1.2.2 CSA Auditor

Within IdenTrust, the CSA Auditor functions are performed by the IdenTrust Security Office with oversight by the IdenTrust Security Officer (see Section 5.2.1.10).

5.2.1.3 Card Management System ("CMS") Roles

The responsibilities for CMS functions are carried out by IdenTrust employees acting in their Trusted Roles and include administration and operation tasks described in the IGC-CP.

5.2.1.3.1 CMS Administrator

Within IdenTrust, CA Administrators also carry out the responsibilities of the CMS Administrator. The CMS Administrator responsibilities and operating procedures performed by IdenTrust CA Administrators, as they relate to CMS Operation, are as follows:

- Installing and maintaining the CMS;
- Establishing and maintaining CMS accounts;
- Configuring CMS application and audit parameters; and
- Generating and backing up CMS Keys.

5.2.1.3.2 CMS Auditor

Within IdenTrust, the CMS Auditor functions are performed by the IdenTrust Security Office with oversight by the IdenTrust Security Officer (see Section 5.2.1.10).

5.2.1.3.3 CMS Operator

Within IdenTrust, the CMS Operator functions are performed by the System Administrators. For functions performed by the System Administrator (see Section 5.2.1.8).

5.2.1.4 Registration Authority ("RA") Administrator

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

5.2.1.4.1 External RA Administrator

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

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

5.2.1.4.2 IdenTrust Internal RA Administrator

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

5.2.1.5 Local Registration Authority ("LRA")

An LRA is a Trusted Role and performs the roles, responsibilities and operating procedures, as they relate to

RA Operations, are as follows:

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

5.2.1.6 Trusted Agent ("TA")

A Trusted Agent is a person authorized to act as a representative of an LRA or RA 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 LRA/RA only to verify the identity of the Subscriber. Trusted Agents are not subject to Background Checks or Security Clearance. The Trusted Agent is not a Trusted Role (see Section 1.3.5). TAs differ from LRAs in that they do not have privileged access to the CA system to take action to Approve, Reject or Revoke Certificates.

5.2.1.7 Machine Operator

There are two Machine Operator roles—a Primary Machine Operator and a Secondary Machine Operator.

5.2.1.7.1 Primary Machine Operator

A Primary Machine Operator is named as a such under the Subscribing Organization Authorization Agreement entered into in connection with a Device and such Primary Machine Operator represents the Device that is named as Certificate subject in a Certificate issued in connection with such Subscribing Organization Authorization Agreement; provided, however, save with respect to revocation and suspension requests, only a Primary Machine Operator may represent a Device to the IdenTrust CA. The Primary Machine Operator works with the LRA, RA or TA to register Devices in accordance with Section 3.2.3.4. The Primary Machine Operator may designate Secondary Machine Operators in relation to a Device Certificate in relation to which the Primary Machine Operator acts on behalf of the Subscriber.

Primary and Secondary Machine Operators may share responsibilities for the Device, as well as the duties of a Subscriber, except as provided otherwise in 5.2.1.7.1.

Primary Machine Operators do not need to be Trusted Roles; however, they must have their identity verified to a Level of Assurance equal to or higher than the Device Certificate for which they are responsible.

5.2.1.7.2 Secondary Machine Operator

Secondary Machine Operators are designated by being named as such in the current Machine Operators List which is included in the Subscribing Organization Authorization Agreement, by the Primary Machine Operator, during the Device Certificate Registration process and are archived in the CA database as a part of the Device Certificate account.

Secondary Machine Operators share responsibilities with the Primary Machine Operator as duties of a Subscriber that is a Device; provided, however, Secondary Machine Operators are prohibited from interacting with the CA in any way with reference to the Device Certificate of such Subscriber save for communicating to the CA a request for the Suspension or Revocation of such Device Certificate.

Secondary Machine Operators are not Trusted Roles and do not require identity verification by the CA.

5.2.1.8 System Administrator

IdenTrust's System Administrators are responsible for the following:

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

5.2.1.9 Network Engineer

IdenTrust's 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.

5.2.1.10 Security Officer

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

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

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

The Security Officer performs, or oversees, internal compliance audits to ensure that CA, CSA, CMS, RA and LRA Systems are operating in accordance with this CPS, IGC-CP and any Memorandum of Agreement ("MOA") applicable to the operation of the IdenTrust IGC PKI.

5.2.1.11 Help Desk Representative

IdenTrust's Help Desk Representatives perform the following duties:

- Troubleshooting of Certificate lifecycle events problems;
- Maintaining Subscriber account information within the RA System;
- Initiating Revocation processes;
- Initiating Suspension processes;

- Initiating escalation of suspected Private Key compromise, or other reasons for potential Certificate Revocation;
- Generation of the IGC Root CA Certificate, Sub CA or Participant CA Certificates, CA Certificate Re-Key, and Revocation of CA Certificates (all CA Certificate lifecycle events performed under two person control); and
- Generation of the CMS Certificates and Revocation of CMS Certificates (all CMS Certificate lifecycle events performed under two person control).

5.2.1.12 PKI Consultant

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

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

5.2.1.13 Operations Manager

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

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

5.2.2 Number of Persons Required per Task

IdenTrust has procedural and operational mechanisms in place to ensure that no single Individual may perform sensitive activities alone. These mechanisms apply principles of Separation-of-Duties/Multi-party Control and require the actions of multiple persons to perform such sensitive tasks as:

- Handling of CA, CSA, RA, CMS and Content Signing Keys throughout the entire Key lifecycles from Generation and activation, into secure storage, through to eventual destruction; and
- Non-automated (manual) Certificate Issuance processes.

Physical and logical Access Controls are invoked to maintain Multi-party Control over CA, CSA and CMS Cryptomodules (see Sections 5.1.2.1 and 6.2.2). Generation, backup, or activation of the Certificate Signing Private Keys requires the actions of at least two Individuals, one of whom is a CA Administrator and the other who may not be a Security Officer.

5.2.3 Identification and Authentication for Each Role

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

the performance of their Trusted Role; (iv) given an account on a computer connected to the CA system, or (v) otherwise granted physical or logical access to a component of the CA system.

Each of these access methods (Certificates and system accounts) are: (i) directly attributable to the Individual; (ii) password protected; (iii) not shared; and (iv) restricted to actions authorized for that role through the use of CA software, operating system and procedural controls. If accessed across shared networks, CA operations are secured, using Cryptomodules, strong system authentication, and AES encrypted SSH connections.

Individuals who administer a CMS or RA System are allowed access only when authenticated using an IGC Certificate of the highest Assurance Level as Issued by the CA in connection with the CMS or RA.

Individuals who access a CMS or RA System to perform RA functions are allowed access only when authenticated using an IGC Certificate of an Assurance Level equal to or higher than the Assurance Level of the Certificates for which services are performed by that individual.

5.2.4 Separation of Roles

Trusted Roles maintain strict Separation-of-Duties/Multi-party Control. These controls are audited annually by a third party auditor as part of the audits performed as described in Section 8 (see Section 8.0 Compliance Audits and Other Assessment: **Table - Required Best-Practices Annual Audits** which includes specific criteria that each audit satisfies).

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

- **CA/CSA/CMS Administrator.** No person participating as IdenTrust CA/CSA/CMS Administrator will assume the role of Security Officer, LRA, System Administrator, Network Engineer or Operations Manager.
- **Local Registration Authority.** An LRA may not assume an Operations Manager, CA/CSA/CMS Administrator, RA Administrator, System Administrator, Network Engineer, Security Officer or management oversight role (Risk Management, Operations Management, Human Resources, or Executive Management).
- **RA Administrator** (whether an IdenTrust Internal RA Administrator or an External RA Administrator). An RA Administrator may not assume the Operations Manager, LRA, System Administrator, Network Engineer, or Security Officer role.
- **System Administrator.** A System Administrator may not assume the Security Officer, LRA, CA/CSA/CMS Administrator or Operations Manager role.
- **Network Engineer.** The Network Engineer may not assume the Security Officer, LRA, CA/CSA/CMS Administrator or Operations Manager role.
- **Security Officer.** The Security Officer may not serve in any other trusted role (e.g. the roles of CA/CSA/CMS Administrator, LRA, RA Administrator, Systems Administrator, or Network Engineer).
- **Help Desk Representative.** Help Desk Representatives may not serve in the role of CA/CSA/CMS Administrator, RA Administrator, System Administrator, or Network Engineer.
- **PKI Consultant.** PKI Consultants may not serve in the roles of CA/CSA/CMS Administrators, System Administrators, Network Administrators, and Security Officers.
- **Operations Manager.** The Operations Manager may not serve as CA/CSA/CMS Administrator, Systems Administrator, LRA, or Network Engineer.

CA systems also identify and authenticate users and ensure through the use of Access Controls and policy that no user identity can assume both the Administrator and Officer, the Administrator and Auditor, or the

Officer and Auditor roles. Additional Separation-of-Duties controls are discussed in Section 5.2.1 above.

Separation of duties between System Administrators and CA/CSA/CMS Administrators is further enforced separating the servers' root-level access and administrative passwords for the function running on the server (i.e., CA, CSA, CMS, etc.). Without the cooperation of both administrators, IdenTrust software is inoperable for purposes of processing requests, generating responses, generating Certificates and CRLs, re-keying, and designating LRAs.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience and Security Clearance Requirements

Personnel for Trusted Roles are identified in a list as described in Section 5.2.1. Trusted Roles are selected on the basis of trustworthiness and integrity as described in Section 5.3.2 below. Personnel who administer or operate components of the CA, CSA, CMS and IdenTrust RA Systems, including LRAs, are under the direct control of IdenTrust and meet the following requirements:

- Successful completion of appropriate training programs;
- Demonstrated ability to perform duties, as indicated by annual performance reviews;
- Trustworthiness as initially determined by a background investigation;
- No other duties that would interfere or conflict with the duties of their Trusted Role;
- Not previously relieved of duties in a Trusted Role for reasons of negligence or non-performance of duties as indicated by employment records;
- Not convicted of a felony offense as indicated by a criminal background check;
- Appointed in writing by Operations Management or pursuant to written contract with IdenTrust or in a Certificate of Incumbency, as evidenced by records maintained for such purpose by such Organization; and
- Hold United States citizenship*.

For External RAs, the Trusted Roles including RA administrators and LRAs are required to demonstrate compliance with at least one of the following requirements:

- The person shall be a citizen of the country* where the RA is located;
- For PKIs operated on behalf of multinational Governmental Organizations, the person shall be a citizen of one of the member countries; or
- For PKIs located within the European Union, the person shall be a citizen of one of the member states of the European Union; or
- The person shall have a security clearance equivalent to U.S. Secret or higher Issued by a NATO member nation or major non-NATO ally as defined by then International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32; or
- For RA Administrator and LRAs, in addition to the above, the person may be a citizen of the country where the function is located.

***Note:**

For PKIs operated only at IGC Basic Software, IGC Medium-CBP and IGC Medium Hardware-CBP Assurance Levels, there is no citizenship requirement or security clearance required.

5.3.2 Background Check Procedures

Persons appointed by IdenTrust to serve in Trusted Roles have undergone local and national criminal background checks and drug tests in conformance with the jurisdictions in which they reside. The following items are examples of the background checks IdenTrust makes:

- A criminal history check, performed through a commercial database, must show no felony convictions.
- Driver's license records, checked through a commercial database, will indicate whether the person has a record of serious or criminal driving violations.
- A Social Security trace must show that 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 numbers or similar identifiers.
- A verification check of the highest educational degree claimed by the Individual must show that the degree was indeed awarded, regardless of the date of award.
- Reference checks

The period of investigation covers at least the previous five years for employment, education, criminal, and references, and the previous three years for places of residence. Adjudication of the background investigation is performed by a competent adjudication authority using a process consistent with U.S. Executive Order 12968 August 1995, or equivalent.

RAs external to IdenTrust are obligated by contract, this CPS, and the IGC-CP to implement background check procedures equivalent to the ones explained above. To the extent that any of the foregoing cannot be met due to circumstances peculiar to that party, substantially similar procedures must be performed and may include background checks performed by Government Agencies or other competent providers of such services in their jurisdictions.

Background checks are renewed at a minimum every ten years. Additional checks may be performed at management's sole discretion. A successfully adjudicated National Agency Check with Written Inquires (NACI) or National Agency Check with Law Enforcement Check (NACLC) on record is deemed to have met the minimum standards specified above. If a National Agency Check with Written Inquires (NACI) or National Agency Check with Law Enforcement Check (NACLC) is the basis for background check, the background refresh shall be in accordance with the corresponding formal clearance. If the initial or subsequent background checks reveal a material misrepresentation by the Individual, substantially unfavorable comments from persons contacted, a criminal conviction, or personal financial problems, then the Issue is brought to the attention of the Chief Information Officer and the Security Office, who will evaluate the severity, type, magnitude, and frequency of the behavior or actions of the Individual and determine the appropriate action to be taken, which may include removal from a Trusted Role.

The acquisition and use of all background check information is in accordance with stipulations in Section 9.4 of this CPS.

5.3.3 Training Requirements

Each person performing duties with respect to the operation of the CA, CSA, RA, and LRA shall receive comprehensive training regarding such person's duties. Training is conducted regarding security principles and procedures, understanding common threats to the information verification process (including phishing and other social engineering tactics), PKI hardware and software used, and disaster recovery and business continuity procedures. IdenTrust maintains records of the training received by persons in Trusted Roles and other important roles. External RAs are obligated by contract and this CPS and IGC-CP to maintain a record of training provided to such personnel. Specific additional areas are covered for each role as outlined in the following sub-sections.

5.3.3.1 CA Administrators

CA Administrators receive training associated with the following topics:

- Key Pair Generation and Certificate Issuance, Re-Keying and Revocation of Root CA, Sub CAs, CSAs and CMSs;

- Configuration and posting of Certificates and CRLs;
- Daily maintenance and other CA-, CSA-, CMS-related administrative functions; and
- Initializing CA, CSA and CMS hardware.

5.3.3.2 LRAs and TAs

LRAs and TAs receive training associated with the following topics:

- Confirming identity, either through personal contact or through TAs;
- Entry of Applicant information and verifying correctness;
- Securely handling requests to and responses from CAs;
- The Certificate Revocation process; and
- The Certificate Issuance process.

5.3.3.3 RA Administrators

RA Administrators receive training associated with the following topics:

- Operating systems, software applications and hardware (including Cryptomodules) used within the RA System, including but not limited to those components that perform enrollment services, card or Cryptomodule personalization services, Certificate delivery services, backup, logging, security and Key storage;
- Key Pair Generation and Certificate Issuance, Re-Keying and Revocation of Subscriber Certificates, including configuration and use of the RA System to Digitally Sign and receive communications from the CA system; and
- Security threats, vulnerabilities and countermeasures, including but not limited to implementation of security policies and practices, physical and logical Access Controls, and system monitoring.

5.3.3.4 System Administrators

System Administrators receive training associated with the following topics:

- Operating systems and software applications used within the PKI systems;
- Backup applications and procedures;
- Use of database tools including reporting and maintenance;
- Restriction for privileged system use; and
- Generation of audit data.

5.3.3.5 Network Engineers

Network Engineers receive training associated with the following topics:

- Network architecture and equipment used in the PKI;
- Proper and secure configuration and switching for the network;
- Intrusion detection monitoring; and
- Requirements for securing network transmissions.

5.3.3.6 Security Officers

Security Officers receive training associated with the following topics:

- Security risk assessment and analysis;
- Security policies and guidelines;
- Computer attack trends, security threats and vulnerabilities;
- Physical security and physical Access Controls;

- Networks, distributed systems trust relationships, PKI and cryptosystems;
- Firewalls and other network security devices;
- Event logging and auditing; and
- Incident response and contingency planning.

5.3.3.7 Help Desk Representatives

Help Desk Representatives receive training associated with the following topics:

- End user systems;
- Proper and secure handling of sensitive customer information; and
- Use of trouble-tracking software.

5.3.3.8 Operations Management Personnel

Operations Management Personnel receive training associated with the following topics:

- Operating systems and software applications used within the PKI system;
- Network architecture; and
- Audit and risk management oversight.

5.3.3.9 Trusted Agents

Trusted Agents receive training associated with the following topics:

- Confirming identity, and providing identity information to LRAs or RAs;
- Securely handling requests to and responses from LRAs or RAs; and
- Securely handling distribution and collection of Cryptomodules.

5.3.4 Retraining Frequency and Requirements

Any significant change (e.g., a planned upgrade of CA equipment, software or changes in procedures) to the CA, CSA, CMS, RA or LRA Systems requires that effected personnel receive additional training. Through change control processes (see Section 6.6), an awareness plan is prepared and training provided to effected personnel. IdenTrust maintains records of the training.

5.3.5 Job Rotation Frequency and Sequence

Job rotation is implemented when in the judgment of management it is necessary to ensure the continuity and integrity of PKI-related services, but is not required at any specific frequency.

5.3.6 Sanctions for Unauthorized Actions

Failure of a Subscriber, a person performing a Trusted Role, an agent of IdenTrust, a CA, RA or agent of an RA to comply with the provisions of the IGC-CP or this CPS, whether through negligence or malicious intent, will subject such entity or Individual to appropriate administrative and disciplinary actions, which may include termination as an employee or agent and possible civil and criminal sanctions. Any person performing a Trusted Role who is cited by management for unauthorized or inappropriate actions, unsatisfactory background investigation results, or similar infractions of IdenTrust policy and procedure will be immediately removed from the Trusted Role pending management review. Subsequent to management review, review of investigation results, discussions with the Individual, and/or discussions with the relevant CA or RA, the Individual may be reassigned to the Trusted Role, transferred to a non-trusted role, removed from ACLs, or dismissed from employment as appropriate.

5.3.7 Independent Contractor Requirements

IdenTrust policy firmly discourages the use of independent contractors in any Trusted Role. Independent contractors who are assigned to perform Trusted Roles are subject to the duties and all requirements of this CPS. Independent contractors are subject to sanctions stated in Section 5.3.6 for unauthorized actions or failure to comply with the provisions of the IGC-CP, this CPS or the contract between IdenTrust or the relevant CA or RA and the independent contractor.

5.3.8 Documentation Supplied to Personnel

Personnel in Trusted Roles are provided with the documentation necessary to define and support the duties and procedures of the role to which they are assigned. IdenTrust provides a copy of the IGC-CP, this CPS and technical and operational documentation needed to fulfill their tasks. The information may be provided in print or on-line, and may consist of internal IdenTrust system and security documentation, IdenTrust policies and procedures, discipline-specific books, treatises and periodicals, and other information developed by or supplied to IdenTrust, or the CA or RA that is relevant to the role being performed. Participant CAs or RAs external to IdenTrust are obligated by contract, the IGC-CP and this CPS to provide to their LRAs all relevant documentation, policies, contracts, and forms required to perform their duties.

5.4 Audit Logging Procedures

For purposes of security audit, events related to operation of the IdenTrust PKI are recorded as described in this Section 5.4, whether the events are attributable to human action (in any role) or are automatically invoked by the equipment that is used to register Applicants, generate, sign and manage Certificates and provide Revocation information. Where possible, the audit data is automatically collected; when this is not possible, a logbook or other physical mechanism is used. All security logs, both electronic and non-electronic, are retained in accordance with requirements of Section 5.4.3 and are made available during compliance audits. IdenTrust operates some components in a virtual machine environment (VME). In these cases, audit logs are generated for all applicable events on both the virtual machine (VM) and isolation kernel (i.e. hypervisor).

5.4.1 Types of Events Recorded

All systems require I&A at system logon with unique user name and password (or the use of Cryptomodules). The accessing of systems, equipment and applications is logged to establish the accountability of system operators who initiate system actions.

IdenTrust's CA, CSA, CMS, RA and LRA equipment, inclusive of operating systems, routers, firewalls, applications, databases and all physical access checkpoints automatically record all significant events related to the operations (installation, modification, and system accesses). For all systems, the minimum information recorded includes the following: type of event, time event occurred; who caused the event; and a success or failure indication. For some types of events, these minimums may be expanded to include: source or destination of a message, and the disposition of a created object (e.g., a filename).

IdenTrust and RAs external to IdenTrust are required by the IGC-CP and this CPS to configure the systems to automatically log the PKI component events as described above and the specific audit events as described in the table below. Where not possible to automatically log events, events must be logged manually.

Table: Types of Events Recorded

Ref ID	Auditable Event	CA	CMS	CSA	RA	LRA
1	SECURITY AUDIT					

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

Ref ID	Auditable Event	CA	CMS	CSA	RA	LRA
2.e	An administrator changes the type of authenticator, e.g., from a password to a biometric - date and time, type of event, and identification of user making modification are logged automatically by the operating system and manually through change management procedures. Changes in configuration files, security profiles and administrator privileges are logged through a combination of operating system and manual change management procedures.	X	X	X	X	X
3	**LOCAL DATA ENTRY**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
3.a	All security-relevant data that is entered in the system – the system records the identity of the local operator performing local data entry so that the accepted data can be associated with the operator in the audit log.	X	X	X	X	X
4	**REMOTE DATA ENTRY**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
4.a	All security-relevant messages that are received by the system - date and time, digital signature/authentication mechanism, and message are automatically logged by the application	X	X	X	X	X
5	**DATA EXPORT AND OUTPUT**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
5.a	All successful and unsuccessful requests for confidential and security-relevant information - date and time of attempted access, username or identity asserted at time of attempt, record of success or failure, logged through a combination of automatic and manual logging. Manual logging by Security Team also collects name of person reporting the event and resolution.	X	X	X	X	X
6	**KEY GENERATION**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
6.a	Whenever a component generates a Key (not mandatory for single session or one-time use symmetric Keys) – CA system automatically records all significant events related to CA operations, including Key Generation. Additionally, manual and audiovisual records of CA, CSA and CMS Key Generation are created. RA System and LRA Key and Certificate generation events are automatically recorded by the CA system.	X	X	X	X	X
7	**PRIVATE KEY LOAD AND STORAGE**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
7.a	The loading of Component Private Keys – An auditable log of all physical access to production CA, CSA, RA and CMS Cryptomodules is maintained, which records action taken, date and time action was taken and name of person who performed action. An electronic log of access to the LRA's Cryptomodule is maintained by the RA System that is accessed.	X	X	X	X	X

Ref ID	Auditable Event	CA	CMS	CSA	RA	LRA
7.b	All access to Certificate subject Private Keys retained within the CA for Key recovery purposes – Date, time, messages between the CA and the requesting component and indicator of success or failure are automatically logged.	X	X	-	-	-
8	**TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
8.a	All changes to the trusted component Public Keys, including additions and deletions are automatically logged through the applications or through manual change management processes and authorization forms.	X	X	X	X	X
9	**SECRET KEY STORAGE**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
9.a	The manual entry of secret Keys used for authentication - secret Keys (PED keys) used to access the CA's Cryptomodules is maintained under separate control from the CA's Cryptomodule in accordance with the principles of Separation-of-Duties/Multi-party Control stated in Section 5.2. An auditable log of the use of PED keys for authentication is maintained, which records action taken, date and time action was taken and name of person who performed the action.	X	X	X	X	X
10	**PRIVATE AND SECRET KEY EXPORT**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
10.a	The export of private and secret Keys (Keys used for a single session or message are excluded) - private and secret Key export involving the CA, CSA, RA and CMS's Cryptomodules take place in accordance with the principles of Separation of Duties/Multi-party Control stated in Section 5.2. An auditable log is maintained, which records the action taken, date and time the action was taken, and name of person who performed the action.	X	X	X	X	X
11	**CERTIFICATE REGISTRATION**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
11.a	All Certificate requests – All Certificate requests including: date and time of request, type of event, and request information automatically logged by the application. This includes initial application, Issuance, Renewal, and Re-Key requests as well as sender/requester DN, Certificate serial number, date and time of response and success or failure indication are automatically logged by the application; manual interactions with PKI Participants such as telephone or in person inquiries and results of verification calls will be logged manually in a logbook or in a computer-based recording/tracking system and include date/time, description of interaction and identity provided.	X	X	-	X	X

Ref ID	Auditable Event	CA	CMS	CSA	RA	LRA
12	**CERTIFICATE REVOCATION**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
12.a	All Certificate Revocation requests – All Certificate Revocation requests including: Date and time of Revocation request, sender/requester DN, Certificate serial number, subjectDN of Certificate to Revoke, End Entity's common name, Revocation reason, date and time of response and success or failure indication are automatically logged by the application; manual interactions with requestors such as telephone or in person inquiries and requests for Revocation are logged manually in a logbook or in a computer-based recording/tracking system. The date/time, description of interaction and identity provided are also recorded.	X	X	-	X	X
13	**CERTIFICATE STATUS CHANGE APPROVAL**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
13.a	The approval or rejection of a Certificate status change request - identity of equipment operator who initiated the request, message contents, message source, destination, and success or failure indication are automatically logged by the application.	X	X	-	-	-
14	**COMPONENT CONFIGURATION**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
14.a	Any security-relevant changes to the configuration of a system component – date and time of modification, name of modifier, description of modification, build information (i.e. size, version number) of any modified files and the reason for modification are manually logged during change management process.	X	X	X	X	X
15	**ACCOUNT ADMINISTRATION**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
15.a	Roles and users are added or deleted – date and time, type of event, and identification of user making modification are logged automatically and manually. Changes roles are logged through a combination of automatic and manual logging. All changes are manually logged through change management procedures. Change management records capture date and time and type of change, reason for change of role, and authorization and approval records.	X	X	-	-	-
15.b	The Access Control privileges of a user account or a role are modified – date and time, type of event, and identification of user making modification are logged automatically and manually. Changes in configuration files, security profiles and administrator privileges are logged through a combination of automatic and manual logging. All changes are manually logged through change management procedures. Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	X	-	-	-

Ref ID	Auditable Event	CA	CMS	CSA	RA	LRA
16	**CERTIFICATE PROFILE MANAGEMENT**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
16.a	All changes to the Certificate profiles – Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	-	-	-	-
17	**CERTIFICATE STATUS AUTHORITY PROFILE MANAGEMENT**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
17.a	All changes to the Certificate status authority profile - Change management records capture date and time and type of change, reason for modification and authorization and approval records.	-	-	X	-	-
18	**REVOCATION PROFILE MANAGEMENT**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
18.a	All changes to the Revocation profile - Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	-	-	-	-
19	**CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
19.a	All changes to the Certificate Revocation list profile - Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	-	X	-	-
20	**MISCELLANEOUS**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
20.a	A message from any source received by the CA requesting an action related to the operational state of the CA – date of the message, source of the message, message request and message authorization are electronically and/or manually logged.	X	-	-	-	-
20.b	Appointment of an Individual to a Trusted Role – date of the appointment, name of the appointee and authorizing signature are manually logged.	X	X	X	X	X
20.c	Appointment of an Individual to a multi-person Role – date of the appointment, name of the appointee and authorizing signature are manually logged.	X	X	-	X	-
20.d	Installation of the Operating System -date and time of server installation, name of installer, and details of installation process are manually recorded during installation. The automatic security auditing capabilities of the underlying operating system hosting the software are enabled during installation. All changes are also manually logged through change management procedures.	X	X	X	X	X

Ref ID	Auditable Event	CA	CMS	CSA	RA	LRA
20.e	Installation of the PKI Application - date and time of installation, name of installer, and details of installation process are manually recorded during installation. All changes are also manually logged through change management procedures.	X	X	X	X	-
20.f	Installation of Cryptomodules - a manual list of Cryptomodules is maintained, and the list records action taken, date and time action was taken and name of person who performed action.	X	X	X	X	-
20.g	Removal of Cryptomodules -- a manual list of Cryptomodules is maintained, and the list records action taken, date and time action was taken and name of person who performed action.	X	X	X	X	-
20.h	Destruction of Cryptomodules -- a manual list of Cryptomodules is maintained, and the list records action taken, date and time action was taken and name of person who performed action.	X	X	X	X	-
20.i	System Startup – date and time of system startup is automatically logged in the system's event log	X	X	X	X	X
20.j	Logon attempts to PKI Application - CA, CSA, CMS and RA applications access – date and time of event, type of event, identity of user accessing the system, and success or failure indication are automatically logged by the application.	X	X	X	X	X
20.k	Receipt of hardware / software – kept manually in a database that records the hardware and software possessed, licensed or owned	X	X	X	X	X
20.l	Attempts to set passwords – date and time, identity of user, and success or failure indication of attempt to set password is kept automatically by the operating system/application or manually in a password change log	X	X	X	X	X
20.m	Attempts to modify passwords – date and time, identity of user, and success or failure indication of attempt to modify password is kept by the operating system/application or manually in a password change log	X	X	X	X	X
20.n	Back up of the internal CA database – date and time of the backup event and location of backup is kept manually in a backup log	X	X	-	-	-
20.o	Restoration from back up of the internal CA database – date and time of restoration tests is kept manually in a disaster recovery log	X	X	-	-	-

Ref ID	Auditable Event	CA	CMS	CSA	RA	LRA
20.p	File manipulation (e.g., creation, renaming, moving) – the file system records the identity of the local operator who created or last modified the file so that the creation, renaming or moving of files can be associated with the operator is kept automatically by the operating system audit and logging facility	X	-	-	-	-
20.q	Posting of any material to a repository – date and time of posting, transaction identifier and success or failure indication are automatically logged by the application. For CRL generation and publication to directory - date and time of generation, DN of Issuing CA and success or failure of publication of CRL is automatically logged by the application.	X	-	-	-	-
20.r	Access to the internal CA database -- date and time of login, username asserted at the time of attempted login, and success or failure indication, are automatically logged by the database audit log;	X	-	X	-	-
20.s	All Certificate compromise notification requests – date and time of notification, identity of person making the notification, identification of entity compromised, description of compromise are logged manually by the personnel who receive the notification (e.g. Help Desk, LRAs, etc.) and by RA/LRA/CMS enrollment application manager system processing logs	X	X	N/A	X	X
20.t	Loading Cryptomodules with Certificates -- an auditable log of all physical access to production Root CA, CAs, CSA, CMS and RA Cryptomodules is maintained, and the log records action taken, date and time action was taken and name of person who performed action.	X	X	X	X	-
20.u	Shipment of Cryptomodules – An auditable log is maintained including receipt, servicing (e.g. Keying or other cryptologic manipulations), and shipping of Cryptomodules for CA, CSA, CMS and RA production Cryptomodules. Recording contains information regarding action taken, (e.g. return, receipt), date and time action was taken, name of person performing action and reason for action.	X	X	X	X	-
20.v	Zeroizing Cryptomodules – An auditable log is maintained of Cryptomodules that includes action taken, date and time action was taken, name of person who performed action, name and role of person authorizing the action.	X	X	X	X	-

Ref ID	Auditable Event	CA	CMS	CSA	RA	LRA
20.w	Re-Key of the Component – CA, CSA, CMS and RA Systems automatically records all significant events related to their respective operations, including Key Generation for Re-Keying. Additionally, manual and audiovisual records of CA Key Generation are created. RA Re-Keying and Certificate generation events are also automatically recorded by the CA system.	X	X	X	X	-
21	**CONFIGURATION CHANGES**	**CA**	**CMS**	**CSA**	**RA**	**LRA**
21.a	Hardware - All changes are manually logged through change management procedures.	X	X	X	-	-
21.b	Software - All changes are manually logged through change management procedures.	X	X	X	X	X
21.c	Operating System - All changes are manually logged through change management procedures.	X	X	X	X	X
21.d	Patches - All changes are manually logged through change management procedures.	X	X	X	-	-
21.e	Security Profiles - All changes are manually logged through change management procedures.	X	X	X	X	X
22	PHYSICAL ACCESS / SITE SECURITY	CA	CMS	CSA	RA	LRA
22.a	Personnel Access to room housing component - a manual recording of physical access to secure rooms is maintained through physical logs that include recording of date and time, person accessing the secure room, and reason for access.	X	X	-	-	-
22.b	Access to a component - logged through a combination of automatic and manual logs based on the type of component and type of access.	X	X	X	-	-
22.c	Known or suspected violations of physical security - any known or suspected violations of physical security – date/time, description of suspected event, name of person reporting the event and resolution are manually logged by Security Team.	X	X	X	X	X
23	ANOMALIES	CA	CMS	CSA	RA	LRA
23.a	Software error conditions - date and time of event, and description of event are automatically logged by the application reporting the event or the operating system;	X	X	X	X	X
23.b	Software check integrity failures - date and time of event, and description of event are automatically logged by the application reporting the event or the operating system;	X	X	X	X	X

Ref ID	Auditable Event	CA	CMS	CSA	RA	LRA
23.c	Receipt of improper messages - date and time of event, and description of event are automatically logged by the application reporting the event or the operating system;	X	X	X	X	X
23.d	Misrouted messages - date and time of event, and description of event are automatically logged by the application reporting the event or the operating system;	X	X	X	X	X
23.e	Network attacks (suspected or confirmed) - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X	X	X
23.f	Equipment failure - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by System Administrator and reviewed by a Security Officer.	X	X	-	-	-
23.g	Electrical power outages - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	-	-	-
23.h	Uninterruptible Power Supply (UPS) failure - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	-	-	-
23.i	Obvious and significant network service or access failures - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	-	-	-
23.j	Violations of Certificate Policy - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X	X	X
23.k	Violations of Certification Practice Statement - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X	X	X
23.l	Resetting Operating System clock - date/time, description of suspected event, name of person are automatically logged by the operating systems logging facility.	X	X	X	X	X

5.4.2 Frequency of Processing Log

The IdenTrust Security Office and System Administrators continuously monitor log data, and conduct reviews of all the audit log data through a combination of automated and manual means at least once every calendar month. In order to ensure a thorough review of all data, the Security Officer selects a statistically relevant sample of CA, CSA and CMS logs for review and other security audit data generated since the last review for

each category of audit data. The Security Officer uses automated tools to scan logs for specific conditions. The Security Officer then reviews the output and produces a written summary of findings. The reviews include date, name of reviewer, description of event, details of findings and recommendations for remediation or further investigation if appropriate. The reviews include CA, CSA, CMS, RA and LRA activities that are listed as recorded in Section 5.4.1. These reviews are made available to IdenTrust's external auditor upon request.

External RA/LRAs are obligated by contract, this CPS and the IGC-CP to incorporate similar audit log processing procedures and to have the audit logs reviewed by an Individual not involved in performing RA functions that performs the Security Officer / Auditor role for the RA/LRA.

5.4.3 Retention Period for Audit Logs

Audit log information generated on CA, CSA, CMS, RA and LRA equipment is kept on the equipment until the information is moved to the offsite archive facility described in Section 5.1.8. The most recent 90 days of active logs remain on the equipment for analysis. The oldest 30 days, (e.g. logs dated between 90 and 120 days), will be removed monthly to be archived by the Security Officer in accordance with Section 5.4.4. Electronic audit logs are deleted only after they have been backed up to archive media. Only Security Officers are authorized to delete these logs and must first verify that the audit log data has been successfully backed up to archive media by checking hash values against the original and the backup copies.

External RA/LRAs are obligated by contract, this CPS and IGC-CP to incorporate similar audit log retention periods and procedures but in no case the retention period will be shorter than two months. RA/LRA are also obligated to provide that only the Individual performing the Security Officer / Auditor role for the RA/LRA authorize deletion of audit data.

5.4.4 Protection of Audit Logs

IdenTrust security audit logs are written simultaneously to three locations: to the host itself, to a separate log server with write/modify access restricted to Systems Administration personnel, and to a separate audit log server with write/modify access restricted to the Security Office. Modification of the security audit log is restricted through Access Controls and the operating system logging process. Storage capability is monitored by the operating system to ensure that sufficient space exists in order to prevent overflow conditions. Alerts are sent to IdenTrust Security Office if space available becomes inadequate. When logs are archived, the integrity of the archive data is ensured with the application of a checksum and a trusted third party time stamp prior to burning the log files to a read-only storage device (e.g., CD-ROM, DVD).

The Security Officer oversees procedures governing the archiving 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 and review summaries are archived monthly and moved to a secure offsite storage location identified in Section 5.1.8.

RAs and LRAs external to IdenTrust are obligated by contract, the IGC-CP and this CPS to: (1) keep the information generated by them on their equipment until it is moved to an appropriate archive facility; (2) have information deleted by an Individual other than the LRA; and (3) retain the data for at least two (2) months on-site. RAs and LRAs are also obligated to archive records in accordance with Section 5.5.

5.4.5 Audit Log Backup Procedures

Backup copies of the security audit logs and audit summary data are transferred to the secure offsite location in a locked metal storage container with no external markings identifying it as belonging to IdenTrust or describing the contents. Containers storing audit data are stored in an area within the storage facility that is separate from the daily backups, and access to the log data is restricted to Security Officers.

5.4.6 Audit Collection System (internal vs. external)

Automated audit log collection systems are internal to the CA, CSA, CMS, RA, LRA, and Repository. These systems invoke audit processes at system startup, which cease only at system shutdown. Processes are enforced technically through the operating system and a secondary monitoring application.

Should it become apparent that an automated security audit system has failed; operations of the affected system(s) will be taken offline until the security audit capability can be restored. If an initial review determines that Revocation processing and CSA services are unaffected, they will remain operable. IdenTrust incident response procedures will be used to determine the extent of the audit logging failure, to identify and remedy the cause, and to bring all systems back online as soon as this can be done in a secure manner.

In the event Participant CAs or External RAs operate RA Systems or a CMS external to IdenTrust, such Participant CAs or External RAs are obligated by contract, this CPS and the IGC-CP to incorporate similar procedures for ensuring the secure operation of the their respective audit data collection system.

5.4.7 Notification to Event-Causing Subject

No notice is provided to the event-causing PKI Participant that an event was audited.

5.4.8 Vulnerability Assessments

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

In addition, Security Officers conduct internal penetration tests quarterly, using industry-standard tools and methods. Annually, an external penetration test is performed by a qualified third-party vendor.

RAs and LRAs external to IdenTrust are obligated by contract, this CPS and the IGC-CP to ensure that the person filling the Security Officer role performs a security audit review of the audit data for events that indicate the presence of vulnerabilities in their systems. Such events include repeated failed actions, requests for privileged information, attempted access of system files, unauthenticated responses and lack of continuity in the security data.

5.5 Records Archive

5.5.1 Types of Events Archived

IdenTrust maintains and archives the following records, in either electronic or paper format. The use of electronic records is preferred, and paper records are digitized whenever possible.

Table – Type of Events Archived

Data To Be Archived	CA	CMS	CSA	RA	LRA
CA Accreditation (if applicable)	X	-	-	-	-
Certificate Policies	X	X	X	-	-
Certification Practice Statement	X	X	X	X	X
Contractual obligations	X	X	X	X	X
Other agreements concerning CA/CSA/CMS/RA operations	X	X	X	X	X

Data To Be Archived	CA	CMS	CSA	RA	LRA
System and equipment configuration	X	X	X	X	-
Modifications and updates to system or configuration	X	X	X	X	-
Certificate requests	As specified in Section 5.4.1 Ref ID 11.a				
Revocation requests	As specified in Section 5.4.1 Ref ID 12.a				
Subscriber identity authentication data (per Section 3.2)	X	-	-	X	X
Documentation of receipt and Acceptance of Certificates	X	-	-	X	X
Subscriber Agreements	X	-	-	X	X
Documentation of receipt of Subscriber's Cryptomodule or Cryptomodule (for non-human Subscriber)	-	-	-	X	X
Documentation of receipt of Cryptomodules (CA/CSA/CMS/RA)	X	X	X	X	-
All Certificates that are Issued or published	X	-	-	-	X
Record of Re-Key (of PKI Participant's Cryptomodule)	X	X	X	X	X
All CRLs Issued and/or published	X	-	X	-	-
Other data or applications to verify archive contents	X	X	X	X	X
Compliance Auditor reports	X	X	X	X	X
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	As specified in Section 5.4.1 Ref ID 1.a				
Any attempt to delete or modify the Audit logs	As specified in Section 5.4.1 Ref ID 1.b				
Whenever the CA generates a key. (Not mandatory for single session or	As specified in Section 5.4.1 Ref ID 6.a				
All access to certificate subject private keys retained within the CA for key	As specified in Section 5.4.1 Ref ID 7.c				
All changes to the trusted public keys, including additions and deletions	As specified in Section 5.4.1 Ref ID 8.a				
The export of private and secret keys (keys used for a single session or	As specified in Section 5.4.1 Ref ID 10.a				
The approval or rejection of a certificate status change request	As specified in Section 5.4.1 Ref ID 13.a				
Appointment of an individual to a Trusted Role	As specified in Section 5.4.1 Ref ID 20.b				
Destruction of cryptographic modules	As specified in Section 5.4.1 Ref ID 20.h				
All certificate compromise notifications	As specified in Section 5.4.1 Ref ID 20.s				
Remedial action taken as a result of violations of physical security	X	X	X	X	-
Violations of Certificate Policy	As specified in Section 5.4.1 Ref ID 23.j				
Violations of Certification Practice Statement	As specified in Section 5.4.1 Ref ID 23.k				
OCSP Requests and Responses	-	-	-	-	-

5.5.2 Retention Period for Archive

Archive records are maintained locally for at least 90 days and archived offsite for at least ten years and six months in accordance with IdenTrust policies. The archives are maintained without any loss of data for the duration of the retention period. IdenTrust applies a checksum to its archive files and stores them on digital tape, CD-ROM or DVD, or similar medium to prevent alteration. Transferring from one storage medium to another medium will not invalidate the applied checksum; however, any attempt to modify the data will be

evident. Repository information is archived in a human readable form such as compressed Lightweight Directory Interchange Format. Paper records are archived in either their original format or as a document image. IdenTrust maintains copies of the applications that can read these types of files for at least the retention period.

IdenTrust's Security Officers oversee procedures governing the archiving of the audit log to ensure that archived data is protected from deletion or destruction during the data retention period. Data being maintained by IdenTrust such as Certificates or CRLs will be returned to a Participant CA at agreed upon terms, if necessary; or the data will be securely destroyed in accordance with IdenTrust's disposal procedures after ten years and six months.

RAs and LRAs external to IdenTrust are obligated by contract, the IGC-CP and this CPS to maintain define a mechanism to transfer archived data to new media in order to maintain for the length of the retention period. Applications to process archive data are also maintained for the same period.

5.5.3 Protection of Archive

Archived data is stored in a separate area of the offsite storage facility identified in Section 5.1.8. Records are uniquely identified. The contents of the archive will not be released as a whole, except as required by law, as described in Section 9.4. Access to the offsite storage facility is strictly limited to those Individuals authorized by IdenTrust Operations management. IdenTrust maintains a list of Individuals authorized to access the archive records and makes this list available to auditors upon request during compliance audits.

Certain sensitive materials are stored in a physically separate area within the offsite storage location, and access to the materials is limited to the IdenTrust Security Office.

In order to protect the integrity of electronic data, a checksum is applied to the archive files and they are stored on digital tape, CD-ROM, DVD, or similar medium to prevent alteration. The checksum is maintained and kept within the backup software program that applies the checksum. No transfer of medium will invalidate the applied checksum.

RAs and LRAs external to IdenTrust are obligated by contract, this CPS and the IGC-CP to protect the archive under the guidelines consistent with this CPS and the Policy.

5.5.4 Archive Backup Procedures

IdenTrust does not back up archives.

5.5.5 Requirements for Time-Stamping of Records

See Section 6.8.

5.5.6 Archive Collection System (internal or external)

Archive information is collected internally and stored externally as described in Section 5.4.6.

5.5.7 Procedures to Obtain and Verify Archive Information

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

Archive data is retrieved from secure storage using defined procedures for accessing archived material. Requested archive material is identified by inventory number, which was recorded for the materials when they were originally placed in the locked metal storage boxes for archival. The request procedure requires two IdenTrust Trusted Role employees who are previously authorized for this procedure. One such employee

requests the material, and the other provides management approval, using processes established in conjunction with the offsite facility.

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

5.6 Key Changeover

CA Signing Keys have the Validity Periods set forth in Section 6.3.2. To facilitate the transition when a CA (i.e., Root or Sub CA) Certificate is set to expire, the IdenTrust Key changeover process requires that the CA begin using a new CA Signing Key to sign newly Issued Certificates for a specific period of time prior to the expiration of the old CA Signing Key. The old CA Signing Key is retained to sign CRLs and OCSP Responder Certificates for the remaining years until the last Certificate Issued with the old CA Signing Key has expired. This is because the CA Certificate must still be valid so that all Certificates that are Issued with the old Key can be properly validated.

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. IdenTrust coordinates the lifecycles of its Root CA Keys/Certificate and Sub CA Keys and Sub CA Certificates by creating new CA Key Pairs and Certificates and ceasing to use expiring CA Signing Keys to sign Certificates prior to the end of their Validity Periods in order to minimize any adverse effects from CA Certificate expiration.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

IdenTrust maintains security incident response and compromise handling policies and procedures as well as disaster recovery and business continuity plans, both of which are approved by the IdenTrust CIO. Such procedures and plans are available for review on-site by external auditors upon request and by major customers who are under an appropriate nondisclosure agreement.

An initial goal of the incident response plan is to determine the degree and scope of the incident. This includes a determination of the cause or source of the incident (internal system failure or external malicious attack) and whether the immediate harm caused by the incident will be mild or severe. For all incidents, data is collected and analyzed to determine, among other things:

- Whether a crime has been committed, and if so, whether evidence can be collected that will be helpful to law enforcement;
- What data was disclosed or compromised, and whether there was a Key compromise; and
- What steps need to be taken immediately to mitigate further damage.

For anticipated threats, IdenTrust maintains step-by-step procedures, flow charts, and task assignments for members of the incident response team, depending on the type of incident that is believed to have occurred.

If it is determined that a CA's Private Key or the CMS has, or may have been, compromised, procedures described in Section 5.7.3 will be followed.

IdenTrust will immediately notify the CA and applicable PAAs of any such disaster or compromise informally via telephone call. This call will be followed formally by a Certificate-based communication if possible; otherwise, by a written letter sent via courier service. Events that will trigger this type of communication include:

- Suspected or detected compromise of the CA system;
- Physical or electronic attempts to penetrate the CA system;
- Denial of service attacks on a CA component;
- Any incident preventing the CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL; or
- A planned CA Certificate Revocation.

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

IdenTrust replicates its data in near real time to its disaster recovery site, and also performs tape backups daily, ensuring their data integrity with the controls explained in Section 5.5.3. Backup tapes and backups of Cryptomodules are stored offsite in a secure location. In the event of a disaster in which both principal and backup CA operations become inoperative, IdenTrust's CA operations will be re-initiated on appropriate hardware using backup copies of software, after their integrity is verified, and Cryptomodules.

Re-initiation will occur according to one of the following contingencies:

- If the CA Signature Keys are not destroyed, CA operation will be reestablished, giving priority to the ability to generate Certificate status information within the CRL Issuance schedule specified in Section 4.9.7.
- If the CA Signature Keys are destroyed, CA operation will be reestablished as quickly as possible, giving priority to the Generation of a new CA Key Pair and Certificate with new DN. The CA Certificate will be Revoked and notification will be placed on a CRL as specified in Section 4.9.3. New Subscriber Certificates will be Issued.

If the CA is the Root CA, Cross-certified CAs will be asked to Revoke the Certificates that are Issued to the Root CA, a new Root CA Key Pair and corresponding new self-signed Certificate with a new DN will be generated. Participant CAs and Cross-certified CAs will be asked to submit new Certificate requests. A new CRL will be Issued by the new Root. Subscribers will be notified and instructed via email and a secure IdenTrust or Participant CA's site (e.g., https://secure.identrust.com) how to remove the old Root CA from their Certificate store and install the new root in their Certificate store.

If the CA cannot Issue a CRL prior to the time specified in the next-update field of its currently valid CRL, then all CAs that have Issued Certificates to the CA will be notified informally via telephone call immediately. This call will be followed formally by a Certificate-based communication if possible; otherwise, by a written letter sent via courier service.

A CA will request Revocation of its Certificate if Revocation services are not reestablished within a reasonable period of time. The period of time will be established between the CA's representatives and the IdenTrust CIO and representatives from the IdenTrust's Risk Management Committee by analyzing the risk exposure at the time. However, the CA may request Revocation at any time. It is advisable, that this period does not exceed 18 hours after a Revocation has been requested of any Certificate Issued under the CA, or 72 hours after the last CRLs next update whichever occurs earlier.

When the Root CA is unable to Issue a CRL, the IdenTrust CIO and representatives from the IdenTrust's Risk Management Committee will establish the risk exposure and determine whether to stand up a new Root CA. If a CA has requested Revocation of its Certificate by the root, the risk exposure must be considered as high and within an 18 hour period after the Revocation has been requested, the procedures described in a prior paragraph in this Section are used to Revoke the old Root and to establish and promulgate the new Root.

5.7.3 Entity (CA) Private Key Compromise Procedures

Procedures pertaining to private Key compromise vary based on the type of key compromise identified. See

specific details in the following sub-sections.

5.7.3.1 Entity (CA) Private Key Compromise Procedures-CA Private Key

In the event that any CA Private Key has been or is suspected to have been compromised, the IdenTrust CIO will convene a meeting of management representatives (including representatives of the CA and RAs) to assess the situation and take appropriate action. IdenTrust personnel in Trusted Roles will implement the procedural steps and tasks that have been outlined for Key compromise in the Security Incident Response Plan, including:

- Quantifying the scope, extent and effects of the compromise;
- Revoking the compromised CA Certificate and ensuring that it is promptly included in a published Certificate Revocation List (CRL);
- Explaining the situation to all employees, and notifying all interested parties (either by Certificate-based communication, telephone or written letter sent by courier service). Recipients of this communication will include:
  - The IdenTrust PMA and the any cross-certified Bridge PAAs, if they have not already received notice;
  - Other IdenTrust Participant CAs;
  - All of RAs and LRAs; and
  - All Subscribers.

As soon as possible, the IdenTrust PMA will investigate the incident, and if necessary will forensically record and analyze the causes of the compromise.

A report will be prepared and delivered to the IdenTrust PMA concerning the causes of the compromise and the measures that have been or will be taken to prevent a future recurrence.

Assuming that the CA does not terminate operations (see Section 5.8) and that the factors leading up to the Key compromise can be satisfactorily addressed, IdenTrust will generate a new Key Pair and Sub-CA Certificate with a new DN, in accordance with its CA Key Generation ceremony procedures. The CA will Issue new Subscriber, RA System and LRA Certificates, upon completing identity verification processes outlined in Section 3.2, Signing them with the new Sub-CA Certificate, and will Issue a new, blank CRL.

Any .p7c, .cer, or other PKCS#7 files that contain or refer to the Certificate, Public Key or corresponding Private Key will be replaced with a new file to reflect that a new CA Certificate has been Issued. All appropriate HTTP and LDAP pointers will be updated to ensure proper path construction and validation.

5.7.3.2 Entity (CA) Private Key Compromise Procedures-Root CA Private Key

When Revocation of the Root Certificate is required, in addition to the foregoing procedures, IdenTrust will immediately notify the PAAs of all Bridges that are Cross-certified and request that the Cross Certificate Issued by the those Bridges be Revoked. A new Root CA Key Pair, self-signed Root CA Certificate with new DN, and CRL will be generated in a Key Generation ceremony consistent with the procedures of Section 6.1.1.

CAs and RAs are required by contract to facilitate the replacement of the Revoked Root CA Certificate with the new Root CA Certificate in Subscriber and Relying Party applications. IdenTrust will also notify PKI Participants that the new Root Certificate is available in a secure area of the IdenTrust website (HTTPS) where it can be downloaded in a Server-authenticated SSL/TLS-encrypted session. See Section 6.1.4 for additional detail on distribution of the Root CA.

Subordinated CAs and Cross-certified CAs will be asked to submit new Certificate requests.

IdenTrust will notify all interested parties via email, telephone or written letter sent by courier service. In addition, IdenTrust will set up an informational secure site (https://) that establishes a Server-side session

secured using one of its high assurance IdenTrust Root Certificates (e.g., DST Root CA X1 or DST Root CA X3), which are embedded in the most widely distributed commercial browsers.

Cross-Certification of the new Root CA with the Bridges will proceed in accordance with each specific PKI Cross Certification Process.

5.7.3.3 Entity (CA) Private Key Compromise Procedures-CSA Key

OCSP Responder Certificates are Issued with the nocheck extension (id-pkix-ocsp-nocheck) specifying that OCSP Responder Certificates are not checked by the Relying Party applications for the lifetime of the Certificate (30 days). If the CSA Signing Key has been or is suspected to have been compromised, then the IdenTrust CIO will convene a meeting of personnel involved in CSA operations to assess the degree and scope of the compromise. If it is determined that Private Keys were compromised, a new OCSP Responder Key Pair and Certificate will be immediately created (signed by the Sub CA) and installed in the OCSP Responder as soon as possible.

For any period of compromise, all signed validations for that period (during which the CSA Key was suspected to have been compromised) will be reviewed and either re-signed with a new Key, or may be handled by agreement with the Participants CAs involved in each affected transaction.

5.7.3.4 Entity (CA) Private Key Compromise Procedures-CMS Keys

In the event that a CMS Content Signing or the master Keys have been or are suspected to have been compromised, the IdenTrust CIO will convene a meeting of management representatives (including representatives of the CA, RAs and smart card vendor/bureau) to assess the situation and take appropriate action. IdenTrust personnel in Trusted Roles will implement the procedural steps and tasks that have been outlined for Key compromise in the Security Incident Response Plan, including:

- Quantifying the scope, extent and effects of the compromise;
- Suspending all Certificates that are Issued to the CMS if there is suspicion of compromise;
- Suspending end entity Certificates that are suspected of being Issued after the compromise;
- Revoking Certificates that are Issued to the CMS and end entities if there is confirmation of compromise;
- Suspension of the CMS operation;
- Notifying all interested parties (either by Certificate-based communication, telephone or written letter sent by courier service). Recipients of this communication will include:
  - IdenTrust, if they have not already received notice;
  - smart card vendor/bureau;
  - all of RAs and LRAs; and
  - all Subscribers affected.

As soon as possible, the IdenTrust PMA will investigate the incident, and if necessary will forensically record and analyze the causes of the compromise. A report will be prepared and delivered to the IdenTrust PMA concerning the causes of the compromise and what measures have been or will be taken to prevent a future recurrence.

If no compromise has been confirmed, all Certificates will be unsuspended in accordance with Section 4.9.16.

If compromise of the Content Signing Private Key has been confirmed, the CMS operator will generate a new Content Signing Key Pair and request a Certificate with a new DN, in accordance with original Key Generation procedures. If compromise of master Keys is confirmed, in collaboration with the smart card vendor, new master Keys will be generated and transferred to the CMS Operator. The CMS will Issue new smart cards and associated Certificates, upon completing identity verification processes outlined in Section 3.2.

5.7.3.5 Entity (CA) Private Key Compromise Procedures-RA System and LRA Private Keys

All RA Administrators and LRAs, including External RA Administrators and LRAs who are obligated by contract, this CPS and IGC-CP are required to immediately notify IdenTrust and request Revocation if they believe an RA System Private Key or an LRA's Private Key has been or is suspected to have been compromised. IdenTrust will Revoke the Certificate and the IdenTrust CIO and the Security Officer or an Authorizing Official for the RA will meet with the LRA or RA Administrator to assess and address the situation (including deciding to what extent Subscriber Certificates should be Revoked) and to take any other actions needed to identify and remedy the causes of the compromise so that they do not recur. These actions include, but are not limited to, Issuance of new RA System or LRA Certificates in accordance with this CPS, Renewal or reissuance of compromised Subscribers' Certificates. In cases where approved Subscribers Certificates cannot be ascertained as legitimate, the Certificates will be Revoked and the Subscribers notified of Revocation.

5.7.4 Business Continuity Capabilities After a Disaster

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

IdenTrust has implemented a completely redundant hardware configuration at its principal site, as well as having tertiary devices at the disaster recovery location for critical services including the repository and all components needed to perform validation and Revocation services. Updates to the repository information are written in near-real time to the disaster recovery site, providing a backup repository that is current to the last validated transaction. Validation and Revocation services can automatically switch from the primary location to the disaster recovery location using global load balancers to direct domain name services. In the event of a disaster in which the main CA operations are physically damaged or otherwise become inoperative, the disaster recovery facility is made aware of a problem at the primary location and these critical services are automatically redirected to the disaster recovery facility. This process typically takes less than a second. Backup copies of the CA's Signing Keys (see Section 6.2.4) will be used, if necessary, to restore CA services at the disaster recovery site. Priority will be given to reestablishing validation services and the ability to publish Revocation information. This ensures compliance with the necessary uptime requirements for the program.

IdenTrust maintains processes to facilitate drop-shipment of hardware to IdenTrust following a major incident. This allows IdenTrust to restore CA operations at the principal site or elsewhere as quickly as possible, and to avoid a single point of failure that could exist in the interim at the disaster recovery site. IdenTrust performs tape backups on a daily basis. Backup tapes and backup Cryptomodules are stored offsite in a secure location.

In the event of disaster whereby the CA at both principal and disaster recovery sites becomes inoperative, CA operations will be re-initiated on appropriate hardware using backup copies of software, backup data and backup Cryptomodules at a third site. Priority will be given to re-establishing validation services and ability to publish Revocation information.

In the event that the CA system cannot reestablish Revocation capabilities prior to the next update field in the latest CRL Issued, then IdenTrust will report this informally by phone call to interested PKI Participants as soon as reasonably possible. The call will be followed by a formal Certificate-based communication if possible; otherwise by a written letter or other reliable means of communication.

In the event of a disaster whereby all operations suffer total physical damage beyond disaster recovery or repair (including destruction or compromise of the backup CA Keys), or if it is otherwise determined that the CA Signing Key has been compromised, then the procedures of Section 5.7.3 will be implemented.

5.8 CA and RA Termination

In the event that it is necessary for IdenTrust, a CA, CMS or an RA to cease operation, all affected PKI Participants, including all Cross-certified Bridges, will be notified of the planned termination, promptly and as far in advance as is commercially reasonable. A termination plan must be submitted to the IdenTrust PMA by the terminating entity. The termination plan must propose methods of minimizing the disruption to the operations of PKI Participants caused by the planned termination and also include provisions for the following.

5.8.1 RA or CMS Termination

In the event of an RA or CMS termination the following steps will be taken:

- Archival of all audit logs and other records prior to termination;
- Delivery of current operating records to a responsible successor RA in the case of an RA termination, or to a successor CMS or the CA in the case of CMS termination, that will provide Certificate Revocation services for the remaining terms of Certificates and accept the assignment of any related, contracted-for support services. Note that 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 the Certificates approved by the RA, or smart cards Issued by a CMS, not need to be Revoked. However, in the case of RA termination, all RA System and LRA Certificates will be Revoked; in the case of CMS termination, the Content Signing Certificates will be Revoked;
- Refund of pro rata portions of Certificate fees and any payments for services that will not be delivered;
- Ensuring of the transfer to, and preservation of, archived records by a responsible RA successor in the case of an RA termination, or a responsible CMS successor or the Participant CA in the case of CMS termination, for the archive retention period specified in Section 5.5.2;
- Surrender and/or Zeroization of Cryptomodules containing Private Keys in accordance with Section 6.2.10 and Revocation of all Certificates, if necessary; and
- If a successor RA will be assuming responsibilities for existing customers, provisions for such transition, e.g. replacement Certificates, customer relations, etc.

5.8.2 CA Termination

In the case of a CA termination, all the steps above will occur, with these exceptions: (1) Revocation of all Certificates that are Issued under the CA will not be optional, (2) Revocation will be effected prior to revoking the CA Certificate, and (3) the nextUpdate in the CRL will be past the expiry date of all Certificates that are Issued by the CA. OCSP validation will not be available since its Certificate must be Revoked.

5.8.3 Root CA Termination

If the Root CA is terminated, prior to the event IdenTrust will notify all Subscribers via signed email about the termination, and will provide instructions on how to remove Trust Anchors representing the CA.

6 TECHNICAL SECURITY CONTROLS

When a FIPS 140-2 validated HSM or Cryptomodule is used, the module will be used in FIPS approved mode.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

All PKI Participants generate their own Keys instances where such is possible. Generation of CA, CSA, RA and CMS Key Pairs is performed using only devices evaluated to meet approved cryptographic standards published by the National Institute of Standards and Technology ("NIST") in Federal Information Processing Standards ("FIPS") Publication 140-2, Security Requirements for Cryptographic Modules.

6.1.1.1 CA Key Pair Generation

Refer to the following sub-sections for Key pair generation by type.

6.1.1.1.1 CA and CSA Key Pair Generation

CA and CSA Key Pairs are generated within Cryptomodules validated to FIPS 140-2 Level 3 or higher. Activation of all Cryptomodules require that they be connected to PED. The PED comes with Keys that are initialized with unique digital identifiers that are made specific to the Cryptomodule during the initialization process.

The CA and CSA Key generation ceremonies are performed in the IdenTrust secure room. The ceremony is scripted, video-recorded and witnessed. The ceremony is performed by personnel in Trusted Roles who use different Keys at the appropriate time depending on whether Key generation, Certificate generation or a Cryptomodule backup/cloning operation is being performed.

6.1.1.1.2 RA and CMS Key Pair Generation

RA and CMS Key Pairs are generated within Cryptomodules validated to FIPS 140-2 Level 2 or higher. The ceremony is performed in a secure room, scripted and witnessed by personnel in Trusted Roles. The CMS master Keys are Generated by the smart card issuer and securely transferred to the CA or RA. The Keys are encrypted and split into three parts for transport. The encrypted master Keys and the components of the transport Key are sent in tamper-evident envelops to Individuals in Trusted Roles via courier with tracking services. The master Key ceremony consists of decryption and injection of the master Keys into the HSM. The ceremony is performed by Individuals in Trusted Roles in the secure room and is scripted and witnessed.

IdenTrust may reset manufacturer CMS master Keys for cards delivered by IdenTrust to a Participant CA or External RA operating a CMS. In such cases, a PKI Consultant directly provides the master Keys in a secure manner to an Individual in a Trusted Role of the Participant CA or External RA for entry into the CMS.

Only the CMS with the correct master Keys can interact with the associated smart cards. During the card personalization process, diversified Keys that result from the combination of the smart card's serial number with the master Keys are injected in the smart cards. The diversified Keys are then used to allow and securely protect the operations between the CMS and the smart card when new objects are inserted in it.

6.1.1.1.3 PIV-I Content Signing Key Pair Generation

PIV-I Content Signing Key Generation ceremonies are performed in a secure room under Separation-of-Duties/Multi-party Control by personnel in Trusted Roles. The ceremony is scripted and witnessed.

6.1.1.2 Subscriber Key Pair Generation

Key pair generation varies based on the type of certificate issued. See sub-sections below for specific processes.

For all IGC Certificates where encryption Keys are escrowed, the CA, CMS or RA System generates the Encryption Key Pair in an attached FIPS PUB 140-2 Level 3 HSM and securely injects the Keys into the Subscriber Cryptomodule.

6.1.1.2.1 Subscriber Non-PIV-I Certificates Key Pair Generation

Subscribers, including LRAs, RA Administrators and TAs are all issued Subscriber Certificates.

For non-PIV-I Certificates, Key Pair Generation may be performed by the Applicant, Subscriber, CA, or RA for all IGC certificate Assurance Levels. Hardware Cryptomodules provided to Subscribers are configured to disallow export of Private Keys.

Whenever possible, Key Pair Generation is performed by the Subscriber within the Cryptomodule in which the Keys are stored. If the CA, CMS or RA System generates Subscriber Key Pairs, Key Pair delivery meets the requirements specified in Section 6.1.2.

Medium Hardware Signing Certificate Private Keys are generated by the Subscriber in the hardware Cryptomodules in which they are stored or by the CMS or RA System. When Key Pairs are generated by the CMS/RA System, they are generated in hardware Cryptomodules validated to FIPS PUB 140-2 Level 2 or higher and injected into the Subscriber hardware Cryptomodule. Subscriber Hardware Cryptomodules are validated to FIPS PUB 140-2 Level 2 or higher. Hardware Cryptomodules provided to Subscribers for Medium Hardware Certificates are configured to not allow export of Private Keys.

Basic and Medium Software Certificate Signing Key Pairs are generated by the Subscriber in the hardware or software Cryptomodules in which they are stored, by the CMS or by the RA System. When Key Pairs are generated by the Subscriber in software Cryptomodules, such Cryptomodules must be validated to FIPS PUB 140-2 Level 1 or higher. When Key Pairs are generated by the CMS/RA System, they are generated in hardware Cryptomodules validated to FIPS PUB 140-2 Level 2 or higher and injected into only hardware Subscriber Cryptomodules validated to FIPS PUB 140-2 Level 2 or higher. Hardware Cryptomodules provided to Subscribers for IGC Basic or Medium Software Certificates are configured to not allow export of Private Keys.

6.1.1.2.2 Subscriber PIV-I Certificates Key Pair Generation

For PIV-I Hardware Certificates, only PIV-compatible smart cards from the FIPS PUB 201 APL are utilized, ensuring the hardware Cryptomodules are validated to FIPS PUB 140-2 Level 2 or higher. Hardware Cryptomodules provided to Subscribers for PIV-I Certificates are configured to not allow export of Private Keys. The CMS ensures the Validity Period of these Certificates do not extend beyond the expiration date of the smart card.

PIV-I Card Authentication Certificate Private Keys and symmetric Card Authentication Keys are generated within the FIPS PUB 140-2 Level 2 or higher FIPS 201 APL PIV-compatible smart card, or generated by the CMS in hardware Cryptomodules validated to FIPS PUB 140-2 Level 2 or higher and injected into the PIV-compatible card. Private Key operations are performed using these Keys without card activation (e.g., the PIN need not be supplied for operations with these Keys).

6.1.1.2.3 Device Key Pair Generation

Devices are required to generate Keys in Cryptomodules meeting the storage requirements for the Certificate type requested:

- IGC Device Medium Software - FIPS PUB 140-2 Level 1 or higher.
- IGC Device Medium Hardware - FIPS PUB 140-2 Level 2 or higher.

Hardware Cryptomodules provided to Subscribers are configured to not allow export of Private Keys.

Subscribers are notified of their obligation and are required by Subscriber Agreement to protect all Private Keys and passwords or PINs required to gain access to them. Subscribers are notified of their obligation to ensure Private Keys never exist in plain text outside of the Cryptomodule in which they were generated.

6.1.2 Private Key Delivery to Subscriber

Where possible, Subscribers generate their own Key Pairs for Signing Certificates and non-escrowed Encryption Certificates. In all other cases, LRAs generate a Subscriber's Keys in the PIN-Protected-Cryptomodule process explained in Section 4.3.1.2. IdenTrust, the CA or RA creates and delivers Key Pairs for all encryption Certificates where Keys are escrowed.

Hardware Cryptomodules provided to Subscribers are configured to not allow export of Private Keys.

Subscribers are notified of their obligation and are required by Subscriber Agreement to protect all Private Keys and passwords or PINs required to gain access to them. Subscribers are notified of their obligation to ensure Private Keys never exist in plain text outside of the Cryptomodule in which they were generated.

The process of delivering Private Keys to Subscribers varies depending on the type of certificate and whether or not the Encryption Key is escrowed. Refer to the following sub-sections for specific details.

6.1.2.1 Signing Private Key Delivery to Subscribers

Signing Private Keys and non-escrowed Encryption Keys are generated within the boundaries of FIPS PUB 140-2 evaluated hardware or software Cryptomodules as described above in Section 6.1.1. If the Subscriber's Cryptomodule generates the Keys, then there is no need to deliver the Private Key.

If the Private Keys are not generated by the Subscriber, accountability for the location and state of the containing hardware Cryptomodule is maintained until delivery and possession occurs. The process used to generate the Keys and protect the Private Key(s) from activation, compromise, or modification until possession occurs is described in Section 4.3.1.2, PIN-Protected-Cryptomodule process. During this process, the Key Pair is generated in an HSM in a secured area of the RA facility, and the Subscriber Cryptomodule is protected by a randomly generated PIN that is sent to the Subscriber in a channel that is separate from the delivery of the Cryptomodule.

6.1.2.2 Encryption Private Key Delivery to Subscriber

For generation of Encryption Keys, three methods are available:

6.1.2.2.1 IdenTrust Generation

- Immediately after the encryption Keys are generated, they are encrypted with a Public Key of an administrative Certificate and stored in the escrow database. The Administrative Certificate is a self-signed 2,048-bit Key Certificate. The administrative Private Key is held on a FIPS PUB 140-2 level 2 validated Cryptomodule.
- During the Server-Authenticated SSL/TLS session also discussed above in Sections 4.1.2 and 4.3.1, the system assembles and downloads a PKCS#12 and its protecting 20-digit, randomly generated PKCS#12 password.
- If the Subscriber is retrieving the Certificate to a hardware Cryptomodule, the PKCS#12 is downloaded into hidden fields in a non-cached web page. Then, a client-side component (e.g., ActiveX control, Java Applet) invokes the Cryptomodule's PKCS#12 import function and inserts the Certificate and encryption Private Key into the Cryptomodule, which has been previously activated by the Subscriber to allow the Generation of the Signing Certificate and Private Signing Keys.

- Keys generated for Certificates asserting an Assurance Level of PIV-I Hardware are encapsulated into PKCS#12/P12 password pairs for transport between the CA and CMS over an encrypted XSMS protocol. Then, the CMS builds a Secure Channel with the smart card using the master Keys, which channel is used to transfer and inject the Certificates and Private Keys into the smart card.
- Under some circumstances, PIV class cards are used for Certificates other than IGC PIV-I Certificates. In these cases, the Certificates are encapsulated into PKCS#12/P12 password pairs for transport between the CA and a card issuance system over an encrypted XSMS protocol, similar to how PIV-I Certificates are delivered through a CMS. The card issuance system builds a Secure Channel with the smart card using the master Keys, which channel is used to transfer and inject the Certificates and Private Keys into the smart card.
- If the PKCS#12 belongs to a Certificate delivered to a software Cryptomodule, both the file and its protecting password are made available to the Subscriber over a secured session and instructions on how to import the Encryption Certificate and Key to the software Cryptomodule are provided.

6.1.2.2.2 CMS Generation:

In this model, IdenTrust as the CA operator never has possession of or access to the Subscriber Encryption Private Key unless IdenTrust is also the operator of the CMS. The CA securely escrows only the symmetric Escrow Wrap Key associated with a given Encryption Key Pair.

- The CMS causes the Encryption Key Pair to be generated within an attached HSM validated to FIPS 140-2 level 3. Additionally, a symmetric Escrow Wrap Key ("EWK") is generated within the HSM;
- The CMS extracts the Encryption Key Pair and cryptographically wraps (encrypts) the Key Pair utilizing EWK;
- The CMS stores the encrypted Key Pair locally;
- The CMS transports the EWK to the CA for escrow with the corresponding PKCS#10 Certificate request; and
- The CMS destroys the local instance of the EWK.

Key recovery through the CMS requires recovery of the wrapped Encryption Key Pair stored local to the CMS and obtaining the EWK from the CA, ensuring Multi-Party control for any key recovery process.

6.1.2.2.3 Subscriber Generation:

When the encryption Private Key and Certificate are not escrowed, the system allows the Subscriber to generate all Private Keys in the same way Signature Keys are generated.

6.1.2.3 Private Key Delivery for CA, CSA, CMS, IGC PIV-I Content Signing and RA System

CA and CSA Private Keys remain under IdenTrust's control during the lifetime of the Keys. For CMS and RA Systems operated by IdenTrust, CMS, Content Signing and RA System Private Keys remain under IdenTrust's control during the lifetime of the Keys.

Participant CAs and External RAs that operate a CMS or RA System are required to maintain strict control over CMS, PIV-I Content Signing and RA System Private Keys.

The RA Administrator, LRA and TA Keys are Subscriber Keys and are under Subscriber control as explained earlier in this Section.

6.1.3 Public Key Delivery to Certificate Issuer

Delivery of Public Keys may vary based on the type of certificates. See sub-sections below for specific details.

6.1.3.1 Subscriber Public Key Delivery to Certificate Issuer

The Subscriber's Public Key is delivered to the CMS, RA or CA in a secure and trustworthy manner. The delivery of the Public Key, in a PKCS#10 structure, binds the Private and Public Keys and is submitted to the CA during a Server-authenticated SSL/TLS-Encrypted Session that is secured with a valid SSL Certificate that chains to one of IdenTrust's Root Certificates. In addition to the PIN-Protected-Cryptomodule-Process discussed in the previous Section (and in Section 4.3.1.2), two other methods are used to bind the confirmed identity to the Public Key:

1) During the registration phase outlined in Sections 4.3.1.3 and 4.3.1.4, the Applicant's information, PKCS#10, and hash of the Applicant-provided Account Password are bound together via the Server-Authenticated SSL/TLS-Encrypted transmission to the CA. Only the Applicant knows the Account Password because only the Account Password hash is stored. After identity confirmation, the LRA provides one or more Activation Codes to the Applicant through confirmed OOB channels. The secret Account Password and Activation Code(s) are used in combination by the Applicant to retrieve the Certificate during a subsequent Server-Authenticated SSL/TLS-Encrypted Session.
2) During the registration process, an LRA enrolls the Applicant and approves Issuance of a Certificate to the Subscriber. Activation Code(s) is/are generated and sent OOB to the Applicant to a confirmed destination. The Applicant uses the Activation Code(s) in a Server-Authenticated SSL/TLS-Encrypted Session during which the Public Key is submitted to the RA/CA in a PKCS#10 and a Certificate is returned back during the same session (see Section 4.3.1.1 and Section 4.3.1.3).

Public Keys generated for Certificates asserting an Assurance Level of PIV-I Hardware are encapsulated on a PKCS#10 and transferred between the smart card and the CMS over the Secure Channel created using the master Keys. Then, the CMS builds a request message and transfers the PCKS#10 to the CA over XSMS.

6.1.3.2 RA Public Key Delivery to Certificate Issuer

For RAs (RA Administrators, LRAs, TAs and RA System), Public Keys are submitted using any of the methods used by standard Subscribers. LRAs are Issued Subscriber Certificates. For RA and CMS Systems, 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.

6.1.3.3 CA Public Key Delivery to Certificate Issuer

All CA Public Keys are created within the confines of the CA system and are delivered directly to the Root CA for creation of the Sub CA Certificate. Manual means, which are documented in the Key Generation ceremony script, ensure that the Public Keys are bound to the correct subject.

6.1.3.4 CA Cross Certification Public Key Delivery to Certificate Issuer

Public Keys for Cross-Certification are delivered and exchanged between the IdenTrust and the Cross-Certifying Bridges as defined herein unless otherwise agreed in other contractual documents required by the Bridges.

1) The identity and authority of persons submitting the Other's PKI Public Key to be Cross-certified will be documented in accordance with Section 3.2.2 (Authentication of Organization Identity for the Bridge's Representatives) and include a facsimile of the manual signature and email address of the authorized Individual who is responsible for delivering the Public Key.

2) The Public Key shall be delivered to IdenTrust in a base64-encoded PKCS#10 via a mutually acceptable secure method, such as via an authenticated session on a secure FTP server, on a CD-ROM or flash memory device sent via USPS/commercial courier, or by hand delivery in-person by an authorized representative of the Bridge.
    a) If by Mail or Courier. The base64-encoded PKCS#10 may also be sent to IdenTrust on a CD-ROM or flash memory device via USPS or courier in a tamper-evident envelope. The envelope shall also contain the SHA-256 hash of the Bridge's Public Key to be signed and a printed version of the Bridge's base64-encoded PKCS#10

To confirm the binding between the Bridge's CA with the Bridge's Key Pair, IdenTrust's CA Administrator reviews the PKCS#10 and cryptographically compares it against the Bridge's CA Public Key.

6.1.4 CA Public Key Delivery to Relying Parties

IdenTrust ensures that Subscribers and Relying Parties receive and maintain the IGC Root CA (Trust Anchor) and IGC Sub CA Public Keys in a trustworthy fashion. Additionally, PKI Service Providers are required by contract to ensure Subscribers and Relying Parties receive and maintain the IGC Root CA (Trust Anchor) and IGC Sub CA Public Keys in a trustworthy fashion, if involved in delivery of CA Public Keys. Public Keys for CAs are contained within CA Certificates. Methods for delivery of CA Certificates include:

1) CA Certificates may be delivered to Subscribers during the Certificate retrieval process for their own Subscriber Certificates during the Server-Authenticated SSL/TLS-Encrypted Session as part of a message formatted in accordance with PKCS#7. When a CMS intermediates the retrieval process, the delivery of the Public Keys may occur through the Secure Channel created between the CMS and the smart card using the master Keys associated to the CMS.
2) Relying Parties may obtain CA Certificates from IdenTrust's secure web site. An email or other communication may be sent to PKI Participants directing them to download the CA Certificate at an https:// website secured with a valid SSL Certificate that chains to one of IdenTrust's Root Certificates. Alternatively, Subscribers and Relying Parties may be directed to an http:// website that is not secured in which case, IdenTrust will provide the hash or fingerprint via authenticated OOB sources (i.e., IdenTrust help desk phone support).
3) In cases where the External RA manages the insertion of CA Certificates into the Cryptomodule, IdenTrust provides the CA Certificates securely to the RA using an IdenTrust PKI Consultant during initial system setup. Once delivered, the RA is obligated by contract, the IGC-CP and this CPS to ensure the Subscriber receives the CA Certificates in a trustworthy fashion.
4) PKI Participants relying on CA Public Keys may deploy CA Certificates through enterprise-wide patch management, system maintenance utilities, directory services and active directories.

6.1.5 Key Sizes

Requirements for Key sizes may vary based on the Certificate to which the Keys are associated. See sub-sections below for specific details.

6.1.5.1 Key Sizes For Subscriber and Device

All end entity (Subscriber or Device) Certificates contain Public Keys that are at minimum 2048 bits for RSA or 224 bits for elliptic curve algorithms. End entity Certificates that expire after 12/31/2030 will contain Public Keys that are at minimum 3072 bits for RSA or 256 bits for elliptic curve algorithms.

6.1.5.2 Key Sizes For Subordinate CAs

Subordinate CAs that generate Certificates and CRLs Sign with Keys that are at least 2048 bits for RSA, or 224 bits for Elliptic Curve Digital Signature Algorithm (ECDSA). All Certificates that expire after 12/31/2030 will

be signed with Keys that are at least 3072 bits for RSA or 256 bits for ECDSA. At minimum, a SHA-256 hash algorithm is used when generating Digital Signatures. CSSs that Sign OCSP Responses do so using the same signature algorithm, Key size, and hash algorithm used by the CA to sign CRLs.

6.1.5.3 Key Sizes For CAs

For the IdenTrust Global Common Root CA, the subject Public and Private Signature Keys are 4096 bit modulus RSA.

6.1.5.4 Key Sizes For TLS or Other Protocols

TLS or other protocols providing similar security to accomplish any of the requirements of this CPS use a minimum of 128-bit AES for the symmetric Key, and at least 2048-bit RSA or equivalent for the asymmetric Keys. After December 31, 2030, these protocols will be configured to use at least 3072-bit RSA or equivalent for asymmetric Keys.

6.1.6 Public Key Parameters Generation and Quality Checking

Cryptomodules and associated software platforms used by CAs, the CSA, CMS, and Subscribers and RAs have been validated as conforming to FIPS 186-2, and provide random number generation and on-board creation of 2048-bit Key lengths for RSA Public Key Generation.

IdenTrust will use Cryptomodules conforming to FIPS 186-3 as vendors make products available.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

The specific Usage of a Key is determined by the key usage extension in the X.509 Certificate. Certificate key usage fields are used in accordance with RFC 5280.

Public Keys that are bound into Certificates assert digitalSignature or keyEncipherment, but not both. With the exception of Device Certificates, "dual use" Certificates asserting both digitalSignature and keyEncipherment are not be Issued by CAs operating under this CP. Certificate key usage is fully defined in IGC Profiles and may include additional extensions and additional key usages or extended key usages not indicated below. Subscribers and Relying Parties are advised to refer to IGC Profiles or the extensions of Issued IGC Certificates for all Certificate key usage purposes.

Key Usage purposes vary based on the type of certificate to which they are associated. See sub-sections below for specific details.

6.1.7.1 Key Usage Purposes for Signing Certificates

The following key usage values are present in the Individual Subscriber Signing Certificates: (i) digitalSignature; and (ii) non-Repudiation, which will be marked as critical.

For End Entity certificates issued after June 30, 2019, the Extended Key Usage extension is always be present and does not contain anyExtendedKeyUsage {2.5.29.37.0}.

For further details see IGC Profiles which address Subscriber Certificate profiles.

6.1.7.2 Key Usage Purposes for Encryption Certificates

The following key usage values are present in the Individual Subscriber Encryption Certificates: (1) KeyEncipherment, which will be marked as critical.

For End Entity certificates issued after June 30, 2019, the Extended Key Usage extension is always be present and does not contain anyExtendedKeyUsage {2.5.29.37.0}.

For further details see IGC Certificate Profiles which address Subscriber Certificate profiles.

6.1.7.3 Key Usage Purposes for DirectTrust Signing and Encryption Certificates

All Subscriber (end-entity) certificates that include a DirectTrust Policy OID and are non-CA certificates assert Basic Constraints as a Critical Extension and must assert a value of CA=False.

For End Entity certificates issued after June 30, 2019, the Extended Key Usage extension is always be present and does not contain anyExtendedKeyUsage {2.5.29.37.0}.

For further details, see IGC Certificate Profiles which address DirectTrust Subscriber Certificates in profiles that are separate from standard IGC Subscriber Certificate profiles.

6.1.7.4 Key Usage Purposes for Group Certificates

A Group Certificate asserts digitalSignature or keyEncipherment, but not both on the same Certificate. A Group Certificate does not assert non-Repudiation.

For End Entity certificates issued after June 30, 2019, the Extended Key Usage extension is always be present and does not contain anyExtendedKeyUsage {2.5.29.37.0}.

6.1.7.5 Key Usage Purposes for CA Certificates

All CA Private Signature Keys are used only to sign Certificates and CRLs.

The following key usage value is present in the CA Certificates: (1) cRLSign; and (2) KeyCertSign.

For further details about the key usage fields in CA Certificates, see IGC Certificate Profiles which address CA Certificate profiles.

6.1.7.6 Key Usage Purposes for RA System Certificates

RA System Certificates are Device Certificates. The following key usage values are present in the Device Signing Certificates: (1) digitalSignature; and (2) KeyEncipherment, which is marked as critical.

For further details see IGC Certificate Profiles which address Device Certificate profiles.

6.1.7.7 Key Usage Purposes for Content Signing Certificates

IGC PIV-I Content Signing Certificates contain a key usage value of digitalSignature, which is marked as critical. Additionally, IGC PIV-I Content Signing Certificates include an Extended key usage of id-fpki-pivi-content-signing, which is marked as critical.

For further details see IGC Certificate Profiles which address Content Signing Certificate profiles.

6.1.7.8 Key Usage Purposes for OCSP Responder Certificates

The following key usage values are present in the OCSP Responder Certificates: (1) digitalSignature; and (2) nonRepudiation, which are marked as critical.

For further details see IGC Certificate Profiles which address OCSP Responder profiles.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

All Cryptomodules used within the IdenTrust PKI are validated to the appropriate FIPS PUB 140-2 security level as identified in this Section.

- RA Administrators and LRAs are required to use hardware Cryptomodules validated to FIPS PUB 140-2 Level 2 or higher. When obtaining IGC Hardware or IGC PIV-I Hardware Certificates, Subscribers are required to use hardware Cryptomodules validated to FIPS PUB 140-2 Level 2 or higher.

- IGC Software Certificate Subscribers are required to use software or hardware Cryptomodules validated to FIPS PUB 140-2 Level 1 or higher.
- For Custodian Key Stores for Rudimentary Assurance Certificates must be validated to FIPS 140 Level 1 (Hardware or Software) and for Custodian Key Stores for Certificates with all other Assurance levels must be validated to FIPS 140 Level 2 or higher hardware KSMs.
- IGC PIV-I Content Signing Keys and RA System Keys are generated and stored in Cryptomodules validated to FIPS PUB 140-2 Level 2 or higher.
- All CA Keys are generated and stored in HSMs validated to FIPS PUB 140-2 Level 3 or higher.
- All CSA Keys are generated and stored in HSMs validated to FIPS PUB 140-2 Level 3 or higher.
- CMS master Keys are generated and stored in HSMs validated to FIPS PUB 140-2 Level 3 or higher.

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location. The Custodial Subscriber Key Store must be implemented by the Custodial Organization in such a way as to prevent any Custodial entity from accessing the Subscriber Private Keys and to prevent any other Subscriber from accessing the Private Keys of another Subscriber.

6.2.2 Private Key Multi-Person Control

The CA, CSA, CMS, RA system and PIV-I Content Signing Private Keys are stored in the secure room under Separation-of-Duties/Multi-party Control as discussed in Sections 5.1.2.1, 6.1.1 and 6.2.8.

For purposes of disaster recovery, backups of CA, CSA, RA system and CMS, and PIV-I Content Signing Private Keys are made under Separation-of-Duties/Multi-party Control (see Section 6.2.4.1) and are stored in the secure room and in a secure offsite facility where Separation-of-Duties/Multi-party Control are implemented as explained in Sections 5.1.6, 5.1.8, 5.2.2, and 5.7.4.

This Separation-of-Duties/Multi-party Control prevents a single Individual from gaining access to CA, CSA, CMS, RA system or PIV-I Content Signing Private Keys.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of FBCA and Entity CA Private Signature Key

Entity CA signature keys that are used to sign certificates or CRLS by the Entity CA are not escrowed by the FBCA; therefore these keys are not recoverable through the FBCA.

6.2.3.2 Escrow of CA Encryption Keys

No stipulations for Entity CAs.

6.2.3.3 Escrow of Subscriber Private Signature Keys

Private Keys of Subscriber encryption certificates may be escrowed in accordance with Section 4.12.1. RAs are prohibited from escrowing the Private Keys of Certificates asserting key usages of nonRepudiation or digitalSignature.

6.2.3.4 Escrow of Subscriber Private Encryption and Dual Use Keys

Except for Device certificates, IdenTrust issues only single-use certificates under the IGC policy. Dual use certificates issued to humans, are not issued under the IGC policy; therefore key escrow is allowed for Subscriber private encryption keys in accordance with Section 4.12.1. Subscriber signing keys are never escrowed.

6.2.4 Private Key Backup

6.2.4.1 Backup of FBCA and Entity CA Private Signature Key

FBCA is responsible for back up of FBCA private signature keys.

CA Private Signature Keys are backed up and stored under the same security precautions and multi-person control as the original CA Private Signature Key on cloned Cryptomodules in order to obviate the need to Re-Key in the case of hardware failure or disaster. No entity other than IdenTrust is allowed to backup or archive CA Private Signature Keys.

Two copies of the Root CA are created in separate Cryptomodules. Two copies of all other CAs are created in a shared Cryptomodule. All backup Cryptomodules are FIPS PUB 140-2 Level 3 or higher.

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

IdenTrust stores the Root CA and all other CA Private Keys and one of the copies in the secure room. The second backup of the Root CA and all other CAs Private Signature Keys are kept in a secure offsite facility.

When the Root CA and all other CAs Keys are no longer needed, the Cryptomodule containing them is Zeroized in accordance with Section 6.2.10.

6.2.4.2 Backup of Subscriber Private Signature Keys

Backup of Private Keys of RA system Certificates by the RA is permitted only to facilitate disaster recovery. Such Private Keys shall be backed up under the same multi-person control as used to generate the original Private Key, as described in Section 5.2.2 and shall undergo audit(s) in accordance with Section 8 of this CPS.

Private Keys of Signing Certificates delivered to hardware Cryptomodules are not backed up. The hardware Cryptomodules are configured to not allow export of Private Keys.

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

6.2.4.3 Backup of Subscriber Key Management Private Keys

Subscribers of Encryption Certificates delivered to hardware cryptomodules are not able to backup Private Keys, as they are not exportable from the hardware Cryptomodule. Issuing CAs may escrow Encryption Private Keys for recovery purposes as described in Section 4.12.

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

6.2.4.4 Backup of CSA Private Key

CSA is also referenced as CSS in this document and the terms can be considered as interchangeable. CSA Private Signature Keys are backed up and stored under the same security precautions and multi-person control as the original CSA Signature Private Key on cloned HSMs to obviate the need to Re-Key in the case of hardware failure or disaster. No entity other than IdenTrust is allowed to backup or archive CSA Private Signature Keys. Two copies of all CSAs are created in a shared HSM. All backup Cryptomodules are evaluated

to FIPS PUB 140-2 Level 3 or higher.

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

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

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

6.2.4.5 Backup of IGC PIV-I Content Signing Key

IGC PIV-I Content Signing Private Signature Keys are backed up and stored under the same security precautions and Separation-of-Duties/Multi-party Control as for generation of the IGC PIV-I Content Signing Private Signature Key.

One backup copy of IGC PIV-I Content Private Signature Key is kept in the secure room. A second backup copy is kept in a secure offsite facility.

When the IGC PIV-I Content Private Signature Key is no longer needed, the HSM containing them is Zeroized in accordance with Section 6.2.10.

6.2.4.6 Backup of Device Private Keys

Private Keys of Device Certificates may be backed up or copied, but must be held under the control of the Primary Machine Operator of the Device. Backed up Private Keys shall not exist in plain text outside the Cryptomodule. Storage must ensure security controls consistent with the protection provided by the original Cryptomodule in which Keys were generated.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The process for Private Key transfer may vary based on the type of certificate to which the Private Key is associated. See the following sub-sections for specific details.

6.2.6.1 Subscriber Private Key Transfer Into or From a Cryptographic Module

Private Keys of Certificates delivered to hardware Cryptomodules are generated and required to be kept inside of hardware Cryptomodules evaluated to FIPS PUB 140-2 Level 2 or higher. LRAs and Subscribers are notified of their obligation not to transfer the Private Keys from the Cryptomodule in which they were generated.

Private Keys of Certificates delivered to software Cryptomodules are generated in a Cryptomodule evaluated to FIPS PUB 140-2 Level 1or higher. Such Private Keys may be transported to another Cryptomodule, provided it is evaluated to FIPS PUB 140-2 Level 1 or higher. During transport, Private Keys must remain under the control of the Subscriber and never exist in plain text outside of the Cryptomodule boundary. Private or symmetric Keys used to encrypt other Private Keys for transport must be protected from disclosure. Subscribers are notified of their obligation to protect Private Keys during transport and to only utilize Cryptomodules evaluated to FIPS PUB 140-2 Level 1 or higher.

6.2.6.2 CA, CSA, CMS and PIV-I Private Key Transfer Into or From a Cryptographic Module

CA, CSA, RA and CMS Private Keys are generated and kept inside HSMs evaluated at FIPS PUB 140-2 Level 3 or higher. Where such Keys must be transferred to other media for backup and disaster recovery purposes, they are transferred in encrypted form. CA, CSA, RA and CMS Private Keys are backed up in accordance with controls described in Section 6.2.4.1. For backup purposes, a clone of the HSM is made using the PED key, and the cloning process ensures that the Private Keys never appear in plain text outside of the HSM.

6.2.7 Private Key Storage on Cryptographic Module

Procedures for Private Key storage on a Cryptographic Module may vary based on the type of Certificate to which the Private Keys are associated. See sub-sections below for specific details.

6.2.7.1 Subscriber Private Key Storage on Cryptographic Module

Private Keys of Certificates delivered to hardware Cryptomodules are maintained in Cryptomodules evaluated to FIPS PUB 140-2 Level 2 or higher.

Private Keys of Certificates delivered to software Cryptomodules are maintained in Cryptomodules evaluated to FIPS PUB 140-2 Level 1 or higher. The Cryptomodule may store Private Keys in any form as long as the Keys are not accessible without an authentication mechanism. Private Keys must never exist in plain text outside of the Cryptomodule.

6.2.7.2 CA Private Key Storage on Cryptographic Module

CA Private Keys are maintained in HSMs evaluated to FIPS PUB 140-2 Level 3 or higher and are always kept in encrypted form. The HSM containing the Root Private Key used in performing IdenTrust's CA certification services is used for no other Keys (apart from certain Keys used in managing the device itself, in some instances). Each HSM containing Sub CA Private Keys may be shared with multiple other Sub CA Keys. They are handled by the same IdenTrust Trusted Role employees and kept in the same secure storage locations as other HSMs, but CA HSMs are used only for CA Keys. Moreover, their Activation Data differs from that used for other Cryptomodules. HSMs containing CA Private Keys are activated by a PIN Entry Device.

6.2.7.3 CSA, RA, CMS Private Key Storage on Cryptographic Module

CSA, RA and CMS Private Keys are maintained in HSMs evaluated to FIPS PUB 140-2 Level 3 or higher and are always kept in encrypted form. Each Cryptomodule containing CSA, RA and CMS Private Keys may be shared with multiple other CSA, RA and CMS Keys.

6.2.8 Method of Activating Private Keys

Methods of Activating Private Keys may vary based on the Certificate type to which they are associated. See sub-sections below for specific details.

When pass-phrases, passwords or PINs are used, they are a minimum of six (6) characters. Data entry of the pass-phrase, password or PINs are masked.

6.2.8.1 Method of Activating Private Keys for Subscribers

Subscribers of Certificates delivered to hardware Cryptomodules protect their Private Keys from unauthorized use with a strong password. Subscribers of Certificates delivered to software Cryptomodules are instructed to protect their Private Keys from unauthorized use with a strong password. Subscribers are obligated by contract, the IGC-CP and this CPS to authenticate to the Cryptomodule before the activation of Private Keys, as well as to protect the password or other data used to activate the Cryptomodule from disclosure.

6.2.8.2 Method of Activating Private Keys For PIV-I

For PIV-I Card Authentication Certificates, Subscriber activation of Private Keys is not required.

6.2.8.3 Method of Activating Private Keys for CA, CSA, RA and CMS

CA, CSA, RA and CMS Private Keys are activated by Activation Data stored securely and separately from the Cryptomodules in which they are kept. Activation of the Private Key requires a PIN Entry Device (PED) key to be connected to the module. The PED keys and Cryptomodules are stored in separate safes. PED keys and Cryptomodules are retrieved and used always under Separation-of-Duties/Multi-party Control (see Sections 5.1.2.1, 6.1.1 and 6.2.2).

For the CA and CSA, the Private Key is activated by use of the proper PED keys during a scripted, videotaped and witnessed Key Generation or Certificate signing ceremony under Separation-of-Duties/Multi-party Control.

For the RA and CMS (including the PIV-I Content Signing Certificate), the Private Key is activated by use of the proper PED keys during a scripted and witnessed Key Generation or Certificate signing ceremony under Separation-of-Duties/Multi-party Control.

6.2.9 Methods of Deactivating Private Keys

Methods for deactivating Private Keys may vary based on the type of Certificate to which the Private Key is associated. See sub-sections below for specific details.

6.2.9.1 Methods of Deactivating Private Keys for Subscribers

All Subscribers are notified of their obligation to not leave their Cryptomodules unattended or open to unauthorized access while active. Subscribers are required to deactivate their Cryptomodules either by a manual logout or by configuring a passive inactivity timeout that does it automatically.

6.2.9.2 Methods of Deactivating Private Keys for LRAs

LRAs are provided instruction on the security procedures by which they remove their Cryptomodule when not in use and configure the automatic passive inactivity timeouts in the Cryptomodule accordance with the security policy.

6.2.9.3 Methods of Deactivating Private Keys for CA, CSA, CMS and RA

CA, CSA, CMS and RA Cryptomodules are:

- Deactivated via logout or removal procedures when not in use; and
- Not left unattended or otherwise active to unauthorized access.

Cryptomodules when unattended and active are kept locked inside steel cabinets located inside the secure room.

6.2.10 Methods of Destroying Private Keys

Methods of destroying Private Keys may vary based on the type of Certificate to which the Private Key is associated. See sub-sections below for specific details.

6.2.10.1 Methods of Destroying Private Keys for Subscribers

All Subscribers are notified of their obligation to destroy their Private Keys and are provided instructions on Zeroizing, re-initializing or destroying the Cryptomodule when they are no longer needed, or when the Certificates to which they correspond are expired or Revoked. Subscribers of Certificates delivered to software Cryptomodules are instructed to delete their Private Keys, delete the swap file, then erase the

unused disk space using disk/file eraser program, and reboot the workstation.

In cases when the Zeroization or re-initialization procedure fails, the Subscriber is instructed to crush, shred and/or incinerate the Cryptomodule in a manner that destroys the ability to extract Private Keys from the Cryptomodule.

6.2.10.2 Methods of Destroying Private Keys for CA, CSA, CMS and RA System

Upon expiration or Revocation of a CA, CSA, CMS or RA System Certificate, or other termination of use of the Private Signature Key, all copies of the Private Signature Key are securely destroyed. When no longer needed, all Private Keys are destroyed in accordance with the FIPS PUB 140-2 validated Zeroize destruction method that is part of the Cryptomodule's design. Physical destruction of the Cryptomodule is not required.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

IdenTrust retains copies of all Public Keys for archival purposes as part of the Certificate archive process in accordance with Section 5.5.

6.3.2 Certificate Operational Periods and Key Usage Periods

All Certificates and corresponding Keys have maximum Validity Periods not to exceed the following table:

Key Type	Key Usage Period[20]	Certificate Lifetime
Root CA	20 years	37 years
Subordinate CA	10 years for CRL Signing and OCSP Responder Certificates 6 years for Subscriber Certificates	10 years
CSA/CSS	3 years	31 days
RA	3 years	3 years
IGC PIV-I Content Signer	3 years	8 years
Individual Identity, Signing, and Card Authentication[21]	3 years	3 years
Individual Encryption	No restriction	3 years
Group Signing	3 years	3 years
Group Encryption	No restriction	3 years

[20] These Certificate lifetime periods are configured in the CA system according to each Certificate type (e.g., IGC PIV-I Content vs. Machine Subscriber) and this system enforces these limits. For Certificates generated during ceremonies (e.g., Root CA or CSA) the script will state the period and the CA administrator will manually enforce it and a witness will verify it.

See Section 5.6 (Key Changeover), which explains that Sub CA Private Signature Keys are voluntarily retired from signing Subscriber Certificates before this time 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 that are Issued with old Sub CA Signing Key.)

[21] IGC PIV-I hardware and IGC PIV-I Card Authentication assurance Certificates expiration shall not be later than the expiration date of the smart card on which the Certificates reside, which is enforced by the CMS.

Device	3 years	3 years
LRA	3 years	3 years
Bridge Cross Certificate	10-20 years[22]	3 years
PIV-I subscriber certificate expiration cannot be later than the expiration date of the PIV-I hardware token on which the certificate resides and the expiration date of the PIV-I Content Signer certificate used to sign the subscriber certificate on the PIV-I card will not expire before the expiration date of such subscriber certificate.		

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

Generation of Activation Data may vary based on the type of Certificate being activated. See sub-sections below for specific details.

6.4.1.1 Activation Data Generation and Installation for Subscribers

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

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

6.4.1.2 Activation Data Generation and Installation for Participant CAs and External RAs

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

6.4.1.3 Activation Data Generation and Installation for CA, CSA, CMS and RAs

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

6.4.2 Activation Data Protection

Protection of Activation Data may vary based on the type of Certificate being activated. See sub-sections below for specific details.

6.4.2.1 Activation Data Protection for Subscribers

All Subscribers are notified of their obligation to protect Activation Data as follows:

- It should be memorized whenever possible, not written down;
- If written down, it must be secured at the level of the data that the associated Cryptomodule is used to protect, and will not be stored with the Cryptomodule; and
- Activation Data must never be shared with or disclosed to another Individual.

RA Administrators will enforce a mechanism to temporarily lock the Cryptomodule, or terminate the application, after a maximum of six failed login attempts.

[22] 10-year usage period is used for subordinate CAs and 20-year period for Root CA.

LRAs and Subscribers will enforce a mechanism to temporarily lock the Cryptomodule, or terminate the application, after a maximum of ten failed login attempts.

6.4.2.2 Activation Data Protection for Participant CAs and External RAs

Participant CAs and External RAs using remote PED keys must ensure PED keys are held by persons in Trusted Roles in a manner through which Separation-of-Duties/Multi-party Control is ensured when accessing HSMs. When not in use, PED keys must be kept in separate secure locations in order to ensure Separation-of-Duties/Multi-party Control when accessing HSMs. Controls for ensuring security of PED keys must be described in the Participant CA or External RA RPS.

6.4.2.3 Activation Data Protection for CA, CSA, CMS and RAs

Activation Data for Cryptomodules used by IdenTrust for CAs, CSAs, CMS and RAs CMSs are protected by keeping the PED keys in separate safes inside the secure room. As explained in Section 5.1.2.1, access to the secure room requires two Individuals in Trusted Roles. Access to content in the safes requires two Trusted Role Individuals with different authentication mechanisms.

6.4.3 Other Aspects of Activation Data

Activation Data for the Cryptomodules of Subscribers in Trusted Roles is changed every three months to decrease the likelihood that it is discovered.

For Certificates asserting an Assurance Level of PIV-I Hardware, the Activation Data may be reset after a successful biometric 1:1 match of the Applicant against the biometrics collected during the identity proofing process in Section 3.2.3.1. This match is conducted by an LRA or TA and consists of both a positive manual comparison of the facial image on record and an automated comparison of the fingerprints data on record with the Subscriber requesting Activation Data Reset. The comparison is performed by the LRA or TA utilizing an EWS attached to the CMS.

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 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.

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) a web server layer,
2) an application layer,
3) an application database, and
4) an 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. 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 Section 1.3.2. External RAs are obligated by contract, this CPS and the IGC-CP to implement computer security controls consistent with this CPS and the IGC-CP.

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.

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 Security Officers, 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.

6.6.2 Security Management Controls

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 previous 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

No stipulation.

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 IGC-CP to implement Network Security controls consistent with this CPS and the IGC-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, CARL/CRL, AND OCSP IGC Profiles Format

7.1 Certificate Profile

Detailed IGC Profiles are found in the document IGC-Profiles, published as a companion document to IGC-CP and this CPS. For ease of reference, some high level profile information is described in this Section 7.

7.1.1 Version Numbers

IdenTrust issues X.509 v3 Certificates with version field populated with integer "2").

7.1.1.1 Serial Number

Unique serial number for Certificate. For all Certificates, IdenTrust generates a non-sequential serial number that exhibits at least 20 bits of entropy.

7.1.2 Certificate Extensions

Certificate extensions used are compliant with IETF RFC 5280 and include but are not limited to: authority key identifier, subject key identifier, key usage, extended key usage, certificate policies, subjectAlternativeName, authority information access, CRL distribution points, and basic constraints (Root CA and CA Certificates).

7.1.2.1 Certificate Policies

The certificatePolicies extension is populated in all Certificates that are Issued by the Root CA with one or more of the OIDs in Section 1.2.2.

One or more of these OIDs are included in the CertificatePolicies extension of Certificates that are Issued to Subscribers. The CertificatePolicies extension is set to non-critical.

7.1.2.2 Policy Constraints

The Policy Constraints extension in Certificates that are Issued by the Root CA to Subordinate CAs is not populated.

7.1.2.3 Critical Extensions

Certificate Type	Key Usage	Extended Key Usage	Basic Constraints	Name Constraints	Inhibit anyPolicy
Cross Certificate	keycertSign cRLSign		cA=True; path length constraint is absent	presence is optional	inhibit anyPolicy skipCerts=0
Root CA Certificate	keycertSign cRLSign		cA=True; path length constraint is absent		
Subordinate CA Certificate	keycertSign cRLSign		cA=True; path length constraint is absent		
Subscriber Signing Certificate	digitalSignature nonRepudiation				

Certificate Type	Key Usage	Extended Key Usage	Basic Constraints	Name Constraints	Inhibit anyPolicy
Subscriber Encryption Certificate	keyEncipherment				
Non-PIV-I Identity Certificate	digitalSignature	keyPurposeID = Id-pkinit-KPClientAuth			
Non-PIV-I Card Authentication Certificate	digitalSignature	KeyPurposeID = id-PIV-cardAuth			
PIV-I Authentication (Identity) Certificate Subscriber	digitalSignature	keyPurposeID = Id-pkinit-KPClientAuth			
PIV-I Card Authentication Certificate	digitalSignature	KeyPurposeID = id-PIV-cardAuth			
PIV-I Content Signing Certificate	digitalSignature	KeyPurposeID = id-fpki-pivi-content-signing			
PIV-I Key Management (Encryption) Certificate	keyEncipherment				
Device Certificate	digitalSignature keyEncipherment	KeyPurposeID= id_kp_clientAuth id_kp_ipsecEndSystem id_kp_ipsecTunnel id_kp_ipsecUser			
OCSP Responder Certificate	digitalSignature	KeyPurposeID = id-kp-OCSPSigning			
PIV-I Signing Certificate	digitalSignature nonRepudiation				
DirectTrust Domain Bound Signing Certificate	digitalSignature		cA=False		
DirectTrust Domain Bound Encryption Certificate	keyEncipherment		cA=False		
DirectTrust Address Signing Certificate	digitalSignature		cA=False		
DirectTrust Address Encryption Certificate	keyEncipherment		cA=False		

See the IGC Profiles document for additional information.

7.1.3 Algorithm Object Identifiers

7.1.3.1 Signature Algorithm OIDs

Certificates are or may be Issued with the following algorithms and OIDs.

Algorithm	OID
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha256(2)}
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }

7.1.3.2 Subject Public Key Information

Certificates that are Issued under this CPS use the following algorithms and OIDs for identifying the subject Public Key information:

Algorithm	OID
rSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) public-Key-type(2) 1}

7.1.3.3 Elliptic Curve Public Key

Where non-CA Certificates contain an elliptic curve Public Key, the parameters shall be specified as one of the following named curves:

Named Curve	OID
Curve P-256 (ansip256r1)	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }
Curve P-384 (ansip384r1)	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }

7.1.4 Name Forms

Certificate subject and issuer fields are populated with X.500 Distinguished Names composed of standard attribute types such as those defined in RFC 5280. Refer to table below for name forms.

Names Form for CAs

Subject Identifier type:	with data content of:	Indicates:
CountryName (C) Optional	Root CA = The letters “US” Sub CA = A two-letter code	Root CA and that the Root Certificate is managed by a CA operated in the United States. Sub CA and the two letter country code indicating the country of operation for IdenTrust branded sub CAs, or the country of Subscribing Organization for Participant CAs.
OrganizationName (O)	Root CA = The word “IdenTrust” Sub CA = The word “IdenTrust”	Root CA and that the Root CA is owned and operated by IdenTrust. Sub CA and that the Sub CA is owned and operated by IdenTrust.

Subject Identifier type:	with data content of:	Indicates:
CommonName (CN)	Root CA = The words "IdenTrust Global Common Root CA [x][23]" Sub CA = The word "IGC CA [x][24]", or in the case of a Subscribing Organization sponsored Sub CA, the words [Customer] CA [x][25].	Root CA and that the name of the Root CA followed by a number starting in one (1) and progressively increasing with each new instance of the Root Certificate Sub CA and the name of the subCA. A number could be appended to indicate the instance of the Sub CA.

Name Forms for End Entity Certificates

Subject Identifier type:	with data content of:	Indicates:
CountryName (C) Optional	A two-letter code	The two-letter code indicating the country where the Subscribing Organization is located
OrganizationName (O)	The word "Unaffiliated", or if affiliated the name of the Subscribing Organization	The name of Subscribing Organization composed by the original Subscribing Organization, or the word Unaffiliated to show no Subscribing Organization affiliation.
OrganizationUnitName (OU)	Alphanumeric text	A subjectID explained in Section 3.1.5
CommonName (CN)	Alphanumeric text	The Individual or Device's common name as described in Section 3.2.
SerialNumber	Hexadecimal Characters for a Universally Unique Identifier (UUID) in the form prescribed by [IETF RFC 4122]	A unique subject ID explained in Section 3.1.5
AlternativeName	Other Name	Subject:AlternativeName

CA Subject Name Form for SAFE CA Only

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Recommended	CN	0…1	Descriptive name for CA (e.g., "CN=IdenTrust Global Common CA N", where "N" is an integer representing unique identification of CA within the IdenTrust Global Common hierarchy)
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	"Certification Authorities" or similar text
	Required	O	1	Issuer name, e.g., "O=XYZ"

[23] [x]: Iteration of the SubCA cn, (e.g., IGC CA 1, IGC CA 2, etc.)

[24] [x]: Iteration of the SubCA cn, (e.g., IGC CA 1, IGC CA 2, etc.)

[25] [Customer]: Unique Subscribing Organization SubCA name as authorized by IdenTrust PMA. [x]: Iteration of the SubCA cn, (e.g., [Customer] CA 1, [Customer] CA 2, etc.)

	Required	C	1	Country name, e.g., “C=US”
2	Recommended	CN	0…1	Descriptive name for CA (e.g., “CN=IdenTrust Global Common CA N”, where “N” is an integer representing unique identification of CA within the IdenTrust Global Common hierarchy)
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Certification Authorities” or similar text
	Optional	O	0…1	Issuer name, e.g., “O=XYZ”
	Optional	C	0…1	Country name, e.g., “C=US”
	Required	DC	1	Domain name, e.g., “DC=xyz”
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or, “DC=com, DC=au”, etc.

Subject Name Form (non-CA) for SAFE non-CA Only

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See Content	1..N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email, etc.
	Optional	OU	0…N	As needed
	Required	O	1	Subject Organization name (e.g., “O=ABC Inc”) or “Unaffiliated” if no Organization affiliation.
	Required	C	1	Country name, e.g., “C=US”
2	Required	See Content	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email, etc.
	Required	OU	0…N	Must include an OU attribute populated with a unique identifier for the Subject. This unique identifier must associate to a specific Subscriber and must not change when issuing a new certificate to that Subscriber.
	Optional	O	0…1	Subject organization name, e.g., “O=ABC Ltd”
	Required	DC	1	Domain name, e.g., “DC=xyz”
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or, “DC=com, DC=au”, etc.

From time to time SAFE-BioPharma may arrange for a cross-certified issuer to issue end-entity certificates to Subscribers who are not members of the Association. When this occurs, Option 1 (unaffiliated certificates should be Issued. All affiliated certificates will include an attribute value.

When multiple values exist for an attribute in a DN, the DN is encoded so that each attribute value is encoded in a separate relative Distinguished Name.

For more detailed information and other Certificate fields, see IGC Profiles.

7.1.5 Name Constraints

IdenTrust does not utilize name constraints except in the instance of Cross-Certificates as necessary to permit or exclude trust sub-trees. When name constraints are utilized, they are marked critical.

Name constraints are not utilized in IdenTrust CAs that Issue SSL Certificates, as IdenTrust OCSP Responders fully support both signed OCSP Certificate Status requests and the GET method of requesting Certificate status in conformance with Baseline Requirements. In the event status is requested for a non-Issued Certificate, IdenTrust OCSP Responders provide an "unknown" Certificate status.

7.1.6 Certificate Policy Object Identifier

CA and Subscriber Certificates that are Issued under this CPS assert one or more of the IGC certificate policy OIDs listed in Section 1.2.2. Additional OIDs asserting compliance with other Certificate policies may be included.

7.1.7 Usage of Policy Constraints Extension

CAs shall adhere to the certificate formats described in this CPS. CAs shall adhere to the certificate formats described in this CPS.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates with a Policy Qualifier in the Certificate Policies extensions contain a User Notice that incorporates this CPS by reference and makes this CPS binding on all PKI Participants, including any potential Relying Party. By using or otherwise relying on a Certificate, the Relying Party Accepts and consents to not only the language in the User Notice, but also to the applicability of this CPS including limitations of liability, disclaimers of warranties, applicable law, and other notices and disclosures made herein that may be determined to have been necessarily made within the Certificate.

Policy Qualifiers will be populated as required in IGC Profiles.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The certificatePolicies extension indicates the IGC-CP. IGC-CP defines the policy for Issuance of all IGC Certificates, including those Issued by Participant CAs. The certificatePolicies extension may assert policies that are in addition to IGC, such as compliance with CA/B Forum baseline Requirements or DirectTrust CP. Certification practices for all IGC CAs are defined in this CPS. The IGC-CP and IGC-CPS are downloadable from the URL listed in the policy qualifier field of the CertificatePolicies extension in each IGC Certificate. IdenTrust shall have no liability for damages asserted by anyone who has used an IGC Certificate for an inappropriate purpose or in an inappropriate manner, as stipulated in the IGC-CP.

7.1.10 Inhibit Any Policy Extension

IdenTrust may assert InhibitAnyPolicy in CA certificates. When used, the extension is marked noncritical*, to support legacy applications that cannot process InhibitAnyPolicy. SkipCerts is set to 0 to support the requirement for certificate policies in the Federal PKI.

7.2 CRL Profile

7.2.1 Version Numbers

IdenTrust Issues X.509 version two (2) CRLs and populated with integer "1". CRLs conform to RFC 5280.

Signature Algorithm in accordance with Section 6.1.5.

7.2.2 CRL and CRL Entry Extensions

IdenTrust CRLs comply with IGC Profiles.

7.3 OCSP Profile

OCSP Requests and responses are in accordance with RFC 6960. IGC Profiles contains the OCSP Request and response formats.

7.3.1 Version Number(s)

The version number for request and responses is version one (1).

7.3.2 OCSP Extensions

IdenTrust supports the nonce extension in responses. See IGC Profiles.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

IdenTrust has compliance audit mechanisms in place to ensure that the requirements of this CPS, the IGC-CP and provisions of any relevant MOA are being implemented and enforced. Participant CAs and External RAs are similarly required to have compliance mechanisms in place for any functions performed in regards to performance under this CPS.

IdenTrust also utilizes a qualified external auditor to conduct annual audits of all of IdenTrust's operations used in performing its obligations under this CPS.

Participant CAs and External RAs are required to have compliance mechanisms in place for any functions performed in regards to performance of their RA function and operation of any CMS or RA Systems. The compliance audit is to ensure the requirements of the entity's RPS, this CPS, IGC-CP and relevant agreements are being implemented and enforced. Annual compliance audit results must be provided to IdenTrust by the Participant CA or External RA before IdenTrust will grant authority to operate, and subsequently by May 31st of each year for inclusion in IdenTrust's external compliance audit.

The following table details appropriate compliance audits performed annually by external auditors pertaining to the IGC-CP and CPS.

Table - Required Best-Practices Annual Audits

Required Audit
Federal Public Key Infrastructure (FPKI) FPKI Annual Review Requirements
WebTrust for Certification Authorities

8.1 Frequency of Audit or Assessments

All of IdenTrust's operations used in performing the CA, CMS, CSA, RA and LRA services described in this CPS are audited annually by an external auditor. Contracts that IdenTrust has with third party entities that perform RA functions (Participant CAs, External RAs) obligate those parties to undergo a periodic compliance audit that meet the requirements of this Section 8 for all RA and LRA activities listed in this CPS that are performed by such party.

The IdenTrust PMA has the right to require aperiodic compliance audits or inspections of RA operations to validate that subordinate entities are operating in accordance with the security practices and procedures described in this CPS and the RA RPS. The IdenTrust PMA shall state the reason for any aperiodic compliance audit.

IdenTrust also conducts internal and external audits and/or completes requisite certifications as required by other governing CP documents (such as Federal Bridge, DirectTrust, SAFE-BioPharma, etc.) to participate in each respective program; in which case the program will outline the requirements in respect to assessments. Results of these audits are provided to each organization upon completion or re-certificate of the audit and/or certification (see Section 8.0 Compliance Audits and Other Assessment: Table - Required Annual Audits which includes specific criteria that each audit satisfies).

8.2 Identity and Qualifications of Auditors

The auditor, Individual or audit group performing internal or external audits of PKI Service Providers must have the following qualifications:

1) **Qualifications and experience**. Auditing must be the Individual's or group's primary business function. The Individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security auditing credential.
2) **Expertise.** The Individual or group must be trained and skilled in the auditing of secure information systems and be familiar with Public Key infrastructures, certification systems, and the like, as well as Internet security Issues (such as management of a security perimeter), operations of secure data centers, personnel controls, and operational risk management.
3) **Rules and standards.** The Individual or group must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.

8.2.1 IdenTrust's External Auditor

To perform the annual external compliance audit, IdenTrust engages the services of a professional, external 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 Public Key infrastructures.
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 Public Key infrastructures, certification systems, and the like, as well as Internet security Issues (such as management of a security perimeter), operations of secure data centers, personnel controls, and operational risk management. The staff must be large enough to have the necessary depth and range of expertise required to audit IdenTrust's operations in a competent manner.
3) **Reputation.** The firm must have a reputation for conducting its auditing business competently and correctly.
4) **Disinterest.** The firm has 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), the Canadian Institute of Chartered Accountants (CICA), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA, or another qualified auditing standards body, and must require its audit professionals to do the same. Moreover, in auditing secure information systems, the firm should be guided by best practices standards (see Section 8.0 Compliance Audits and Other Assessment: **Table - Required Annual Audits** which includes specific criteria that each audit satisfies). The engagement of the auditing firm takes the form of a contract obligating the firm to assign members of its professional auditing staff to perform the audit when required. While the audit is being performed, those staff must, by agreement, perform the audit as their primary responsibility.

In addition, the members of the firm's staff performing the audit are contractually subject to the following requirements:

1) **Professional qualifications.** Each auditing professional performing the audit must be a member of the AICPA, CICA, ISSA, (ISC)2, IIA, or ISACA. In addition, at least one staff member must be qualified as a Certified Information Systems Auditor, AICPA Certified Information Technology Professional (CPA.CITP), or have another recognized information security auditing credential.
2) **Primary responsibility.** The 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 must conform to the ethical and other professional rules of the AICPA, CICA, ICAEW, ISSA, (ISC)2, IIA, or ISACA or those of the applicable other qualified auditing standards body.
4) **Professional background.** The professionals assigned to perform the audit must be trained to a standard generally accepted in the auditing field. They must also be familiar with PKI and other information security technologies and their secure operation. IdenTrust's operations are audited to ensure that IdenTrust conforms to its CPs and CPS, as well as to all audits as listed in Section 8.0 Compliance Audits and Other Assessment: **Table - Required Annual Audits** (also includes specific criteria that each audit satisfies). , and familiarity with those documents is necessary for performing the audit. The auditor that IdenTrust has selected for past audits has in every case been one of the large, well-known auditing firms. IdenTrust expects to continue this practice while changing from time to time the specific firm selected.

8.3 Assessor's Relationship to Assessed Entity

The auditor, Individual or audit group that performs an internal compliance audit of a given PKI Service Provider may be a Security Officer or other individual within the Organization, but shall not be an Individual responsible for the daily operation of the PKI Service Provider's PKI environment or involved in RA functions.

For CAs, the compliance auditor either shall be a private firm, that is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.

8.3.1 IdenTrust's Internal Auditor for Quarterly Audits

The auditor may be a Security Officer, but shall not be an Individual responsible for daily operation of IdenTrust's PKI environment or involved in RA functions.

8.3.2 IdenTrust's External Auditor

IdenTrust has a contractual relationship with the auditing firm for performance of the audit, but otherwise, auditors shall be independent, unrelated entities having no financial interest in each other. Auditors shall maintain a high standard of ethics designed to ensure impartiality and the exercise of independent professional judgment, subject to disciplinary action by their licensing bodies. The auditor(s) shall have no other relationships with IdenTrust or its officers and directors, including financial, legal, social or other relationships that would constitute a conflict of interest.

8.4 Topics Covered by Assessment

The scope and substance of the annual compliance audits performed on CA, CMS, CSA, RA and LRA operations shall meet those required under the laws and policies specified in the IGC-CP to maintain approval to operate.

The annual compliance audit shall cover all aspects of the IGC-CP, this CPS, the RA RPS (if any), and any relevant Memorandum of Agreement (MOA) or agreement between IdenTrust and entity. See Section 8.0 Compliance Audits and Other Assessment: Table - Required Annual Audits which includes specific criteria that

each audit satisfies. .

Components other than CAs may be audited fully or by using a representative sample. If the auditor uses statistical sampling, all PKI components, PKI component managers and operators shall be considered in the sample. The samples shall vary on an annual basis.

8.5 Actions Taken as a Result of Deficiency

If an internal quarterly Audit determines the quality of Issued SSL Certificates has deficiencies in regards to meeting requirements of this CPS, IGC-CP. The RA RPS (if any) and any relevant MOA, the following actions will be performed:

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

If an annual compliance audit reports any material noncompliance with applicable law, the IGC-CP, this CPS, any applicable RPS, any relevant MOA, or any other contractual obligations related to the CA, CMS, CSA, RA or LRA services it provides to the PKI, the following actions will be executed:

- The responsible party, if not IdenTrust, will notify the IdenTrust PMA of the discrepancy;
- The Security Officer will note the discrepancy;
- The Security Officer will notify the IdenTrust PMA and any other relevant PMAs about the discrepancy; and
- The audited party will develop a plan to resolve the discrepancy, subject to IdenTrust PMA approval.

In the event the audited party fails to take appropriate action in response to the report or due to the nature of discrepancy, the IdenTrust PMA may instruct the CIO to Revoke Certificates that are Issued to or halt temporarily operations of the affected CA, RA and/or CMS, or take other actions deemed as appropriate. The PMA may also refer the matter to IdenTrust legal counsel for further action. The nature of problem may dictate (per this CPS or IGC-CP) to Revoke Certificates or halt operation even if the audited party is planning to take action.

8.6 Communications of Results

Results of annual compliance audits are required to be communicated by Participant CAs and External RAs to IdenTrust's Security Officer no later than May 31st of each year. Annual compliance audit results from Participant CAs and External RAs may be included in IdenTrust's annual compliance audit.

Results of external audits are communicated by IdenTrust's Security Officer to the IdenTrust CIO, the IdenTrust PMA and any appropriate regulatory bodies, as may be required by law, regulation or agreement. IdenTrust will provide interested PKI Participants with a letter containing the attestation of management and its auditor's letter concerning the effectiveness of controls. Otherwise, all audit information will be considered confidential business information in accordance with Section 9.3.

All audits will identify the CP, CPS, RA RPS (if any) and any MOA documents used in the assessment including their dates and version numbers.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance/ Renewal Fees

CAs and RAs may charge reasonable fees for Certificate Issuance and Certificate Renewal in accordance with a fee schedule. The fee schedule is established either by publication or by written agreement between the provider of the service (CA, or the RA) and the consumer of the service.

9.1.2 Certificate Access Fees

IdenTrust does not charge Certificate access fees. All Participant CAs shall not charge Certificate access fees.

9.1.3 Revocation or Status Information Access Fees

CAs must publish CRLs for all Certificates and provide OCSP-based Certificate status information for Certificates asserting an Assurance Level of PIV-I Hardware at no charge.

No other stipulation.

9.1.4 Fees for Other Services

CAs or RAs may set any reasonable fees for any other services that the CA or RA may offer.

9.1.5 Refund Policy

CAs or RAs may have a documented refund policy.

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

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

9.2.3 Insurance/Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

All information stored locally on CA or RA equipment is handled as sensitive, and access is restricted to those with an official need-to-know in order to perform their official duties. Private Keys used to sign Certificates asserting security privileges are classified at the same level as the privileges that are to be asserted. In any cases where IdenTrust does not independently confirm security privilege information, RAs are required to perform such confirmation.

Audit information is considered sensitive and may not be disclosed to anyone for any purpose other than for auditing and mandatory reporting requirements, or as required by law.

9.3.1 Scope of Confidential Information

The following are considered within the scope of Confidential Business Information:

- All Private Keys;
- Any Activation Data used to access stored Private Keys or to gain access to any CA system component;
- Any business continuity and disaster recovery plans;
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information used by PKI Participants;
- Any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS);
- Any information held by CAs, an LRA, and TA that is held as private information in accordance with Section 9.4; and
- Any transactional, audit log and archive record identified in Section 5.4 or 5.5.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate Revocation Lists, OSCP Responses, and other publicly available information in the Repository are not considered Confidential Business Information.

9.3.3 Responsibility to Protect Confidential Information

All PKI Participants are responsible for protecting the Confidential Business Information in their possession, custody or control.

9.4 Privacy of Personal Information

As described below, Certificates, and personal or corporate information appearing in them or in public directories, are not considered confidential. All other personal or corporate information held by IdenTrust, a Participant CA, External RA, LRA or a TA are considered confidential and shall be used only for the purpose of providing PKI-related services.

9.4.1 Privacy Plan

CAs, RAs, LRAs, and TAs collect only such personal information about an Applicant and Subscribing Organization as necessary for Issuance of the Certificate. For the purpose of proper administration of Certificates, a CA, RA, LRA or TA may request information not intended to be included in the Certificate for use in issuing and managing the Certificate (e.g., identifying numbers, business or home addresses and telephone numbers, etc.). Personal information collected for the purposes of Certificate Issuance, maintenance and Revocation is used only for such purposes. CAs, RAs, LRAs, and TAs comply with the information collection and storage requirements of the privacy and data protection laws applicable for the jurisdictions in which they operate. Also, personal information will be made available to, and subject to correction by, the subject following an appropriate request by, and authentication of, the subject.

9.4.2 Information Treated as Private

Confidential information about a Subscriber and their Subscribing Organization that is not publicly available in the contents of a Certificate, CRL or in the LDAP Directory is considered private.

Collection of PII is limited to the minimum necessary to validate the identity of the subscriber. This may include attributes that correlate identity evidence to authoritative sources. IdenTrust provides a Privacy Statement available on the IdenTrust website. Additionally, the Subscriber Agreements include notice to the subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing purposes

is not be used for any other purpose.

9.4.3 Information Not Deemed Private

Certificates, CRLs and OCSP Responses, and personal or corporate information appearing in them and in the LDAP Directory, are not considered private.

9.4.4 Responsibility to Protect Private Information

Each PKI Participant is responsible for protecting the confidentiality of private information that is in its possession, custody or control with the same degree of care that it exercises with respect to its own information of like importance, but in no event less than reasonable care, and shall use appropriate safeguards and otherwise exercise reasonable precautions to prevent the unauthorized disclosure of private information.

In the event that IdenTrust terminates PKI activities, IdenTrust will be responsible for disposing of or destroying sensitive information, including PII, in a secure manner, and maintaining its protection from unauthorized access until destruction.

9.4.5 Notice and Consent to Use Private Information

A PKI Participant may use private information with the subject's express written consent or as required by applicable law or court order.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Private information is not disclosed to any law enforcement agency, except when:

a) authorized or required by IGC-CP;
b) required to be disclosed by law, Government rule/regulation, or court order; or
c) authorized by the Subscriber when necessary to effect an appropriate use of the Certificate. All requests for disclosure of private and/or confidential information from a law enforcement agency must be made in accordance with applicable law.

All requests for disclosure of private and/or confidential information for purposes of litigation must be made in writing. Unless prohibited by law, the custodian of such information shall give all interested persons or parties reasonable prior written notice before making any disclosure of private information.

9.4.7 Other Information Disclosure Circumstances

Except as provided above or in a written agreement, the disclosure of private information requires the Subscriber's express written consent.

9.5 Intellectual Property Rights

Neither IdenTrust nor any CA or RA shall knowingly violate any intellectual property rights held by others.

A Private Key will be treated as the sole property of the legitimate holder of the Certificate containing the corresponding Public Key.

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 to a license or other express permission from IdenTrust. Any other use of the above without the express written permission of IdenTrust is expressly prohibited.

A RA RPS shall define restrictions of use of the intellectual property within the RPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CAs represent and warrant that they conform to the stipulations of this document, including:

- Conforming their practices and procedures to the stipulations of RPS (if any), this CPS, the IGC-CP, any applicable cross-certified CPs, and the policies associated with any third party OIDs asserted in certificatePolicies;
- For DirectTrust the Issuer CAs MUST represent to DirectTrust, Subscribers, and Relying Parties that they comply, in all material aspects, with this CP, their CPS, and all applicable laws and regulations.
- For RAs providing services related to Issuance of DirectTrust Certificates, ensuring that the organization is accredited under the Direct Trusted Agent Accreditation Program for Registration Authorities (DTAAP-RA) prior to issuing the RA a production DirectTrust Certificate;
- For HISPs providing services related to use of DirectTrust Certificates, ensuring that the organization is accredited under the Direct Trusted Agent Accreditation Program for Health Information Service Providers (DTAAP-HISP) prior to issuing the HISP a production DirectTrust Certificate;
- Ensuring that registration information is accepted only from RAs or LRAs who understand and are obligated to comply with this CPS and applicable policy(s);
- Including only valid and appropriate information in the Certificate, and maintaining evidence that due diligence was exercised in validating the information contained in the Certificate;
- Ensuring that obligations are imposed on Subscribers in accordance with Section 9.6.3, and the Subscribers are informed of the consequences of not complying with those obligations;
- Revoking the Certificates of Subscribers found to have acted in a manner counter to those obligations; and
- Operating or providing for the services of an on-line repository that satisfies the obligations under Section 9.6.5, and informing the repository service provider of those obligations if applicable.

CAs represent and warrant that they conform to the provisions and stipulations of any applicable Cross-Certified entity MOA.

CAs maintain an agreement with Subscribing Organizations concerning the obligations pertaining to authorizing affiliation with Subscribers.

A CA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

9.6.2 RA Representations and Warranties

An RA represents and warrant to the CA at the time it approves a Certificate for Issuance that:

- It has verified all information required for Issuance for a Certificate and all information contained in the Certificate as required by processes defined in the RA RPS (if any), this CPS and IGC-CP;
- It approved Issuance of the Certificate in accordance with the RA RPS (if any), this CPS, and IGC-CP;
- It knows of no material misrepresentations of fact in the Certificate; and
- There are no errors in the information in the Certificate that were introduced by it as a result of a failure to exercise reasonable care in processing the application for the Certificate.

In addition to these representation and warranties, RAs represent and warrant that they conform to and comply with the stipulations of RPS (if any), this CPS and the IGC-CP and ensure that their LRAs and TAs also comply with these stipulations. Any RA, LRA or TA who is found to have acted in a manner inconsistent with these obligations is subject to Revocation of their registration authorizations and responsibilities.

For RAs performing I&A for DirectTrust Certificates, RAs are additionally required to represent and warrant that they conform to and comply with the stipulations of DirectTrust CP.

9.6.3 Subscriber Representations and Warranties

At the time of Issuance and during the Certificate's Validity period, as long as it has not been Revoked, the Subscriber warrants and represents to CA and the RA (if any) that:

- All information provided by it (and its Subscribing Organization, where applicable) and included in the Certificate, and all representations made by it during its efforts to obtain a Certificate, are true and not misleading;
- Each Digital Signature created using the Private Key corresponding to the Public Key listed in the Certificate is the Subscriber's Digital Signature;
- The Private Key has been continuously protected and that no unauthorized person has ever had access to the Private Key; and
- The Certificate and Key Pair are being used exclusively for authorized and legal purposes.
- Their Private Key will be used only from machines that are protected and managed using commercial best practices for computer security and network security controls.
- In addition to these representation and warranties, Subscribers are required to represent and warrant that they conform to and comply with the stipulations of this CPS and the IGC-CP, including that they will:
- Accurately represent themselves in all communications with the PKI;
- Protect their Private Keys from compromise at all times (including if the Subscriber Keys are held by a Custodian, or authorized third party who has implemented a Custodial Subscriber Key Store and uses secure processes against potential compromise), in accordance with this CPS and IGC-CP, as stipulated in their Subscriber Agreement;
- Notify, in a timely manner, the CA, RA, or LRA that Issued their Certificates of suspicion that their Private Keys are compromised or lost. Such notification shall be made directly, or indirectly through mechanisms consistent with this CPS;
- Abide by all the terms, conditions, and restrictions levied upon the use of their Private Keys and Certificates; and
- Use Certificates in accordance with this CPS and the IGC-CP.

Primary Machine Operators are required to assume the obligations of Subscribers for the Certificates associated with their Devices. They also warrant and represent that FQDNs or other information used to identify Devices, Organization names and domain names are accurate, current, complete, and not misleading and that they will install the Certificate only on the Device corresponding to the Device represented in the Certificate subjectDN or server accessible at the domain name listed on the Certificate.

Group Certificate Sponsors are required to assume the obligations of Subscribers for the Certificates associated with Groups. They also warrant and represent that information contained in applications for Group Certificates is accurate, current, complete, and not misleading and that they will use the Certificate only for legitimate business purposes of the Group Certificate.

9.6.4 Relying Party Representations and Warranties

Any time that a Relying Party uses or otherwise relies on a Certificate, he or she represent and warrant to the CA and the RA (if any) that:

- He or she has read and agree to the terms and conditions of relevant Sections of this CPS;
- He or she has sufficient information, independent from the Certificate, to make an informed decision as to the extent to which they will rely on the information in the Certificate;

- That he or she is solely responsible for deciding whether or not to rely on such information and use the Certificate for the purpose for which it was Issued, as indicated in the Certificate information (e.g., the key usage extension) in accordance with guidelines set by the X.509 Version 3 Amendment;
- To establish trust in the Certificate using certification path validation procedures described in RFC 5280, prior to reliance; and
- To 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/Subscribing Organizations

A Subscribing Organization represents and warrants that it:

a) Authorizes the affiliation of Subscribers with the Organization for Affiliated Certificates;
b) Verifies that any information it may provide during the identity proofing and/or registration processes is accurate; and
c) Will immediately inform the CA of any severance of affiliation with any current Subscriber.

9.6.6 Representations and Warranties of Other PKI Participants

No stipulation.

9.6.6.1 Repository Representations and Warranties

See Section 2.

9.6.6.2 CSA Obligations

A CSA, who provides Revocation status and/or complete validation of Certificates represents and warrants that it conforms to the stipulations of this CPS and the IGC-CP, including:

- Providing this CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of this CPS and the IGC-CP;
- Ensuring that Certificate and Revocation information is accepted only from valid CAs; and
- Including only valid and appropriate response, and to maintain evidence that due diligence was exercised in validating the Certificate status.

A CSA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5 of IGC-CP.

9.7 Disclaimers of Warranties

EXCEPT AS EXPRESSLY WARRANTED IN (A) SECTIONS 9.6.1 AND 9.6.2 ABOVE, CAs AND RAs GOVERNED BY THIS CPS AND IGC-CP HEREBY DISCLAIM ANY AND ALL OTHER WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND ONINFRINGEMENT WITH REGARD TO ANY CERTIFICATE, REPOSITORY OR CERTIFICATE STATUS SERVICE.

Except as expressly warranted in (a) Sections 9.6.1 and 9.6.2 above and without limiting the foregoing disclaimer, neither IdenTrust, CA, RA, nor any of their affiliates, officers, directors, licensors, employees or representatives represent or warrant (i) that a Certificate, Repository or Certificate Status Service will meet particular requirements or be error free; (ii) that any Certificate, Repository or Certificate Status Service will

be available, uninterrupted, accessible, timely or secure; (iii) that any defects will be corrected, or that a Certificate, Repository or Certificate Status Service will be free from viruses, worms, Trojan horses or other harmful properties; or (iv) that the information provided will be accurate, reliable, timely, or complete.

9.8 Limitations of Liability

The liability (and/or limitation thereof) of IdenTrust to Participant CAs to which IdenTrust CA Certificates are Issued shall be set forth in the applicable agreements.

OTHER THAN THE ABOVE DESCRIBED LIMITATIONS OF LIABILITY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL IDENTRUST BE LIABLE FOR ANY DIRECT OR INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CPS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE TOTAL, AGGREGATE LIABILITY FOR A PARTICIPANT CA ARISING OUT OF OR RELATED TO IMPROPER ACTIONS BY THE PARTICIPANT CA SHALL BE LIMITED TO ONE THOUSAND DOLLARS ($1,000 USD) PER TRANSACTION AND ONE MILLION DOLLARS ($1 MILLION USD) PER INCIDENT).

9.9 Indemnities

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

Unless agreed upon in separate agreement, neither IdenTrust nor any PKI Service Provider assumes financial responsibility for improperly used or improperly relied upon Certificates.

A CAs agreement between itself and other entities (such as Cross-Certification Bridge Authority) shall specify any additional indemnification terms between the CA and entity (e.g. indemnification of the Cross-Certification Bridge Authority).

Each Subscriber shall indemnify PKI Service Providers for any loss suffered by any PKI Service Provider(s) that are occasioned by the Subscriber’s (a) improper use of Certificates or Key Pairs; (b) failure to safeguard Private Keys; (c) failure to comply with the provisions of the IGC-CP, this CPS, or any agreement with such PKI Service Provider, (d) breach of a representation or warranty of Subscriber hereunder, or (e) other acts or omissions giving rise to the loss.

Subject to the other provisions of this Section 9.9 and the rest of Section 9, bilateral agreements between PKI Service Providers and other PKI Participants may include additional indemnity obligations.

9.10 Term and Termination

9.10.1 Term

This CPS and any amendments hereto shall become effective upon publication in the Repository.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

The conditions and effect resulting from termination of this document will be communicated via IdenTrust's or the alternative Participant CA's Repository upon termination outlining the provisions that may survive termination of the document and remain in force.

- For IdenTrust repository, https://secure.identrust.com/Certificates/policy/globalcommon/index.html.
- For the Participant CA repository see Appendix A.

The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the Validity Periods of such Certificates.

9.11 Individual Notices and Communications with PKI Participants

9.11.1 The provisions below in this Section 9.11.1 shall govern with respect to any notice provided in relation to this CPS to or from IdenTrust; provided; however, this Section shall not be construed to govern with respect to any communication, including notices, for which a different method is expressly provided for (a) in this CPS (e.g. notices under Section 9.12) or (b) in an agreement between IdenTrust and the Participant.

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

i. by digitally signed communication sent from the Participant to IdenTrust via email Registration@IdenTrust.com, which communication will be deemed effective when acknowledged via email by IdenTrust; or
ii. by written communication sent from the Participant to IdenTrust via internationally recognized overnight courier to IdenTrust Registration, 5225 Wiley Post Way, Ste 450, Salt Lake City, UT 84116, which such communication will be deemed effective when delivered as evidenced by written confirmation of receipt as recorded by the courier.

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

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

9.11.2 The method(s) of providing notice between each CA (other than IdenTrust) and Participants (other than IdenTrust) shall be set forth in the CA's CPS, provided that at a minimum the CA must provide a physical address at which notice by via internationally recognized overnight courier will be deemed effective when

delivered as evidenced by written confirmation of receipt as recorded by the courier.

9.12 Amendments

This CPS will be reviewed by IdenTrust from time to time. Errors, updates, or suggested changes to this document should be communicated to policy@IdenTrust.com. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.1 Procedure for Amendment

All changes to this CPS that may materially affect Subscribers or Relying Parties are subject to a 15-day notification requirement. Affected PKI Participants may file comments with IdenTrust within 15 days of original notice. Written and signed comments on proposed changes must be directed to IdenTrust. Decisions with respect to the proposed changes are at the sole discretion of IdenTrust.

9.12.2 Notification Mechanism and Period

IdenTrust will notify all interested persons of proposed changes, the final date for receipt of comments, and the proposed effective date of change. A copy of this CPS is available in electronic form on the Internet at https://secure.identrust.com/Certificates/policy/globalcommon/index.html, and via email from policy@IdenTrust.com. In the event that IdenTrust considers making changes to this CPS that are subject to notification requirements, IdenTrust will post the proposed changes on its Web site, the final date for receipt of comments, and the proposed effective date of change.

Editorial and typographical corrections, changes to contact details and other minor changes that do not materially impact PKI Participants may be changed without notice and are not subject to the notification requirements herein.

9.12.3 Circumstances Under Which an OID Must be Changed

A certificate policy OID for Certificates that are Issued pursuant to this CPS will change only if the change in the IGC-CP results in a material change to the trust by the relying parties.

9.13 Dispute Resolution Provisions

In the absence of other agreements between the parties covering the services provided under this CPS, the dispute resolution procedures specified in this CPS provide the sole remedy for any claim against a PKI Service Provider for any loss sustained by any, Applicant, Subscriber, Subscribing Organization, or Relying 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 IGC-CP, and/or this CPS, or from any other act or omission. No Relying Party, Applicant, Subscriber, or Subscribing Organization shall require IdenTrust or Bridge Service Providers under its Root Certificate to respond to any attempt to seek recourse through any other means.

Notwithstanding the foregoing, any Applicant, Subscriber, Subscribing Organization, or Relying Party may enter into a separate bilateral agreement with a PKI Service Provider under which those parties may agree that the remaining provisions of this Section shall provide (a) the sole remedy for any claim against a PKI Service Provider, or (b) an alternative dispute resolution mechanism.

9.13.1 Claims and Initial Determinations

Before making a claim to recover a loss for which a PKI Service Provider may be responsible, an Applicant, Subscriber, Relying Party, or Subscribing Organization (the “Claimant”) shall make a thorough investigation. IdenTrust will cooperate reasonably in that investigation.

The Claimant will then present to IdenTrust reasonable documented proof:

- That the Claimant has suffered a recoverable loss as a result of a System Transaction;
- Of the amount and extent of the recoverable loss claimed; and
- Of the causal linkage between the alleged System Transaction and the recoverable loss claimed, itemized as necessary.

Immediately upon the occurrence of any reliance event, the Claimant will notify IdenTrust of any matter, which may result in a claim against a PKI Service Provider. In any event, the Claimant must file notice and all required proof of the claim (using a mandatory procedure accessed through IdenTrust's web site) not later than four months after the reliance event out of which the claim arises. Any failure to provide the required notice and proof of claim within the required four-month period will constitute a conclusive waiver of the claim and an agreement with the PKI Service Provider that the Claimant will seek no remedy against it to recover for any liability for the claim.

Notice of the claim must be given on a form that is downloadable at:

https://www.IdenTrust.com/externaluse/claim-form-loss.html.

Instructions for completion and submission of the claim form also appear on that web page.

On receipt of a claim form, IdenTrust will forward the claim to the PKI Service Provider who may determine to pay the claim or deny it. The PKI Service Provider may also pay the claim in an amount less than the amount claimed if it determines that the loss calculations exceed the amount that the PKI Service Provider is obligated to pay. IdenTrust will notify the Claimant of the PKI Service Provider's determination within 30 days of receipt of the claim form. If a response is not made within 30 days of receipt of the claim form, then the claim is deemed denied. If the Claimant is not satisfied with the initial determination, the Claimant may appeal it as provided in the next Section.

If IdenTrust determines that the Claimant has failed to provide information required to determine the claim, IdenTrust shall deny the claim, subject to the right of the Claimant to resubmit the claim one time, within 30 days after IdenTrust's initial denial, with all required information. A Claimant shall not submit more than one claim form for the same claim except for a resubmission pursuant to the preceding sentence. The Claimant shall pay to IdenTrust the reasonable costs of processing any claim for which IdenTrust finds the proof required by this Section to be so clearly lacking that the claim must be considered frivolous.

9.13.2 Appeals

In the event that the Claimant wishes to contest the PKI Service Provider's initial determination of the claim, it may appeal that determination to the IdenTrust Appeals Officer, which can review the decision in the exercise of its oversight of IdenTrust's policies and their implementation in practice.

To appeal an initial determination of a claim, the Claimant must notify the IdenTrust Appeals Officer that it appeals the decision. Failure to file formal written notice of appeal within 30 days after denial of the initial claim constitutes waiver of the appeal and the PKI Service Provider's initial determination shall be final and binding upon the Claimant. Claimant's waiver of the appeal as provided herein shall be a complete defense, and shall bar any attempt at judicial review of the initial determination on the ground of failure to exhaust administrative remedies.

The notice of appeal may simply request the IdenTrust Appeals Officer to review the initial determination, or it may state reasons why the initial determination is in error. The IdenTrust Appeals Officer has discretion to undertake an investigation of the basis for the claim, consider additional evidence or facts not previously considered, or base its decision entirely on evidence previously provided for the initial determination.

The IdenTrust Appeals Officer must decide the appeal within thirty (30) days after of receipt of the notice of appeal, unless the claimant agrees to an extension of time. In deciding the appeal, the IdenTrust Appeals Officer may reverse the initial determination and determine that the PKI Service Provider pay or otherwise resolve the claim, or the IdenTrust Appeals Officer may affirm the initial determination. The IdenTrust Appeals Officer may also require payment of any portion of the original claim that was not already paid or take other action to settle or resolve the claim.

The IdenTrust Appeals Officer shall give notice to the Claimant of the final determination of claim appeal in writing. If the final determination of the claim is to pay the claimant any sum, payment shall be made within thirty (30) days after the final determination is sent.

The decision of the IdenTrust Appeals Officer shall be final and binding upon the Claimant.

9.13.3 Confidentiality of Claims Process

Neither IdenTrust, nor the PKI Service Provider, nor the Claimant shall disclose to any third party:

1) The fact that the claim was made;
2) The amount or other details of the claim;
3) The circumstances that gave rise to the claim;
4) The outcome of the claim, including the amount recovered; or
5) Any opinion regarding the processing or disposition of the claim.

This Section, however, does not apply in relation to legal counsel representing either the Claimant or the PKI Service Provider. It also does not apply in the event that the Claimant seeks relief through arbitration.

9.14 Governing Law

Choice of Law. Subject to any limits appearing in applicable law, the laws of the state of New York, U.S.A., shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in the State of New York. This choice of law is made to ensure uniform procedures and interpretation for all PKI Participants, no matter where they are located. This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

Headings. The headings of the Sections of this CPS are included for the purposes of convenience only and shall not affect the interpretation of any provision hereof.

Plurals/Pronouns/Gender. All pronouns and any variations thereof shall be deemed to refer to the masculine, feminine or neuter, singular, or plural, as appropriate.

9.15 Compliance with Applicable Law

This CPS shall be subject to applicable national, state, local, and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting or importing software, hardware or technical information.

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

PKI Participants (other than IdenTrust) 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

In the event that a clause or provision of this CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

Except where an express time frame is set forth in this CPS, no delay or omission by any PKI Participant to exercise any right, remedy or power it has under this CPS shall impair or be construed as a waiver of such right, remedy or power. A waiver by any party of any breach of this CPS shall not be construed to be a waiver of any other or repeated breach of this CPS. Bilateral agreements between PKI Service Providers and other PKI Participants may contain additional provisions governing enforcement; provided, however that in no event can such additional provisions alter the rights of IdenTrust hereunder.

9.16.5 Force Majeure

NO PKI SERVICE PROVIDER SHALL INCUR LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: (I) ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; (II) CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; (III) THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH THE PKI SERVICE PROVIDER HAS NO CONTROL; (IV) FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; (V) STRIKE; (VI) ACTS OF TERRORISM OR WAR; (VII) ACT OF GOD; OR (VIII) OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT THE FAULT OR NEGLIGENCE OF THE PKI SERVICE PROVIDER.

9.17 Other Provisions

None.

10 DIRECTORY INTEROPERABILITY PROFILE

10.1 Protocol

An area in the IdenTrust's secure website that is accessed via Server-authenticated SSL/TLS-Encrypted session contains the Root CA Certificate.

Other areas in the IdenTrust website that are accessed through HTTP protocol will contain the Root CRL, all the latest versions of all other CRLs and the subordinate signing CA Certificates.

The LDAP Directory contains the CRL for the Root CA, and optionally, signing CA Certificates and the most recent corresponding CRLs for each Participant CA.

10.2 Authentication

No Client authentication is required to read or get information from the Repository.

Access to the LDAP Directory is allowed through anonymous authentication and no authentication is needed to read CRL information.

All write, update, add entry, delete entry, add attribute, delete attribute, change schema, and exercise of other directory modification rights in the Repository require Client Certificate authentication and encryption using Secure Shell (SSH) protocol.

10.3 Naming

When CA Certificates are stored under the directory entry for the Subject Name of the CA. The issuedByThisCA element of crossCertificatePair shall contain the Certificate(s) issued by a CA whose name the entry represents.

All CRLs are filed under the directory entry of the CA that issued the CRL.

10.4 Object Class

Entries that describe CAs are defined by the organizationUnit structural object class. All CA entries belong to the pkiCA cpCPS auxiliary object classes.

10.5 Attributes

CA entries are populated with the caCertificate, crossCertificatePair, CertificateRevocationList, and cPCPS attributes, as appropriate.

11 INTEROPERABLE SMART CARD DEFINITION

This CPS and IGC-CP provide for the Issuance of smart cards that are technically interoperable with Federal Personal Identity Verification ("PIV") Card readers and applications as well as PIV-Interoperable ("PIV-I") card readers and applications. Smart cards used for Certificates asserting an Assurance Level of PIV-I Hardware Certificates fully map to the PIV-I specification as defined by the U.S. Federal Government. This Section defines the specific requirements of smart cards mandatory for Issuance of PIV-I Hardware Certificates. It relies heavily on relevant specifications from the National Institute of Standards and Technology ("NIST"), as promoted within the US FBCA CP.

1) The smart card platform(s) utilized for Certificates asserting an Assurance Level of PIV-I Hardware are included in the GSA FIPS 201 Evaluation Program Approved Product List (APL). The smart card platform is inclusive of the smart card, embedded FIPS PUB 140-2 certified cryptographic storage module and smart card middleware designed to provide secure access to Certificate Private Key Material.
2) Smart cards utilized for Certificates asserting Assurance Levels of PIV-I Hardware contain appropriate Private Keys and OIDs, and PIV-I Identity Certificate Private Keys and OIDs, mapped to equivalent US FBCA Assurance Levels.
3) Smart cards utilized for Certificates asserting Assurance Levels of PIV-I Hardware contain appropriate Private Keys and OIDs, and PIV-I Card Authentication Private Keys and OIDs, mapped equivalent US FBCA Assurance Levels.
4) Smart cards may contain a Private Key and associated Signing Certificate asserting an Assurance Level of PIV-I Hardware or any lesser Assurance Level. Which Certificates are present in the smart card is based on specific customer requirements and implementation needs.
5) Smart cards may contain a Private Key and associated Encryption Certificate asserting an Assurance Level of PIV-I Hardware or any lesser Assurance Level. Which Certificates are present in the smart card is based on specific customer requirements and implementation needs.
6) Smart cards utilized for Certificates asserting an Assurance Level of PIV-I Hardware contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the card holder facial image printed on the card.
7) Smart cards utilized for Certificates asserting an Assurance Level of PIV-I Hardware are Issued under PIV-I Hardware policies and all data objects on it are in accordance with SP 800-73 as specified for PIV-Interoperable (PIV-I) by the Federal Bridge.
8) Biometrics on the smart cards utilized for Assurance Level of PIV-I Hardware comply with Section 4.4 of FIPS 201-1 and SP 800-76.
9) Card Holder Unique Identifier (CHUID) complies with Section 4.2 of FIPS 201-1. The Federal Agency Smart Credential Number (FASC-N) is modified as defined in Section 3.3 of SP800-73-3. FASC-N is constructed using Agency Code equal to 9999, System Code equal to 9999, and Credential Number equal to 999999. CHUID contains a 16 byte Global Unique Identifier (GUID).
10) The CMS-signed objects such as fingerprints and photographs contain the GUID as entry UUID attribute in place of the FASC-N as pivFASC-N attribute.
11) Smart cards are visually distinct from the US Federal PIV Card.
12) The Smart card physical topography includes, at a minimum, the following items on the front of it:
    a) Subscriber facial image;
    b) Subscriber full name;
    c) Affiliation with a Subscribing Organization, if such affiliation is asserted in Certificate(s) contained in the card Cryptomodule; otherwise the Issuer of the card; and
    d) Card expiration date.

13) Smart cards have an expiration date at most six (6) years from Issuance. The expiration date is calculated by the system at time of encoding and kept in the smart card and in the system.
14) Smart card expiration is no later than the expiration of the PIV-I Content Signing Certificate on the card, which conforms to the Content Signing Certificate profile specified in IGC Profiles. This is accomplished by creating new Content Signing Certificates prior to the expiration of its Keys and manually configuring the CMS to start signing content with the new Certificate/Keys. Since the difference between the longer life of a Content Signing Certificate and shorter life of its Keys is more than a smart card lifespan, there will always be enough life in a Content Signing Certificate to sign the card appropriately.
15) The PIV-I Content Signing Certificate and corresponding Private Key are managed within a trusted CMS in accordance with the practices specified in this document.
16) At Issuance the TA or LRA activates and releases the smart card to the Subscriber only after a successful 1:1 biometric match of the Applicant against the biometrics collected during identity-proofing (see Section 3.2.3.1).

Smart cards utilized for Certificates asserting an Assurance Level of PIV-I Hardware are activated by the CMS to support card personalization and post-Issuance card update. To activate the smart card for personalization or update, the CMS performs a challenge response protocol using Cryptographic Keys stored on the smart card in accordance with [SP800-73]. The Card Management Keys are specific to each smart card and meet the algorithm and Key size requirements stated in [SP 800-78].

12 REFERENCES

The following documents were referenced in development of this CPS.

Document	Description
RFC 1034	Introduction to DNS (Nov 1987) http://tools.ietf.org/html/rfc1034
RFC 2253	Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names (Dec. 1997) http://www.ietf.org/rfc/rfc2253.txt
RFC 2616	Hypertext Transfer Protocol -- HTTP/1.1 (June 1999) http://www.ietf.org/rfc/rfc2616.txt
RFC 3379	Delegated Path Validation and Delegated Path Discovery Protocol Requirements (Sept. 2002) http://www.ietf.org/rfc/rfc3379.txt
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (Nov. 2003) http://www.ietf.org/rfc/rfc3647.txt
RFC 4122	A Universally Unique Identifier (UUID) URN Namespace (Jul. 2005) http://www.ietf.org/rfc/rfc4122.txt
RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP) (Sept. 2005) http://www.ietf.org/rfc/rfc4210.txt
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (May 2008) http://tools.ietf.org/html/rfc5280
RFC 5322	Internet Message Format (Oct. 2008) http://tools.ietf.org/html/rfc5322.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (June 2013) http://tools.ietf.org/html/rfc6960
NIST SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure (Feb. 2001) http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf
NIST SP 800-53	Recommended Security Controls for Federal Information Systems and Organizations http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
NIST SP 800-83	Guide to Malware Incident Prevention and Handling (Nov. 2005) http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
NIST SP 800-57	Recommendation for Key Management (Mar. 2007) http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf
NIST SP 800-90A	Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Jan. 2012) http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf
NIST SP 800-21	Guideline for Implementing Cryptography In the Federal Government (Dec. 2005) http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf
NIST SP 800-73	Interfaces for Personal Identity Verification (4 parts) (Feb. 2010) http://csrc.nist.gov/publications/PubsSPs.html
NIST SP 800-85A-2	PIV Card Application and Middleware Interface Test Guidelines (Jul. 2010) http://csrc.nist.gov/publications/nistpubs/800-85A-2/sp800-85A-2-final.pdf

NIST SP 800-78-3	Cryptographic Algorithms and Key Sizes for Personal Identity Verification (Dec. 2010) http://csrc.nist.gov/publications/nistpubs/800-78-3/sp800-78-3.pdf
NIST SP 800-76-1	Biometric Data Specification for Personal Identity Verification (Jan. 2007) http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf
FIPS PUB 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors (Mar. 2006) http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
FIPS PUB 186-3	Digital Signature Standard, (Jun. 2009) http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
FIPS PUB 140-2	Security Requirements for Cryptographic Modules (May 2001) http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS PUB 112	Password Usage (May 1985) http://www.itl.nist.gov/fipspubs/fip112.htm
FIPS PUB 180-2	Secure Hash Standard (Aug. 2002) http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
FPKIPA	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards (Apr. 2010) http://www.idmanagement.gov/fpkipa/documents/pivi_Certificate_crl_profile.pdf
FPKIPA	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (Dec. 2011) http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf
FPKIPA	X.509 Certificate Policy for the Federal Bridge Certification Authority (Dec. 2011) http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf
FPKIPA	FBCA Supplementary Antecedent, In-Person Definition http://www.idmanagement.gov/fpkipa/documents/FBCA_Supplementary_Antecedent.pdf
CA/Browser Forum	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.2.5 https://cabforum.org/wp-content/uploads/BRv1.2.5.pdf (Apr. 2015)
Direct Project	Applicability Statement for Secure Health Transport, v1.1 http://wiki.directproject.org/file/view/Applicability%20Statement%20for%20Secure%20Health%20Transport%20v1.1.pdf/353270730/Applicability%20Statement%20for%20Secure%20Health%20Transport%20v1.1.pdf.
DirectTrust	DirectTrust Certificate Policy, v1.4 http://www.directtrust.org/about-policies/
W3C Recommendation	XML Key Management Specification, ver. 2 (XKMS 2.0) (Jun. 2005) http://www.w3.org/TR/xkms2

APPENDIX A – PIV-INTEROPERABLE SMART CARD DEFINITION

The intent of PIV-I is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Agency. Thus, reliance on PIV-I Cards requires compliance with technical specifications and specific trust elements. This appendix defines the specific requirements of a PIV-I Card. It relies heavily on relevant specifications from the National Institute of Standards and Technology (NIST).

The following requirements shall apply to PIV-I Cards:

1) To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).
2) PIV-I Cards shall conform to [NIST SP 800-732].
3) The mandatory X.509 Certificate for Authentication shall be issued under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.
4) All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile].
5) PIV-I Cards shall contain an asymmetric X.509 Certificate for Card Authentication that:
    a) conforms to [PIV-I Profile];
    b) conforms to [NIST SP 800-73]; and
    c) is issued under the PIV-I Card Authentication policy.
6) PIV-I Cards shall contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder Facial Image printed on the card.
7) The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.
8) Visual distinction of a PIV-I Card from that of a Federal PIV Card is required to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. At a minimum, images or logos on a PIV-I Card shall not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201].
9) The PIV-I Card physical topography shall include, at a minimum, the following items on the front of the card:
    a) Cardholder facial image;
    b) Cardholder full name;
    c) Organizational Affiliation, if exists; otherwise the issuer of the card; and
    d) Card expiration date.
10) Special attention should be paid to UUID requirements for PIV-I.
11) PIV-I Cards shall have an expiration date not to exceed 6 years of issuance.
12) Expiration of the PIV-I Card should not be later than expiration of PIV-I Content Signing certificate on the card.

13) The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID. The PIV-I Content Signing certificate shall conform to [PIV-I Profile].

14) The PIV-I Content Signing certificate and corresponding private key shall be managed within a trusted Card Management System as defined by Appendix B.

15) At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.

16) PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78]

APPENDIX B – CARD MANAGEMENT SYSTEM REQUIREMENTS

PIV-I Cards are issued and managed through information systems called Card Management Systems (CMSs). The complexity and use of these trusted systems may vary. Nevertheless, Entity CAs have a responsibility to ensure a certain level of security from the CMSs that manage the token on which their certificates reside, and to which they issue certificates for the purpose of signing PIV-I Cards. This appendix provides additional requirements to those found above that apply to CMSs that are trusted under this Certificate Policy.

The Card Management Master Key shall be maintained in a FIPS 140-2 Level 2 Cryptographic Module and conform to [NIST SP 800-78] requirements. Diversification operations shall also occur on the Hardware Security Module (HSM). Use of these keys requires PIV-I Hardware or commensurate. Activation of the Card Management Master Key shall require strong authentication of Trusted Roles. Card management shall be configured such that only the authorized CMS can manage issued cards.

The PIV-I identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV-I credential without the cooperation of another authorized person.

Individual personnel shall be specifically designated to the four Trusted Roles defined in Section 5.2.1. Trusted Role eligibility and Rules for separation of duties follow the requirements for Medium assurance in Section 5.

All personnel who perform duties with respect to the operation of the CMS shall receive comprehensive training. Any significant change to CMS operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

Audit log files shall be generated for all events relating to the security of the CMS shall be treated the same as those generated by the CA (see Sections 5.4 and 5.5).

A formal configuration management methodology shall be used for installation and ongoing maintenance of the CMS. Any modifications and upgrades to the CMS shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CMS.

The CMS shall have document incident handling procedures that are approved by the head of the organization responsible for operating the CMS. If the CMS is compromised, all certificates issued to the CMS shall be revoked, if applicable. The damage caused by the CMS compromise shall be assessed and all Subscriber certificates that may have been compromised shall be revoked, and Subscribers shall be notified of such revocation. The CMS shall be re-established.

All Trusted Roles who operate a CMS shall be allowed access only when authenticated using a method commensurate with PIV-I Hardware.