IdenTrust Global Common Certificate Policy

Version 1.4.7

November 29, 2018

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Summary of Changes/Comments
1.1	April 19, 2013	Initial version following completion of mapping to US FBCA CP; baseline CP for Day Zero Audit
1.2	May 06, 2013	Revisions to Sections 9.1.2, 9.1.3 and 9.6.3 to clarify language in response to US FBCA CPWG comments.
1.2.1	August 13, 2013	Minor language changes to better incorporate and bind Participants to IGC Certificate Profiles.
1.3	July 15, 2015	The following sections have been modified primarily to meet business requirements for IGC Certificates: ➢ Section 1 to distinguish IGC Basic Assurance Certificates by Key Storage Mechanism. Additional Certificate Policies (OIDs) added for IGC Basic Hardware Certificates. Old OIDs deprecated. ➢ Section 1 to add Card Authentication and Identity Certificate Policies (OIDs) for Basic Hardware and Medium Hardware Assurances. ➢ Section 3.2.3.3. to add requirements for Group Certificates. ➢ Section 4.12.1 add Key escrow and recovery policy. ➢ Section 6.2.6 to clarify Private Key transfer requirements for software and hardware KSMs. ➢ Section 6.3.2 to provide more Certificate granularity. ➢ Section 6.4.2 to allow backup of RA Private Signing Keys. ➢ Section 8 to better align audit requirements with current US FBCA CP audit requirements. ➢ Section 9.11 regarding Participant communications. In addition, RA requirements clarified and corrections to terms, formatting and spelling errors have been made throughout. This version 1.3 was approved by IdenTrust PMA, but not published pending auditor approval in regards to DirectTrust issuance.
1.3.1	July 31, 2015	Final version including minor changes needed for DirectTrust issuance.
1.4	May 27, 2016	Removed the requirement for Machine Operators of Device Certificates to have an Individual Certificate. Increased PIV-I card lifetime to 6 years. Revised Table of OIDs

		Clarified primary and Secondary Machine Operator roles and requirements Clarified use of term certificate policy OID
1.4.2 NOTE: Skipping version 1.4.1 to align with CPS and Certificate Profiles version 1.4.2	October 12, 2016	Removing duplicate Group Software Certificate OIDs Adding new Group Device Software Certificate OIDs Clarified definition of Group Device and Address Certificates
1.4.3	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.
1.4.4	April 11, 2018	Add Group Organization OIDs Clarify HSM and KSM storage section 6.2.1 Remediate items requested by FPKIPA
1.4.5	June 22, 2018	Integrated SAFE-BioPharma Bridge Certificate Authority (SBCA) cross-certification with IGC.
1.4.6	October 3, 2018	Revision to Section 6.1.7 added for support of DirectTrust Basic Constraint requirement.
1.4.7	November 29, 2018	Updates to list external CPs to clarify version numbers and approval dates. Update to align with DirectTrust CP V1.4 06262018 Modifications to support automated retrieval

TABLE OF TABLES

1 INTRODUCTION

1.1 Overview

This IdenTrust Global Common ("IGC") Certificate Policy ("IGC-CP") is the policy under which IdenTrust establishes and operates a Public Key Infrastructure ("PKI") for the purpose of issuing Certificates that can be used in an interoperable manner through Cross-certification with multiple bridges. It does not define a particular implementation practice of the IGC PKI, nor the plans for future implementations or future Certificate policies. This document will be reviewed and updated as described in Section 9.12, based on criteria that include but are not limited to the current and expected use of the IGC PKI, operational experience, changing threats, and further analysis.

This document defines the creation and management of X.509 Version 3 Public Key Certificates for use in applications requiring authentication of an end entity, digital signing of content by an end entity, digital signing of content by a content signer, and data or message confidentiality between networked computer-based systems and/or individuals. Such applications include, but are not limited to electronic mail, transmission of confidential information, signature of electronic documents and authentication of infrastructure components such as web servers, firewalls, and directories.

References and bibliography of related publications are included at the end of this document. Related publications contain information that forms the basis for PKI. Acronyms used throughout this Certificate Policy ("CP") are defined in Section 1.6.

1.1.1	Relationship between IGC CP and cross-certified CPs	The relationship between this IGC CP and other cross-certified CPs is asserted in CA certificates issued by IdenTrust in the policyMappings extension. This extension shall include all relevant policy mappings and indicate that these policies are equivalent to each other.

1.2 Document Identification

1.2.1	Alphanumeric Identifier	The alphanumeric identifier (i.e., the title) for this CP is the "IdenTrust Global Common Certificate Policy, Version 1.4.5" dated June 22, 2018.
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 Issued by CAs under this CP is 2.16.840.1.113893.0.100. The following table defines the Certificates types and IGC-CP Assurance Levels for Issuance under this CP. 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 shall be consistent with Assurance Levels as specified in other cross-certified CP documents: • DirectTrust CP v1.4 dated June 26, 2018 • SAFE-BioPharma Bridge Certificate Authority (SBCA) v3.15 dated March 14, 2018 Basic Assurance Level Certificates 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 Certificate storage type. Basic Hardware and Basic Software Certificates are Assurance Level of Basic.

Certificates Issued under this CP shall 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 on customer requirement and use case. 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 an OID under this CP. Additional OIDs may be asserted in Certificates Issued under sub-CAs that are signed under this CP. In this case, certificate policy OIDs are detailed in the IGC-CPS, the IGC Certificate Profile document and the specific CP correlated to the sub-CA signed under this policy.

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; (iii) IGC Medium SSL/TLS Software; (iv) IGC Medium SSL/TLS Hardware; (v) or IGC PIV-I Content Signing. All other policies defined in this CPS are reserved for human Subscribers.

Certificates may use additional OIDs to assert affiliations, compliance with particular policies, intended usages or for other purposes. All IGC specific certificate policy OIDs are provided in Table 1, below; refer to the most current versions of the IGC-CPS, the IGC Certificate Profiles document and any other IGC related CP documents. All OIDS that are designated in cross-certified CP documents are provided in the IGC CPS document and incorporated into the IGC Certificate Profiles document. Cross-certified CPs include:

- DirectTrust
- SAFE-BioPharma

Unless otherwise specified, a requirement specified in this CP applies to all Certificates Issued under this CP.

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

Table 1 - IGC-CP 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 June 15, 2016 Signing Certificate Encryption Certificate – superseded June 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 Signing Certificate Group 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
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 SSL/TLS Software	Medium Device Software	SSL/TLS Certificate	2.16.840.1.113839.0.100.37.2
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
IGC Medium SSL/TLS Hardware	Medium Device Hardware	SSL/TLS Certificate	2.16.840.1.113839.0.100.38.2

1.3 PKI Participants

This CP describes an open-but-bounded PKI. Other relevant documents will include the Certification Practice Statement ("CPS"), if any, of the CAs participating within the PKI, and the individual contracts signed (on paper or electronically) by each Participant within the PKI.

PKI Participants' functions, rights and obligations within the PKI are shown at a high level in the diagram below, and described generally in the following subsections and more specifically throughout this CP.

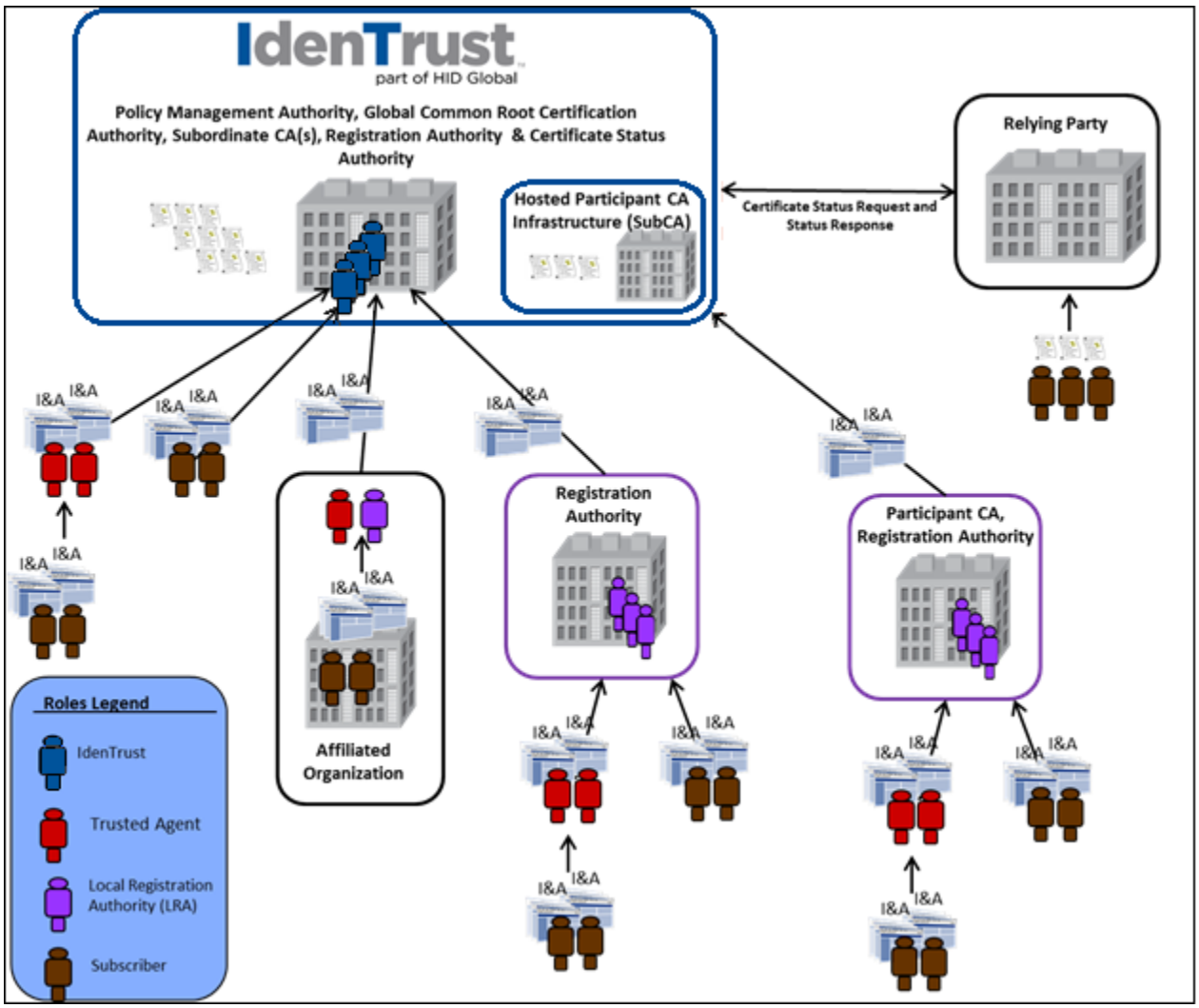

Figure 1: IGC-CP Participants

1.3.1	IdenTrust Policy Management Authority	The IdenTrust PMA oversees the adoption, administration of this CP with CAs, RAs, Certificate Status Authorities, and other PKI Participants. The IdenTrust PMA shall be responsible to approve the cross-certification of other policies to this IGC CP.

1.3.1.1 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 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 CP and the IdenTrust Global Common Certification Practice Statement ("IGC-CPS"). 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 Subordinate 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 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 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 Issued by Participant CAs.

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 CP is an assertion of the certificate policies that IdenTrust, Participant CAs, RAs and others implement, and they are bound by and shall comply with the undertakings and representations of this CP.

CAs may delegate their Registration functions to Registration Authorities who meet the financial requirements of Section 9.2.

1.3.1.2 Certificate Status Authority

A Certificate Status Authority ("CSA") provides status information on Certificates on behalf of a particular CA through online transactions. A CSA operates a Certificate Status Server ("CSS") which provides authoritative Certificate status and Revocation information to Relying Parties. Examples of a CSA include OCSP servers identified in the authority information access extension of a Certificate.
All CAs that Issue IGC PIV-I Certificates shall provide an OCSP-based CSS.

1.3.2 Registration Authority

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. RA functions are generally related to the performance of I&A and include the following:

- Establishing an environment and procedure for Certificate Applicants to submit their Certificate applications (e.g., creating a web-based enrollment page);
- I&A of Individuals or entities submitting requests for new Certificate Issuance, Certificate Re-Key, Certificate Modification or Certificate Renewal;
- Approving or rejecting Certificate applications;
- Initiation of Certificate Revocations, either at the Subscriber's request or upon the RA's own initiative;
- Authenticating the subject's identity;
- Verifying the attributes requested by the subject for their Certificate;
- Assigning Distinguished Names ("DNs") to subjects; and
- Distributing KSMs and associated software to Subscribers.

Each RA operating under the terms of this CP shall agree to perform such RA functions, and may perform other duties, provided they satisfy all requirements of this CP and the CPS of the CA under which they operate.

Communication between the RAs and CAs shall be accomplished in a secure manner ensuring confidentiality and integrity.

Communications between CA and RA Systems or CMSs shall be authenticated and encrypted using an RA Certificate Issued by IdenTrust for the purposes of such communication.

1.3.3 Card Management System

The Card Management System (CMS) manages smart card token content. In this context the CMS requirements are associated with the PIV-I policies only. A CMS will only be deployed within IdenTrust or an authorized RA Organization. IdenTrust, as the CA, is responsible for ensuring that each CMS implementation meet the requirements described in this CP, including requirements stated in Appendix B. A CMS shall not be issued any certificates that express the PIV-I Hardware or PIV-I Card Authentication policy OID.

1.3.4	Subscribers	A Subscriber is an end-entity Individual or Device 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 (e.g. authorized third party), a Private Key that corresponds to the Public Key listed in the Certificate. Subscribers may only use Certificates for purposes indicated by the Certificate Type (ex. Signing Certificate or Encryption Certificate). Where Certificates are Issued to Devices, there shall be an Individual (Primary Machine Operator) who is responsible for carrying out Subscriber duties. Secondary Machine Operators may also carry out some responsibilities related to a Device as described in the IGC-CPS.
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	Subscribing Organizations	A Subscribing Organization is an Organization that authorizes affiliation with Subscribers. A Subscriber may be Issued an affiliated Certificate, which expresses a relationship between an Organization and the subject of the Certificate. The Organizational affiliation shall be indicated in a relative DNs in the subject field in the Certificate. Certificates expressing affiliation shall be Revoked in accordance with Section 4.9 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. A Relying Party is required to act reasonably in determining whether to rely on a Certificate as further defined in Section 4.5.2. By using or relying on a Certificate, the Relying Party agrees to be bound by the provisions of this CP and the CPS under which the Certificate was Issued.
1.3.7	Other Participants	

1.3.7.1 Local Registration Authority

The Local Registration Authority ("LRA") is an Individual who collects and confirms Applicant identity information and any other information provided by the Applicant for inclusion in a Certificate (LRAs are Individuals, whereas RAs are Organizations). The LRA is a Trusted Role held by Individuals who are subject to the requirements of Section 5.3. LRAs are required to comply with this CP and with the CPS of the CA under which they operate. LRAs generally service a limited population as authorized by the RA.

Except where otherwise in this CP or the CPS of the CA under which an LRA operates, all requirements applicable to RAs apply to LRAs.

1.3.7.2 Trusted Agent

Trusted Agents are Individuals who act 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 shall be either:

1) An employee of the CA or RA;
2) An Individual who, while not a direct employee of the CA or RA, has a direct contractual relationship with the CA or RA, either as: a) an Individual; or b) an employee of an Organization that has a direct contractual relationship with the CA or RA that involves performance of collection and/or confirmation of information regarding Applicants and/or Subscribers; or
3) An employee of an Organization that has an employer/employee relationship with the Applicants and/or Subscribers for whom the Trusted Agent will be collecting and/or confirming information.

All activities of the Trusted Agent shall be performed in accordance with the IGC-CP and CPS of the applicable CA. The duties to be performed by the Trust Agent include:

1) Performance of in-person identification of Applicants;
2) Collection of copies of supporting identity documentation;
3) Delivery of said documentation and/or supporting electronic input to the LRA for the applicable CA or RA; and
4) Support for Applicants and Subscribers as appropriate or necessary during the various applicable life-cycle processes (i.e. application, Registration, Revocation, and Re-Key).

The CA or RA may provide the Trusted Agent with material to facilitate the activities being performed by the Trusted Agent on behalf of the CA or RA, including, but not limited to: software products, dedicated web pages, electronic or paper forms, instruction manuals, and training sessions; however, under no circumstances shall the CA or RA provide the Trusted Agent with automated interfaces to the CA or provide the Trusted Agent with direct access into the CA/RA systems.

The Trusted Agent role is not a Trusted Role.

1.4 Certificate Usage

1.4.1	Allowed Certificate Uses	A CA shall specify allowed Certificate uses in their CPS.
1.4.2	Prohibited Certificate Uses	Certificates Issued under the provisions of this CP 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) for use in any software or hardware architectures that provide facilities for interference with encrypted communications, including, but not limited to: (a) active eavesdropping or (b) traffic management of Domain Names or IP Addresses that the Organization does not own or control; or (iii) 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 CP	This CP is administered by: IdenTrust Services, LLC 5225 Wiley Post Way Salt Lake City, UT 84116
1.5.2	Contact Person	Questions regarding the implementation and administration of this CP should be directed to: Attn: PMA Chair IdenTrust Services, LLC 5225 Wiley Post Way Salt Lake City, UT 84116 Email: helpdesk@IdenTrust.com
1.5.3	Person Determining CP and Participant CPS Suitability for the Policy	The suitability and applicability of this CP is determined by the IdenTrust PMA. The IdenTrust PMA also determines CPS suitability of any CA operating under this CP, based on a compliance analysis performed by the PMA itself or a party independent from the CA and who is not the CPS author.
1.5.4	CPS Approval Procedures	All CAs shall submit a CPS to the IdenTrust PMA for approval. The IdenTrust PMA shall determine whether a CPS complies with this policy. The CA shall meet all IGC-CP requirements and receive written approval of the CPS from the IdenTrust PMA prior to commencing operations.
1.5.5	Waivers	There shall be no waivers to this CP.

1.6 Definitions and Acronyms

Capitalized terms and acronyms used herein and in related agreements and other documents incorporating this CP have the meaning described in this Section 6. Where the context and usage of a term implies that a substantive conflict occurs between definition of a term as provided in this CP and term definitions in

CPS, RPS or other policy documents, the definition provided in this CP will govern interpretation of the term.

1.6.1 Definitions

Accept or Acceptance: Acceptance is a Subscriber act that triggers the Subscriber's rights and obligations with respect to the Certificate under this CP, and the CA'S 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).

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 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.

Business Associate: A Business Associate (BA) helps Covered Entities carry out healthcare 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.

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.

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 CP, the CMS requirements contained throughout this CP 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 the IGC PIV-I Hardware Assurance or IGC PIV-I Card Authentication Assurance certificate policy OIDs.

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. CA Certificates in a Certificate Chain are connected by successive, superior CA Certificates up to the Root Certificate, which may be a self-signed Certificate. For Subscribers under this CP, the Root Certificate is a self-signed Certificate Issued by the IGC Root CA.

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 CP 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 CP are defined as:

- Signing Certificate;
- Encryption Certificate;
- Identity Certificate;
- Card Authentication Certificate;
- Content Signing Certificate;
- Device Certificate;
- SSL / TLS Certificate;
- Group Certificate; and
- Group Device 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 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 secure software or hardware that: (i) generates Key Pairs; (ii) stores cryptographic information; and (iii) performs cryptographic functions.

Custodian: A Custodian is an organization or authorized third party that operates a Custodial Subscriber Key Store. The Custodial Organization will typically appoint an Information System Security Officer (ISSO) who is responsible to administer the Custodial Subscriber Key Store.

Custodial Subscriber Key Store: A Custodial Subscriber Key Store holds keys for Custodial-managed Subscriber Certificates in one location. The Custodial Subscriber Key Store is typically managed by an Information System Security Officer (ISSO).

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 digital certificate Issued to a Device and is typically managed by a Machine Operator or .Custodian.

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 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, 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), e-mail address (e) or (mail), Organization name (o), Organizational unit (ou), locality (l), state (st) and/or country (c).

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 Certificate: A Group Certificate can be either a Group Medium Assurance Software or a Group Medium Assurance Device Software Certificate. Group Certificates include both Signing and Encryption Certificates.

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 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).

Health Information Services Provider: A Health Information Services Provider (HISP) is an entity or organization that processes or manages security and transport for health information exchange among health care entities or individuals using the Direct standard for transport.

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 CP 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.

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 itself as Issuer. 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 is named as the Issuer in the Issuer DN field in a Certificate.

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.

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 shall able to demonstrate through policy and audit that the data is accurate and maintained with appropriate integrity, privacy and confidentiality.

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 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.

IdenTrust SubjID: has the same meaning as IdenTrust subjectID.

Information System Security Officer: Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle. Is responsible to execute the responsibilities associated with holding and managing the Private Keys of a Subscriber when such Private Keys are held in a Custodial Subscriber Key Store.

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 a 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.

Machine Operator: A Machine Operator may be a Primary Machine Operator or a Secondary Machine Operator.

National Provider Identifier: A National Provider Identifier (NPI) is a unique 10-digit identification number issued by the Centers for Medicare and Medicaid Services (CMS). Some certificates may require inclusion of the NPI.

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.

Non-Declared Entity Certificate: A Non-Declared Entity Certificate is a Certificate issued to a Non-Declared Entity.

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 CP 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 Subordinate 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 CP and the relevant CA'S CPS when performing RA functions.

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 CP 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 CA's CPS and this CP;
- Verified the Digital Signature and Certificate were valid at the time of reliance by using OCSP and the RFC 5280 certification path validation process as required by the CA'S CPS and in accordance with this CP; and
- Used the Certificate for purposes appropriate under the CA'S CPS, without 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.

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, and is approved by IdenTrust as a part of the Organization onboarding process.

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 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 CP, 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 Operator to act in the role of Secondary Machine Operator. This list is a section within the Subscribing Organization Authorization Agreement that is initially submitted during the Registration process and archived as a document in the related Device Certificate account record in the CA database. Changes, in the form of a new Secondary Machine Operators List are submitted by the Primary Machine Operator to the CA and added to archived documents associated with the 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 an SSL server). 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 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.

Subject Name or Subject Distinguished Name: See Distinguished Name.

Subordinate CA: A Subordinate CA is an Organization Issued a Subordinate CA Certificate by the IGC Root CA. All Subordinate CAs under this CP are required to be operated and managed by IdenTrust. All Subordinate CAs are required to follow and adhere to the provisions of this CP and the relevant CA'S 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 shall 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. This form authorizes individuals named in the form to act in specific roles, such as Subscriber, Primary Machine Operator and Secondary Machine Operator.

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). Suspension can be reversed and in some cases may revert to Revocation, if a specific period of time has passed and the Certificate has been left in a Suspended status.

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 CA'S CPS and in accordance with this CP.

Trust Anchor: See Root Certificate.

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

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

ASN.1	Abstract Syntax Notation (version 1)
ATAB	DirectTrust Accredited Trust Anchor Bundle
BA	Business Associate
CA	Certification Authority
CE	Covered Entity
CHUID	Card Holder Unique Identifier
CIS	Certificate Information System
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSS	Certificate Status Server
DN	Distinguished Name – See Subject Name / Subject Distinguished Name
DNS	Domain Name System
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EWS	Enrollment Work Station
FASC-N	Federal Agency Smart Credential Number
FBCA	U.S. Federal Bridge Certification Authority

FHIR	Fast Healthcare Interoperability Resources
GTAB	DirectTrust Government Trust Anchor Bundle
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	Object Identifier
OCSP	Online Certificate Status Protocol
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
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 directory protocol organized by country, region, Organization, etc.
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

CAs shall operate repositories available over the internet to support their PKI operations for its own and all Relying Party populations. CAs that cross-certify with the US FBCA or other bridges shall ensure interoperability with bridge repositories.

Mechanisms used for posting information into a Repository shall include:

- Availability of the information as required by the Certificate information posting and retrieval stipulations of this CP, and
- Access control mechanisms when needed to protect Repository availability and information as described in later sections.

2.2 Publication of Certificate Information

At a minimum, all CAs shall publish CA Certificates and CRLs.

2.2.1	Publication of Certificates and Certificate Status	CA and Subscriber Certificates shall only contain valid Uniform Resource Identifiers ("URIs") that are accessible by relying parties. Certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., LDAP, HTTP).
2.2.2	Publication of CA Information	The IdenTrust PMA shall publish information concerning the IGC PKI necessary to support its use and operation. The IGC-CP and IGC-CPS shall be publicly available on the IdenTrust web site (see http://www.identrust.com).
2.2.3	Interoperability	Where Certificates and CRLs are published in directories, standards-based schemas for directory objects and attributes are required. Directory interoperability information is provided in Section 10.

2.3 Time, Frequency, and Availability of Publication

CA Certificates shall be published to the Repository immediately upon Issuance. Certificates of Subscribers may be published to a publicly available Repository to the locations specified in the CA's CPS. CRLs shall be published immediately upon issuance to the locations specified in the CA's CPS upon issuance.

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

Any CA Repository information not intended for public dissemination or modification shall be protected. Access to information in a CA's Repositories shall be determined by the CA pursuant to the rules and statutes that apply to that CA.

Certificates and Certificate status information in the CA Repository should be publicly available through the internet wherever reasonable. At a minimum, the CA repositories shall make CA Certificates and CRLs published by the CA and CA Certificates Issued to the CA available to Relying Parties.

However, Certificates that contain a Universally Unique Identifier ("UUID") in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., LDAP, HTTP, etc.).

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

A CA shall only generate and sign Certificates that contain a non-null subjectDN complying with the X.500 standard. Certificates may also include other name forms in the subject alternative name forms field provided the field is marked as non-critical. This CP does not restrict the types of names that can be used.

The table below summarizes the naming requirements that apply to each level of assurance for this CP.

Table 2 - Level of Assurance Naming Requirements

Basic	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical. Email addresses may optionally be included in Subject Alternative Name. If included, email addresses must be verified.
Medium Software Medium Software CBP Medium Hardware Medium Hardware CBP PIV-I Hardware	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical. Email addresses may optionally be included in Subject Alternative Name. If included, email addresses must be verified.
PIV-I Card Authentication	Non-Null Subject Name, and Subject Alternative Name.

Content Signing Certificates shall clearly indicate the Organization administering the CMS.

Basic Hardware Card Authentication Certificates, IGC Medium Hardware Card Authentication Certificates and PIV-I Card Authentication Certificates subjectDN shall not contain the Subscriber's common name. Instead, the DN shall populate the serialNumber attribute with the UUID associated with the card by taking one of the following forms:

- For Certificates with Subscribing Organization: serialNumber=UUID, ou=Subscribing Organization Name,{Base DN};
- For Certificates with no Subscribing Organization: serialNumber=UUID, ou=Unaffiliated, ou=entity CA's Name, {Base DN}.

The UUID shall be encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").

		For PIV-I Hardware Certificates, the subjectDN shall either contain the value "Unaffiliated" in the last Organizational unit (ou) attribute or shall contain the Subscribing Organization name in an appropriate relative DN attribute (e.g., Organization (o), Organizational unit (ou), or domain component (dc) attribute).
3.1.2	Need for Names to Be Meaningful	Names shall identify the person or object to which they are assigned. The CA shall ensure that an affiliation exists between the Subscriber and any Organization that is identified by any component of any name in its Certificate. When DNs are used, the common name shall represent the Subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be FQDNs, IP addresses, program component identifiers, serial numbers or other (Subject Name) expressed similar identifiers within the subjectCommonName (cn) of the subjectDN of the Device Certificate. For Certificates Issued to Individual Subscribers, the subjectDN shall either contain the value "Unaffiliated" in the last Organizational unit (ou) attribute or shall contain the Subscribing Organization name in an appropriate relative Distinguished Name attribute (e.g., Organization (o), Organizational unit (ou), or domain component (dc) attribute). Names shall never be misleading. When DNs are used, they shall accurately reflect Organizational structures. When DNs are used, the common name shall observe name space uniqueness requirements. When User Principal Names ("UPNs") are used, they shall be unique within the Participant CA namespace and accurately reflect Organizational structures. Each CA shall only Issue Certificates with Subject Names from within a name-space approved by the IdenTrust PMA. Unless approved by IdenTrust PMA, CAs shall not certify other CAs.
3.1.3	Anonymity or Pseudonymity of Certificate Holders	CA Certificates shall not contain anonymous or pseudonymous identities. 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	DNs in Certificates shall be interpreted using the X.500 series of specifications and ASN.1 syntax. If present, e-mail names in the Subject Alternative Name field shall be interpreted using RFC 5322, specifying the format of internet e-mail messages. E-mail addresses and FQDNs can be resolved through DNS. Sections 4.1.2.4 and 4.2.1.7 of RFC 5280 describe how character sets and strings are to be interpreted in Issuer, subject, and alternative name fields. RFC 2253 explains how an X.500 DN 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. If present, UUID values in the Subject and/or Subject Alternative Names shall be interpreted using 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	The IdenTrust PMA is responsible for ensuring CAs and RAs enforce name uniqueness within the X.500 name space for which they have been authorized. Specifically, name uniqueness shall be enforced. It is recommended that the CA's CPS shall define the following: • What name forms shall be used, and • How the CA will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith" leaves a CA's community of Subscribers, and a new, different "Joe Smith" enters the community of Subscribers, how will these two people be provided unique names?).
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. An End Entity is not guaranteed that its Distinguished Name or Subject Name will contain any requested trademark. The Issuing CA is not required to subsequently issue a new IGC Certificate to the rightful owner of any name if the Issuing CA has already issued to that owner an IGC Certificate containing a DN and Subject Name that are sufficient for identification within the PKI. The Issuing CA is not obligated to seek evidence of trademarks or court orders.
3.1.7	Name Claim Dispute Resolution Procedure	The IdenTrust PMA shall 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. CAs and RAs may also enroll Trusted Agents 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, the Subject shall be required to prove possession of the Private Key that corresponds to the Public Key in the Certificate request. For Signing Keys, the Subscriber may use its Private Key to sign a value and provide that value to the CA issuing the Certificate. The CA shall then validate the signature using the Subject's Public Key.

The PMA may allow other mechanisms that are at least as secure as those cited here.

In the case where a Key is generated by the CA or RA either (1) directly on the party's hardware or software KSM, or (2) in a Key generator that securely transfers the Key to the party's KSM, then proof of possession is not required.

3.2.2	Authentication of Organization Identity	Requests for Participant CA or Subscriber Certificates in the name of Subscribing Organization shall include the Organization name, address, and documentation of the existence of the Organization. The RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the Organization. **For Custodian-managed Certificates:** When performing Identification and Authentication of the Applicant of a Custodian-managed Certificate, the individual appointed by the Custodian as the Information System Security Officer (ISSO), and who will physically control the Subscriber Private Keys, must also be authenticated by the RA. Requests for Certificates that are not in the name of an Organization are unaffiliated.
3.2.3	Authentication of Individual Identity	Individual identity Certificates, including PIV-I Hardware Certificates shall only be Issued to human Subscribers.
3.2.3.1	Authentication of Human Subscribers	Individual identity Certificates, including PIV-I Hardware Certificates shall only be Issued to human Subscribers. For Applicants, the CA, RA, and/or associated Registration Agents (either CA, RA, LRA or TA) shall ensure that the Applicant's identity information is verified in accordance with the process established by this CP and the CA'S CPS. Process information shall depend upon the Assurance Level of the Certificate level and shall be addressed in the CA'S CPS or RA's RPS. The documentation and authentication requirements shall vary depending upon the level of assurance. For all Medium Assurances and PIV-I Assurances, identity shall be established no more than 30 days before initial Issuance of the Certificate. A Registration Agent shall record the information set forth below for Issuance of each Certificate: • The identity of the Registration Agent performing the identification; • A signed declaration by the Registration Agent that he or she

verified the identity of the Subscriber. This declaration shall use the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable format under local law. The signature on the declaration may be either a handwritten or Digital Signature using a Certificate that is of equal or higher level of assurance as the credential being Issued;

- A unique identifying number(s) from the ID(s) of the Registration Agent and Applicant (or some other trusted source of information on the Applicant), or a facsimile of the ID(s);
- The date and time of the verification; and
- A declaration of identity signed by the Applicant using a handwritten signature or appropriate Digital Signature and performed in the presence of the person performing the identity authentication using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

In those cases in which the Applicant is in possession of a valid Digital Signature credential of equal or higher Assurance Level or when the Certificate is generated immediately upon authentication of the Applicant's identity, the Applicant may Digitally Sign the declaration of identity using the digital credential. In the latter case, if the Applicant fails to Digitally Sign the declaration of identity then the Certificate shall be Revoked.

For All Levels: If an Applicant is unable to perform face-to-face Registration, the Applicant may be represented by a trusted person already Issued a Certificate of equal or higher Assurance Level than the Certificate being applied for by the Applicant. The trusted person will present information sufficient for Registration at the level of the Certificate being requested for the Applicant who the trusted person is representing.

For Basic and Medium Assurance Levels: An Individual certified by a State or Federal entity as being authorized to confirm identities may perform in-person authentication on behalf of the RA. The Individual forwards the information collected from the Applicant directly to the RA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data.

For PIV-I Certificates: The following biometric data shall be collected during the identity proofing and Registration process, and shall be formatted in accordance with [NIST SP 800-76]:

- An electronic facial image used for printing facial image on the

card, as well as for performing visual authentication during card usage. A new facial image shall be collected each time a card is Issued; and

- Two electronic fingerprints to be stored on the card for automated authentication during card usage.

The table below summarizes the identification requirements for each level of assurance.

Table 3 - Level of Assurance Identification Requirements

Assurance Level	**Identification Requirements**
Basic	Identity may be established by in-person proofing before a Registration Agent; or remotely verifying identity attribute information provided by Applicant and relied upon for identity proofing purposes through record checks either with the applicable agency, institution, or through credit bureaus or similar databases, and confirms that: name, Date of Birth ("DoB"), address, and other Applicant provided personal information in records are consistent with the application and sufficient to identify a unique Individual. Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the Applicant; or b) Issue credentials in a manner that confirms the ability of the Applicant to receive telephone communications at a number associated with the Applicant in records.
Medium Software Medium Software CBP Medium Hardware Medium Hardware CBP	Identity shall be established by in-person proofing before a Registration Agent. A trust relationship between the Registration Agent and the Applicant which is based on an in-person antecedent as described below may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., or one REAL ID Act compliant picture ID[1], or two Non-Federal Government I.D.s, one of which shall be a picture I.D. (e.g., Non-REAL ID Act compliant Driver's

(a) [1] REAL ID Act compliant IDs are identified by the presence of the DHS REAL ID star

Assurance Level	Identification Requirements
	License). Any credentials presented shall be unexpired.
PIV-I Hardware	Identity shall be established by in-person proofing before a Registration Agent. Credentials required are two identity source documents in original form. The identity source documents shall come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal Government-issued picture identification (ID). The use of an in-person antecedent is not applicable.

3.2.3.1.1 In-Person Antecedent

In-person Antecedent:

The requirement for antecedent is identical with the exception of using a historical in-person ID proofing event. Hence, a proposed antecedent process shall:

- Meet the thoroughness (rigor) of the in-person event;
- Provide supporting ID proofing artifacts or substantiate the Applicant through a relationship; and
- Bind the Applicant to asserted identity.

Two generic use cases have been identified as valid antecedent processes:

1. Sponsor Antecedent, where the Applicant, such as an employee, member, or associate has no reasonable access to a Registration Agent. The Sponsor will attest to the validity of the Individual through their on-going relationship, date of Antecedent Event and provide unique Applicant identity information to the Registration Agent. Applicant will be bound remotely with known attributes or shared-secrets.
2. Third-party Antecedent, where identity proofing is performed

by multiple parties, Sponsor, Registration Agent, and trusted third-party or IVP. In this model, the IVP collects the in-person proofing antecedent artifacts. Sponsor will attest to the validity of the Individual through their on-going relationship and provide unique Applicant identity information to the Registration Agent. Subscriber will be bound remotely with known attributes or shared-secrets. The date and supporting artifacts verifying the historical identity proofing event are provided to the Registration Agent. Trusted parties are required to have a contractual relationship with at least one other trusted party.

An antecedent process requires various actors, roles, responsibilities, and activities. These sections outline specific requirements for the process.

ID Proofing Relationships

- The Individual performing the identity proofing, IVP or Sponsor of the Applicant shall have a contractual relationship with the CA or RA represented by the Registration Agent.

- Sponsor or IVP shall have an established relationship with Subscriber. The relationship shall be sufficient enough to enable the authenticating Sponsor or IVP to, with a high degree of certainty, verify that the person seeking the PKI Certificate is the same person that was identity proofed.

- Sponsor's application shall contain a description of the relationship with Applicant describing the initial identity proofing or qualifications and the on-going relationship.

Antecedent In-person Identity Proofing Event

- Credentials required are one Federal Government-issued Picture ID, or one REAL ID Act compliant picture ID, or two Non-Federal Government IDs, one of which shall be a picture ID (e.g., Non-REAL ID Act compliant Driver's License). Any credentials presented shall be unexpired.

- The Sponsor or an Individual certified by a State or Federal entity as being authorized to confirm identities is required to obtain Applicant's signature. In all cases, the name of both the Sponsor and Individual confirming the identity's signature or auditable confirmation of identity proofing process is to be recorded.

Participant CA

- The RA shall record the date of the antecedent in-person

identity proofing event.

- The RA shall obtain any historical artifacts from the Antecedent Event.

- The date of the antecedent identity proofing event shall be the basis for determining the timeframe for the next identity Registration event required by Section 3.3.1 of this CP.

Information Source Requirements

- The antecedent process shall use information acquired from an Identity Verification Provider to identify an Applicant. When information is obtained through one or more information sources, an auditable, chain of custody shall be in place.

- The antecedent process shall require that all data received from Identity Verification Provider (including the antecedent) shall be validated, protected, and securely exchanged.

- All Participants shall store and exchange private information in a confidential and tamper evident manner, and protect from unauthorized access.

Binding the Certificate Request to the Identity

The process to bind the claimed identity to the specific Certificate request shall provide commensurate levels of assurance with the Certificate being Issued.

- A Sponsor for the Applicant shall provide the RA with initial contact information, (e.g., name, email address, phone number, Subscribing Organization).

- The PKI shall use the Sponsor provided information to contact the Applicant.

- Applicant, using a prescribed method, shall initiate the credentialing process by identifying themselves through a series of initial questions. At least one question shall be derived from private information occurring in the course of the in-person Antecedent Event. This identity binding process shall not be repeated in the event of failure.

- If successful, Applicant progresses to a second phase of questions. This on-line verification process shall be a set of additional (non-repetitive) questions. The system shall score the responses and determine the probability that the claim is or is not fraudulent.

3.2.3.2 Authentication Role-based Certificates identify a specific role on behalf of which the

	of Human Subscribers for Role-based Certificates	Subscriber is authorized to act rather than the Subscriber's name and are Issued in the interest of supporting accepted business practices. Role-based Certificates shall not be Issued under this CP.
3.2.3.3	Authentication of Human Subscribers for Group Certificates	A Group certificate corresponds to a credential with a Private Key that is shared by multiple Subscribers. Two different Group Certificate Types are defined under this CP and have differing authentication requirements: 1) **Group Device Software Certificates**. Group Domain-Bound Certificates assert only Organization name in the subjectName DN, which may be in the form of a group organizational level address. Group Certificates are by their nature Affiliated Certificates. Authentication requirements are: • 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; and, • The Device associated with Group Device Certificates must also be verified according to Section: 3.2.3.4 Authentication of Devices. 2) **Group Software Certificates**. Group Software Certificates assert Organization and may contain an address associated with a group member (Individual acting on behalf of the Organization) in the subjectName DN. Group Software Certificates are Affiliated Certificates. Authentication requirements are: • Organization authentication as described in Section 3.2.2; • Authentication of the Individual with whom the address is associated in accordance with Section 3.2.3.1 at a Medium Assurance Level; and • 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. 3) **Custodian-managed Certificates**. Custodian-managed Certificates (e.g. authorized third party) assert the Custodian and may contain the Organization. Custodian managed Certificates are by their nature Affiliated Certificates. Authentication requirements are:

- Issuer CA or RA shall also record the information identified in Section 3.2.3.1 for the Information Systems Security Officer (ISSO) (or equivalent) of the Custodian, before issuing the Certificate.
- The Custodian (e.g. authorized third party), ISSO or equivalent shall be 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 must 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 shall 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.

Users must be identity proofed at a level corresponding to the level of authority 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 level of authority of the associated Certificate.

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

- Group Software Signing 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).

Antecedent In-Person Identity Proofing Events may be used for

authentication of Group Certificates.

3.2.3.4 Authentication of Devices

Some computing and communications Devices (e.g., routers, firewalls, servers, etc.) may be named as Certificate subjects. In such cases, the Device shall be associated with a human Sponsor who is known as the Primary Machine Operator. The Primary Machine Operator is named in the Subscribing Organization Authorization Agreement during the Registration of the Device Certificate The Primary Machine Operator is an Individual responsible for providing the following Registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name);
- Equipment Public Keys;
- Equipment authorizations and attributes (if any are to be included in the Certificate);
- Contact information to enable the CA or RA to communicate with the Primary Machine Operator when required; and
- Designation of Secondary Machine Operators.

These Certificates shall be Issued only to Devices under the Primary Machine Operator's control (i.e., require Registration and validation that meets all issuing CA requirements, as well as requiring re-validation prior to being re-issued). In the case where the Primary Machine Operator is changed, the new Primary Machine Operator shall review the status of each Device under his or her responsibility to ensure it is still authorized to receive a Device Certificate. The CA's CPS shall describe procedures to ensure that Device Certificate accountability is maintained.

The Device Registration information shall be verified to an Assurance Level commensurate with the certificate Assurance Level being requested. For Certificates Issued with the Medium Device Software and Medium Device Hardware policies, Registration information shall be verified commensurate with the Medium Assurance Level. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of Digitally Signed messages sent from the Primary Machine Operator (using Certificates of equivalent or greater assurance than that being requested), and
- In person Registration of the Device by the Primary Machine Operator, including verification of the identity of the Primary Machine Operator as both an Individual and as associated with the Subscribing Organization as confirmed in accordance with the requirements of this CP 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

As a part of the Device Registration process, the Primary Machine Operator will be named in the Subscribing Organization Authorization Agreement.

	Machine Operator	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 initially designated in conjunction with the Device, then the Primary Machine Operator is also responsible to provide the names of all Secondary Machine Operators in the Secondary Machine Operators List, which is a part of the Subscribing Organization Authorization Agreement submitted at the time of Device Certificate Registration.
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, and will remain effective 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 in adherence with the IGC-CPS. Confirmation of Identity and Affiliation with Subscribing Organization is not required for Secondary Machine Operators.
3.2.4	Non-verified Subscriber Information	Information that is not verified shall not be included in Certificates.
3.2.5	Validation of Authority and Other Attributes	IdenTrust shall validate any CA Certificate Requestor's authorization to act in the name of the CA. Additionally, IdenTrust shall validate that the CA has been approved by the PMA based on successful compliance analysis of the CA's CPS. Certificates that assert affiliation shall be 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.

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

3.2.6 Criteria for Interoperation

A CA shall adhere to the following requirements:

- Operate a PKI that has undergone a successful compliance audit pursuant to Section 8 of this CP;
- Issue Certificates interoperable with the profiles described in this CP, and make Certificate status information available in compliance with this CP; and
- Provide CA Certificate and Certificate status information to the relying parties.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

In the event that a Participant CA Re-Key is required, a new Certificate will be Issued to the Participant CA by the Root CA. Before Issuance, the Participant CA shall identify itself through use of its current Signature Key or the initial Registration process. If it has been more than three years since the Participant CA was identified as required in Section 3.2, identity shall be re-established through the initial Registration process.

Subscribers of CAs shall identify themselves for the purpose of Re-Keying as required in table below.

Table 4 - Identification and Authentication for Routine Re-Key

Assurance Level	**Routine Re-Key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates**
Basic (all policies)	Identity may be established through use of a current (unexpired) Signature Key, except that identity shall be reestablished through initial Registration process at least once every nine years from the time of initial Registration.
Medium (all policies)	Identity may be established through use of current Signature Key, except that identity shall be established through initial Registration process at least once every nine years from the time of initial Registration. For IGC Medium Device Software and IGC Medium Device Hardware Certificates, identity may be established through the use of current Signature Key or using means commensurate with the strength of the Certificate being requested, except that identity shall be established through initial Registration process at least once every nine years from the time of initial Registration.
PIV-I Hardware (all	Identity may be established through use of the current Signature Key,

Assurance Level	Routine Re-Key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates
policies) PIV-I Card Authentication	except that identity shall be established through initial Registration process at least once every nine years from the time of initial Registration. 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.

When any current Signature Private Key Certificate is used for I&A purposes, the life of the new Certificate shall not exceed beyond the initial identity-proofing times specified in the paragraphs above and the Assurance Level of the new Certificate shall not exceed the Assurance Level of the Certificate being used for I&A purposes.

3.3.2	Identification and Authentication for Re-Key after Revocation	For Re-Key after Revocation, all Participants shall undergo the initial I&A processes specified in Sections 3 and 4 of this CP.

3.4 Identification and Authentication for Revocation Request

Revocation requests shall be authenticated. Requests to Revoke a Certificate may be authenticated using that Certificate's Public Key, regardless of whether or not the associated Private Key has been compromised.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENT

4.1 Certificate Application

IdenTrust, when operating as a CA participating in a cross-certified program (such as Federal Bridge, DirectTrust and SAFE SBCA) shall comply 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, Trusted Agents, and Applicants supporting the Certificate application and Issuance process shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the Certificates being Issued (i.e. communications supporting the Issuance of hardware assurance Certificates shall be protected using hardware assurance Certificates, or some other mechanism of equal or greater strength). Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the Certificates being Issued.

4.1.1	Submission of	Certificate application may be submitted to a CA or RA by the

	Certificate Application	Applicant, compliant Custodian (e.g. authorized third party), ISSO or the Subscribing Organization of the Applicant.
4.1.2	Enrollment Process and Responsibilities	The Applicant and the CA shall perform the following steps when an Applicant applies for a Certificate: • Obtain a functioning Public/Private Key Pair for each Certificate required; • Establish and record identity of Applicant (per Section 3.2); • Record the Applicant's basis for requesting a Certificate, including a point of contact for verification, if required; and • Provide a point of contact for verification of any roles or authorizations requested. All communications among PKI authorities supporting the Certificate application and Issuance process shall be authenticated and protected from modification. If databases or other sources are used to confirm Applicant attributes, then these sources and associated information sent to a CA shall require: • When information is obtained through one or more information sources, an auditable chain of custody from the information source to the CA be in place, and • All data received be protected and securely exchanged in a confidential and tamper evident manner, and protected from unauthorized access. Requests by CAs for CA Certificates shall be submitted to the PMA using the contact provided in Section 1.5.2. The PMA will evaluate the request for acceptability. At a minimum the CA's CPS shall have successfully completed a compliance analysis conducted by either the PMA or an independent party. The PMA shall only accept requests from an approved CA.

4.2 Certificate Application Processing

Information in Certificate applications shall 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	Upon receiving the Certificate application, the CA or RA shall verify the identity of the Applicant in accordance with Sections 3.2 and 3.3 of this CP: • Verify the authority of the Applicant and the integrity of the information in the Certificate request; • Generate and sign a Certificate, if all Certificate requirements have been met (in the case of a RA, have the CA sign the Certificate); and • Make the Certificate available to the Subscriber. The Certificate request may contain an already built ("to-be-signed")

		Certificate. Such a Certificate will not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction. Prior to Certificate Issuance, Applicant shall be required to agree to the requirements that they shall protect the Private Key and use the Certificate and Private Key for authorized purposes only.
4.2.2	Approval or Rejection of Certificate Applications	The CA or RA shall be responsible for: • Verifying the information is correct and accurate; • Ensuring the I&A requirements as defined in Section 3.1 and 3.2 of this CP have been followed; • Ensuring the application process requirements as defined in Sections 4.1 have been met; and • Approve or Reject the application.
4.2.3	Time to Process Certificate Applications	For all Medium Assurances and PIV-I Assurances, application processing from the time the complete Certificate application is posted on the CA or RA system to Certificate Issuance shall take no more than 30 days.

4.3 Certificate Issuance

4.3.1	CA and RA Actions During Certificate Issuance	The CA shall authenticate a Certificate request, ensure that the Public Key is bound to the correct Subscriber, obtain a proof of possession of the Private Key, ensure all fields and extensions are properly populated, then generate a Certificate, and finally provide the Certificate to the Subscriber. After generation and verification, the CA shall publish the Certificate to a Repository in accordance with this CP. Certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., LDAP, HTTP).
4.3.2	Notification to Subscriber of Certificate Issuance	A CA shall notify a Subscriber of Certificate Issuance.

4.4 Certificate Acceptance

4.4.1	Conduct Constituting Certificate Acceptance	Failure to object to the Certificate or its contents shall constitute Acceptance of the Certificate.
4.4.2	Publication of the Certificate by the CA	As specified in Section 2.2, all CA Certificates shall be published in publicly accessible Repository.

		Certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., LDAP, HTTP). This CP makes no other stipulation regarding publication of Subscriber Certificates.
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	The IdenTrust PMA and other relevant entities (e.g., PMAs of Cross-Certified entities) shall be notified upon Issuance of all CA Certificates. The process or requirement for notifying any other entities (e.g., PMAs of Cross-Certified entities) shall be specified in relevant agreements between the IdenTrust PMA or CA and other entity.

4.5 Key Pair and Certificate Usage

4.5.1	Subscriber Private Key and Certificate Usage	Subscribers or their authorized Custodian (e.g. other authorized third party) representatives, who take possession of their Private Key, shall protect it from access by unauthorized parties and shall use the Private Keys only as specified by the certificatePolicies and keyUsage extensions of the corresponding Certificate. The Subscriber shall not use the signature Private Key after the associated Certificate has been Revoked or has expired. The Subscriber may continue to use the decryption Private Key solely to decrypt previously encrypted information after the associated Certificate has been Revoked or has expired. Use of the Private Key shall be limited in accordance with the key usage extension in the Certificate. If the extended key usage extension is present and implies any limitation on the use of the Private Key, those constraints shall also be observed. For example, the OCSP Responder Private Key shall be used only for signing OCSP Responses.
4.5.2	Relying Party Public Key and Certificate usage	Relying Parties shall ensure that a Public Key in a Certificate is used only for the purposes indicated by the key usage extension, if the extension is present. If the extended key usage extension is present and implies any limitation on the use of the Certificate, those constraints shall also be followed.

4.6 Certificate Renewal

Renewing a Certificate consists of issuing a new Certificate with the same name, Key, and other information as the old Certificate, but with a new, extended Validity Period and a new serial number.

After Certificate renewal, the old Certificate may or may not be Revoked, but shall not be further Re-Keyed, renewed, or modified.

4.6.1	Circumstance for Certificate	A Certificate may be renewed if the Public Key has not reached the end of its Validity Period, the associated Private Key has not been compromised, and the Subscriber name and attributes are unchanged.

	Renewal	In addition, the Validity Period of the Certificate shall meet the requirements specified in Section 6.3.2. CA Certificates and Certificates related to a CA's PKI, such as OCSP Responder Certificates and Cross-Certificates may be renewed. Additionally, Device Certificates may be renewed. Human Subscriber Certificates shall not be renewed under this CP.
4.6.2	Who May Request Renewal	A CA or CSA Administrator may request renewal of CA and CA PKI component Certificates. The designated Primary Machine Operator of a Device Certificate may request renewal of Device Certificates.
4.6.3	Processing Certificate Renewal Requests	Certificate renewal identity-proofing shall be achieved using one of the following processes: • Initial Registration process as described in Section 3.2; or • I&A for Re-Key as described in Section 3.3, except the old Key can also be used as the new Key.
4.6.4	Notification of New Certificate Issuance to Subscriber	A CA shall notify Subscribers of Certificate Issuance.
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate	Failure to object to the Certificate or its contents shall constitute Acceptance of the Certificate.
4.6.6	Publication of the Renewal Certificate by the CA	As specified in Section 2.2, all CA Certificates shall be published in publicly accessible Repository. Certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., LDAP, HTTP). This CP makes no other stipulation regarding publication of Subscriber Certificates.
4.6.7	Notification of Certificate Issuance by the CA to other Entities	The IdenTrust PMA and other relevant entities (e.g., PMAs of Cross-Certified entities) shall be notified upon Issuance of all CA Certificates. The process or requirement for notifying any other entities (e.g., PMAs of Cross-Certified entities) shall be specified in relevant agreements between the IdenTrust PMA or CA and other entity.

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.

Subscribers shall identify themselves for the purpose of Re-Keying as required in Section 3.3.1.

After Certificate Re-Key, the old Certificate may or may not be Revoked, but shall not be further Re-Keyed, renewed, or modified.

4.7.1	Circumstance for Certificate Re-Key	A CA may Issue a new Certificate to the Subscriber when the Subscriber has generated a new Key Pair and is entitled to a Certificate.
4.7.2	Who May Request Certification of a New Public Key	A CA or CSA Administrator may request re-key of CA and CA PKI component Certificates. All Subscribers may request Certificate re-key.
4.7.3	Processing Certificate Re-keying Requests	See Sections 3.2 and 3.3.
4.7.4	Notification of New Certificate Issuance to Subscriber	A CA shall notify Subscribers of Certificate Issuance.
4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate	Failure to object to the Certificate or its contents shall constitute Acceptance of the Certificate.
4.7.6	Publication of the Re-keyed Certificate by the CA	As specified in Section 2.2, all CA Certificates shall be published in publicly accessible Repository. Certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., LDAP, HTTP).
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	The IdenTrust PMA and other relevant entities (e.g., PMAs of Cross-Certified entities) shall be notified upon Issuance of all CA Certificates. In the event a Cross-Certified CA is re-keyed, new Cross-Certificates shall be Issued to and requested from the entity with which the CA is Cross-Certified following procedures specified in relevant agreements between the entities. Before Issuance, both the CA and the Cross-Certifying CA shall identify itself through use of its current Signature Key or the initial registration process. If it has been more than three years since identification of the Cross-Certifying CA as required in Section 3.2, identity shall be re-established through the initial registration process.

4.8 Certificate Modification

Certificate modification consists of creating new Certificates with subject information (e.g., a name or email address) that differs from the old Certificate. For example, a CA may perform Certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new Certificate may have the same or different subject Public Key.

After Certificate modification, the old Certificate may or may not be Revoked, but shall not be further Re-Keyed, renewed, or modified.

4.8.1	Circumstance for Certificate Modification	A CA may Issue a new Certificate to the Subscriber when some of the Subscriber information has changed, (e.g., name change due to change in marital status, change in subject attributes, etc.), and the Subscriber continues to be entitled to a Certificate.
4.8.2	Who May Request Certificate Modification	A CA or CSA Administrator may request modification of CA and PKI component Certificates. All Subscribers may request Certificate modification. Additionally, CAs and, RAs and LRAs may request Issuance of modified Certificates.
4.8.3	Processing Certificate Modification Requests	Certificate modification identity-proofing shall require proof of all subject information changes be provided to the RA, LRA, or Trusted Agent and verified before the modified Certificate is Issued. Certificate modification identity-proofing shall be achieved using one of the following processes: • The Registration process as described in Section 3.2; or • I&A for re-key as described in Section 3.3, except the old Key can also be used as the new Key.
4.8.4	Notification of New Certificate Issuance to Subscriber	A CA shall notify Subscribers of Certificate Issuance.
4.8.5	Conduct Constituting Acceptance of Modified Certificate	Failure to object to the Certificate or its contents shall constitute Acceptance of the Certificate.
4.8.6	Publication of the Modified Certificate by the CA	As specified in Section 2.2, all CA Certificates shall be published in publicly accessible Repository. Certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories

(e.g., LDAP, HTTP).

This CP makes no other stipulation regarding publication of Subscriber Certificates.

4.8.7	Notification of Certificate Issuance by the CA to Other Entities	The IdenTrust PMA and other relevant entities (e.g., PMAs of Cross-Certified entities) shall be notified upon Issuance of all CA Certificates. The process or requirement for notifying any other entities (e.g., PMAs of Cross-Certified entities) shall be specified in relevant agreements between the IdenTrust PMA or CA and other entity.

4.9 Certificate Revocation and Suspension

Revocation and Suspension requests shall be authenticated. Requests to Revoke or suspend a Certificate may be authenticated using that Certificate's Public Key, regardless of whether or not the associated Private Key has been compromised.

All CAs shall publish CRLs.

4.9.1	Circumstances for Revocation	A Certificate shall be Revoked when the binding between the Subject and the Subject's Public Key defined within a Certificate is no longer considered valid. Examples of circumstances that invalidate the binding include, but are not limited to: • 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, Issuer or Member Agreement, or the stipulations of this CP; • Private Key is compromised or is suspected of compromise; • The PMA or CA suspects or determines that Revocation of a Certificate is in the best interest of the integrity of the PKI; • Certification of the Subject is no longer in the interest of the Issuer; • Subscriber or other authorized agent (as defined in the CA's CPS) asks for his/her Certificate to be Revoked; • Subscriber no longer holds one or more of any authorizations explicitly stated in the Certificate; • Termination of the service agreement held between the Subscriber and the Custodian that holds the Private Key ends; or • The Subscriber Custodian, or RA requests Certificate revocation. For Certificates that express an Organizational affiliation, CAs shall require that the Organization shall inform the CA of any changes in the Subscriber affiliation. If the Subscribing Organization no longer authorizes the affiliation of a Subscriber, the CA shall Revoke any Certificates Issued to that Subscriber containing the affiliation. If an

Organization terminates its relationship with a CA such that it no longer provides affiliation information, the CA shall Revoke all Certificates affiliated with that Organization.

Whenever any of the above circumstances occur, the associated Certificate shall be Revoked and Certificate Revocation status placed on a CRL. Revoked Certificates shall be included on all new publications of the Certificate status information until the Certificates expire. Revoked Certificates shall appear on at least one CRL.

4.9.2	Who Can Request Revocation	A Subscriber, their Subscribing Organization, the RA, or the issuing CA may request Revocation of Subscriber Certificates at any time for any reason. The Primary Machine Operator named as the Subscriber for the Device Certificate to be Revoked may request the Revocation of Device Certificates An individual who is name on the current version of the Secondary Machine Operator List which is archived as a part of the Device Certificate account record of a Device Certificate may request the Revocation of Device Certificates. A RA may request Revocation of their RA Certificate. An operator of a CMS may request Revocation of a CMS Certificate or Content Signing Certificate. An Authorizing Official of a CA may request Revocation of their CA Certificate. 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	A request to Revoke a Certificate shall identify the Certificate to be Revoked, explain the reason for Revocation, and allow the request to be authenticated (e.g., digitally or manually signed). Upon receipt of a Revocation request, a CA shall authenticate the request and then Revoke the Certificate. If an RA performs this function on behalf of the CA, the RA shall send a message to the CA requesting Revocation of the Certificate. The RA shall digitally or manually sign the message. The message shall be in a format known to the CA. Upon receipt of a Revocation request from an RA, a CA shall authenticate the request and then Revoke the Certificate. For PIV-I Assurance Levels, CAs shall directly or through a delegate collect and destroy PIV-I cards from Subscribers whenever the cards are no longer valid, whenever possible. CAs shall record destruction of PIV-I cards. Upon receipt of a Revocation request from a CA asking that a Certificate Issued by the IGC Root CA be Revoked, IdenTrust shall authenticate the request, apprise the IdenTrust PMA, and then take whatever action the PMA directs. Separate from the publication of the Revocation

		information, prompt oral or electronic notification of a CA Revocation shall be given by IdenTrust to previously designated agents in all Organizations having a CA to which IGC Root CA has Issued a Certificate.
4.9.4	Revocation Request Grace Period	There is no Revocation grace period. In the case of Key compromise, Subscribers are required to request Revocation within one hour. For all other reasons, Subscribers are required to request Revocation within 24 hours.
4.9.5	Time Within Which CA Must Process the Revocation Request	CAs will Revoke Certificates as quickly as practical upon receipt of a proper Revocation request. Excepting those requests validated within two hours of CRL issuance, Revocation requests shall be processed before the next CRL is published. Revocation requests validated within two hours of CRL issuance shall be processed before the subsequent CRL is published.
4.9.6	Revocation Checking Requirements for Relying Parties	Use of Revoked Certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new Revocation data should be obtained is a determination to be made by the Relying Party. If it is temporarily infeasible to obtain Revocation information, then the Relying Party shall either reject use of the Certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a Certificate whose authenticity cannot be guaranteed.
4.9.7	CRL Issuance Frequency	**Subordinate or Participant CA** Subordinate and Participant CAs shall generate and publish a CRL no less than once every 24 hours. In case of Key compromise or Revocation of any Certificate issued by the Participant CA for any reason, the Participant CA shall publish a CRL within 18 hours of notification. **Root CA** IdenTrust shall publish the CRL for Certificates Issued by the IGC Root CA at least every 31 days. In the case of CA compromise or Key compromise, IdenTrust shall publish an emergency CRL within 18 hours of notification. **All CAs** All CAs shall publish to Repository a new CRL prior to the time specified in the nextUpdate field of the active CRL. Upon publishing of a new CRL, the Root CA and Participant CA shall remove any and all old CRLs published in the Repository.
4.9.8	Maximum Latency of CRLs	CRLs shall be published within 4 hours of generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously published CRL for same scope.
4.9.9	Online Revocation / Status Checking	CAs may support on-line Revocation/status checking. For PIV-I Assurance Levels, CAs shall support on-line status checking via OCSP using the CA-delegated trust model specified in RFC 6960. If on-line Revocation/status checking is supported by a CA, the latency

	Availability	of Certificate status information distributed on-line by the CA or its delegated status responders shall meet or exceed the requirements for CRL issuance stated in 4.9.7.
4.9.10	Online Revocation Checking Requirements	Unless specified in Section 4.9.9, CAs are not required to provide OCSP based Revocation checking.
4.9.11	Other Forms of Revocation Advertisements Available	A CA may also use additional methods to publicize the Certificates it has Revoked. Any alternative method shall meet the following requirements: • The alternative method shall be described in the CA's approved CPS, and • The alternative method shall provide authentication and integrity services commensurate with the Assurance Level of the Certificate being verified. • The alternative method shall meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.
4.9.12	Special Requirements Related to Key Compromise	In the event of a CA or Subscriber Private Key compromise or loss, a CRL shall be published at the earliest feasible time. At a minimum, a CRL shall be published according to the requirements in Section 4.9.7.
4.9.13	Circumstances for Suspension	Suspension shall be permitted for all Certificates types Issued by IGC-CP CAs. The most common reason for Certificate suspension is as an interim action prior to Certificate Revocation. Examples of possible circumstances include but are not limited to when a Key compromise is suspected but not known to be true, or if a Revocation request cannot be properly validated.
4.9.14	Who Can Request Suspension	A Subscriber, their Subscribing Organization, or the issuing Participant CA may request Suspension of Subscriber Certificates at any time for any reason. The Primary Machine Operator named as the Subscriber for the Device Certificate to be Suspended may request the Suspension of Device Certificates An individual who is name on the most current version of the Secondary Machine Operator List which is archived as a part of the Device Certificate account record of a Device Certificate may request the Suspension of Device Certificates. An Authorizing Official of a Participant CA may request suspension of their CA Certificate.
4.9.15	Procedure for Suspension Request	A request to suspend a Certificate shall identify the Certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated (e.g., digitally or manually signed). Upon receipt of a suspension request, a CA shall authenticate the request and then suspend the Certificate.

If an RA performs this function on behalf of the CA, the RA shall send a message to the CA requesting suspension of the Certificate. The RA shall digitally or manually sign the message. The message shall be in a format known to the CA. Upon receipt of a suspension request from an RA, a CA shall authenticate the request and then suspend the Certificate.

Upon receipt of a suspension request from a Participant CA asking that a Certificate Issued by the IGC Root CA be suspended, IdenTrust shall authenticate the request, apprise the IdenTrust PMA, and then take whatever action the PMA directs. Separate from the publication of the Revocation information, prompt oral or electronic notification of a Participant CA suspension shall be given by IdenTrust to previously designated agents in all Organizations having a Participant CA to which IGC Root CA has Issued a Certificate.

4.9.16	Limits on Suspension Period	A Certificate may be suspended for a maximum of 14 days. If the Subscriber or LRA has not removed their Certificate from hold (suspension) within that period, the Certificate shall be Revoked for reason of "Key Compromise". In order to mitigate the threat of unauthorized person removing the Certificate from hold, the Subscriber identity shall be authenticated: • In person using initial identity proofing process described in Section 3.2.3; • By sending a digitally signed message with a valid, unexpired Certificate of an equal or higher Assurance Level than the suspended Certificate, which was Issued under the IGC PKI to the same Individual seeking suspension removal; or • Via a Client-authenticated SSL/TLS-Encrypted Session using a Certificate of an equal or higher Assurance Level than the suspended Certificate, which was Issued under the IGC PKI to the same Individual seeking suspension removal. In the instance a Certificate is used for proof of identity, the CA or RA shall ensure the request is authenticated and verify the Certificate Subject is the same as in the suspended Certificate.

4.10 Certificate Status Services

CAs shall support CRLs for Certificate status advertisement. CAs may support OCSP for Certificate status advertisement.

4.10.1	Operational Characteristics	No stipulation.
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.
4.10.3	Optional	No stipulation.

Features

4.11 End of Subscription

Certificates that have expired prior to or upon end of subscription are not required to be Revoked. Unexpired CA Certificates shall always be Revoked at the end of subscription.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Private Keys of CA, CSA, RA Certificates and PIV-I Content Signing Certificates may not be escrowed. Private Keys of Subscriber Signature Certificates may not be escrowed.

Issuing CAs may escrow copies Private Keys of Subscriber Encryption Certificates to provide key recovery services. Such Private Keys shall be encrypted and protected with at least the level of security used to generate and deliver the Private Key. Controls shall be in place to prevent unauthorized access to escrowed Private Keys.

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 requests 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.

When Private Keys of Subscribers are escrowed, the CA, and where applicable the RA shall:

- Notify Subscribers that their Private Keys are escrowed;
- Protect Keys in escrow from unauthorized disclosure;
- Protect any authentication mechanisms or Key encrypting Keys maintained for the purpose of recovering Private Keys that are escrowed;
- Release escrowed Keys only for properly authenticated requests meeting one of the conditions stated in this Section; and
- Comply with any legal obligations to disclose and keep confidential escrowed Keys, escrowed Key-related information, or the facts concerning any key recovery request or process.

CAs may escrow Private Keys within a Key escrow database on the premise of and in a database belonging to a third party RA operating a CMS. In such

cases escrowed Private Keys shall be encrypted and protected in a manner that requires involvement of both the CA and RA for Key recovery.

Key escrow and recovery practices shall be described in the CA'S CPS and when recovery involves both a CA and RA, also the RA'S RPS. Documents describing Key recovery practices shall be publicly posted.

CAs that support session Key encapsulation and recovery shall identify the document describing the practices.

4.12.2	Session Key Encapsulation and Recovery Policy Practices	CAs that support session Key encapsulation and recovery shall identify the document describing the practices.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

CAs and RAs shall impose physical security requirements specified in Section 5.1.2. All equipment shall be protected from unauthorized access while a KSM is installed and activated. Physical Access Controls shall be implemented to reduce the risk of equipment tampering even when the KSM is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the PKI environment.

Unauthorized use of CA, CSA, CMS, and RA equipment is forbidden. Physical security controls shall be implemented that protect the CA, CSA, CMS, and RA hardware and software from unauthorized use. CA, CSA, CMS, and RA KSMs shall be protected against theft, loss, and unauthorized use.

5.1.1	Site Location and Construction	The location and construction of the facility that will house CA, CSA, CMS, and RA equipment and operations shall be in accordance with that afforded the most sensitive business and financial information.
5.1.2	Physical Access	The CA, CSA, CMS, and RA equipment shall always be protected from unauthorized access. The equipment shall be protected from unauthorized access while the KSM is installed and activated. Physical Access Controls shall be implemented to reduce the risk of equipment tampering even when the KSM is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the equipment environment. The physical security mechanisms for CAs, CSAs, CMSs, and RAs shall be in place to: • Permit no unauthorized access to the hardware; • Store all removable media and paper containing sensitive plain-text information in secure containers; • Monitor, either manually or electronically, for unauthorized intrusion at all times; • Maintain and periodically inspect an access log; • Require two person physical access control to both the KSM and computer system; and

- At a minimum, provide three layers of increasing security such as perimeter, building, and CA room.

Removable KSMs shall be inactivated prior to storage. When not in use, removable KSMs and activation information used to access or enable KSMs used by CAs, CSAs, CMSs, and RAs shall be placed in secure containers. Activation Data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the KSM, and shall not be stored with the KSM.

In addition, LRA equipment shall be protected from unauthorized access while LRA's KSM is installed and activated. The LRA shall implement physical Access Controls to reduce the risk of equipment tampering even when the KSM is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the LRA equipment environment.

A security check of the facility housing the CA, CSA, or CMS equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that KSMs are in place when "open", and secured when "closed");
- For off-line CAs and CMSs, all equipment other than the PKI Repository is shut down;
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

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

The facility that houses the CA, CSA, CMS, Repository, and RA equipment shall be supplied with power and air conditioning sufficient to create a reliable operating environment.

5.1.3	Power and Air Conditioning	The CA, CSA, CMS, Repository, and RA equipment shall have backup power and cooling system capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories shall be provided with uninterrupted power sufficient for a minimum of six hours operation in the absence of commercial power, to support continuity of operations.
5.1.4	Water Exposures	Commercial best practices to mitigate the risks of water damage shall be used for the CA, CSA, CMS and RA equipment.

5.1.5	Fire Prevention and Protection	Commercial best practices for fire prevention and protection shall be used for the CA, CSA, CMS and RA equipment.
5.1.6	Media Storage	Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access. Media that contains security audit, archive, or backup information shall be stored in a location separate from the equipment. Media used to collect or transmit information discussed in Section 9.4 shall be destroyed, such that the information is unrecoverable, prior to disposal. All other types of sensitive information shall be disposed of in a secure fashion.
5.1.7	Waste Disposal	Media used to collect or transmit information discussed in Section 9.4 shall be destroyed, such that the information is unrecoverable, prior to disposal. All other types of sensitive information shall be disposed of in a secure fashion.
5.1.8	Off-site Backup	System backups, sufficient to recover from system failure, shall be made on a periodic schedule for CA, CMS and RA systems. Backups shall be performed and stored off-site not less than once every 7 days, unless the system is off-line, in which case it shall be backed up whenever it is activated or every 7 days, whichever is later. At least one full backup copy shall be stored at an offsite location (separate from the equipment). Only the latest backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational system.

5.2 Procedural Controls

5.2.1	Trusted Roles	A Trusted Role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles shall be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the Root and Participant CAs. . Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. • The following roles shall be fulfilled by Individuals that have met the requisite requirements for a Trusted Role: • CA Administrator: authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate and backup component Keys. • CA Agent: authorized to request or approve Certificates, or

Certificate Revocations.

- CA Auditor: authorized to view and maintain CA audit logs.
- CA Operator: authorized to perform system backup and recovery.
- CSA Administrator: authorized to configure and operate the CSA.
- CSA Auditor: authorized to view and manage CSA audit logs.
- CMS Administrator: authorized to configure and operate the CMS.
- CMS Auditor: authorized to view and manage CMS audit logs.
- CMS Operator: authorized to perform system backup and recovery.

The following sections define these and other Trusted Roles.

5.2.1.1 Certification Authority ("CA") Roles

The **CA Administrator** role responsibilities are as follows:

- Installation and configuration of the CA software;
- Installation and configuration of Repository software;
- Establish CA System accounts;
- Configuration of Certificate profiles, templates, and audit parameters; and
- Root CA and Sub CA Key management including generation and/or destruction.

CA Administrators do not Issue Certificates to Subscribers.

The **CA Agent** role responsibilities are as follows:

- Registering new Subscribers and requesting the Issuance of Certificates;
- Verifying the identity of Subscribers and accuracy of information included in Certificates;
- Approving and executing the Issuance of Certificates; and
- Requesting, approving and executing the Revocation of Certificates.

The **CA Auditor** role responsibilities are as follows:

- Reviewing, maintaining, and archiving CA audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS.

The **CA Operator** role responsibilities are as follows:

- Routine operations of the CA equipment; and
- System backups and restore, and recovery or changing of recording media.

5.2.1.2 Certification Status Authority ("CSA") Roles

The **CSA Administrator** role responsibilities are as follows:

- Installation, configuration, and maintenance of the CSA;
- Establishing and maintaining CSA system accounts;
- Configuration of CSA software and audit parameters; and
- Generating and backing up CSA Keys.

The **CSA Auditor** role responsibilities are as follows:

- Reviewing, maintaining, and archiving CA audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS.

5.2.1.3 Card Management System ("CMS") Roles

The **CMS Administrator** role responsibilities are as follows:

- Installation, configuration, and maintenance of the CMS;
- Establishing and maintaining CMS accounts;
- Configuring CMS application and audit parameters; and
- Generating and backing up CMS Keys.

The **CMS Auditor** role responsibilities are as follows:

- Reviewing, maintaining, and archiving audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CMS is operating in accordance with its CPS.

The **CMS Operator** role responsibilities are as follows:

- The routine operation of the CMS equipment; and
- Operations such as system backups and recovery or changing recording media.

5.2.1.4 Registration Authority ("RA") Administrator

The **RA Administrator** responsibilities are:

- Verifying identity, either through personal contact, or via LRA or Trusted Agents;
- Entering Subscriber information, and verifying its correctness;
- Securely communicating requests to and responses from the CA; and
- Receiving and distributing Subscriber Certificates.

5.2.1.5 Local

The **LRA** responsibilities are:

	Registration Authority ("LRA")	• Verifying identity, either through personal contact, or via Trusted Agents; • Entering Subscriber information, and verifying correctness; • Securely communicating requests to and responses from the CA and RA; and • Receiving and distributing Subscriber Certificates. An LRA is authorized by a RA to serve a limited population of Subscribers, based on logical or geographical Organization.
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.
5.2.2	Number of Persons Required per Task	Proper procedural and operational mechanisms shall be 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 and CMS Private Keys throughout the entire Key lifecycle from generation and activation, into secure storage, into backup, and through to eventual destruction; • Non-automated (manual) Certificate Issuance processes; and • PIV-I Content Signing Key lifecycle from generation and activation, into secure storage, into backup, and through to eventual destruction. The IGC 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. For activities and tasks requiring principles of Separation-of-Duties/Multi-party Control, at least one of the Participants shall be an Administrator. All Participants shall serve in a Trusted Role as defined in Section 5.2.1. Principles of Separation-of-Duties/Multi-party Control shall not be achieved using personnel that serve in CA Auditor, CSA Auditor or CMS Auditor roles.
5.2.3	Identification and Authentication for Each Role	An Individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity. Trusted Roles who operate a CMS shall be allowed CMS access only when authenticated using a Certificate than has an equal or higher Assurance Level than the highest Assurance Level Certificate Issued by that CMS.

5.2.4 Roles Requiring Separation of Duties

Role separation, when required as set forth below, may be enforced either by the CA, CSA or CMS equipment, procedurally, or by combination of different means.

Individual personnel shall be specifically designated to the roles defined in Section 5.2.1 above. Individuals may assume more than one role subject to the following limitations:

- Individuals assigned a CA Agent role may not assume a CA Administrator or CA Auditor role; and

An Individual assigned a CA, and/or CSA and/or CMS Auditor role shall not perform any other Trusted Role except CA and/or CSA and/or CMS Auditor.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

A group of Individuals responsible and accountable for the operation of each CA, CSA and CMS shall be identified. The Trusted Roles of these Individuals per Section 5.2.1 shall be identified. All persons filling Trusted Roles shall be selected on the basis of loyalty, trustworthiness, and integrity. Trusted Roles responsible and accountable for the operation of the CA, CMS, CSA and RA shall be subject to background investigation. Personnel appointed to Trusted Roles (including CA Trusted Roles, CSA Trusted Roles, CMS Trusted Roles, RA Administrator, and LRA) shall:

- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere or conflict with their duties for the Trusted Role;
- Have not been previously relieved of duties for reasons of negligence or nonperformance of duties;
- Have not been denied a security clearance, or had a security clearance Revoked;
- Have not been convicted of a felony offense; and
- Be appointed in writing by an approving authority.

For PKIs operated at a Medium Software or Medium Hardware Assurance Level, each person filling a Trusted Role shall satisfy at least one of the following requirements:

- The person shall be a citizen of the country where the CA is located;
- For PKIs operated on behalf of multinational governmental Organizations, the person shall be a citizen of one of the member countries;
- For PKIs located within the European Union, the person shall be a

citizen of one of the member states of the European Union;

- 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 the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32; or
- For RA Administrator, LRAs and personnel appointed to the Trusted Roles for the CSAs, in addition to the above, the person may be a citizen of the country where the function is located.

For PKIs operated at Basic, Medium Software CBP and Medium Hardware CBP Assurance Levels, there is no citizenship requirement or security clearance specified.

5.3.2 Background Check Procedures

Personnel appointed to Trusted Roles (including CA Trusted Roles, CSA Trusted Roles, CMS Trusted Roles, LRAs, and RA Administrators) shall, at a minimum, pass a background investigation covering the following areas:

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

The period of investigation shall cover at least the last five years for each area, excepting the residence check which shall cover at least the last three years. Regardless of the date of award, the highest educational degree shall be verified. Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with U.S. Executive Order 12968 August 1995, or equivalent.

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

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

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 shall be conducted in the following areas: • CA/CSA/CMS/RA security principles and mechanisms; • Use and operation of all PKI associated equipment; • All PKI software versions in use on the CA system; • All PKI duties an Individual is expected to perform; and • Disaster recovery and business continuity procedures. Documentation shall be maintained identifying all personnel who received training and the level of training completed.
5.3.4	Retraining Frequency and Requirements	Individuals responsible for Trusted Roles shall be aware of changes in the CA, CSA, CMS, RA, or LRA operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, RA, LRA software upgrades, changes in automated security systems, and relocation of equipment. Documentation shall be maintained identifying all personnel who received training and the level of training completed.
5.3.5	Job Rotation Frequency and Sequence	Job rotation shall be implemented when in the judgment of management it is necessary to ensure the continuity and integrity of the CA or RA's ability to continually provide PKI-related services, but is not required at any specific frequency.
5.3.6	Sanctions for Unauthorized Actions	The entity PMA and IdenTrust shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions not permitted by this CP, IGC-CPS and any applicable RPS.
5.3.7	Contracting Personnel Requirements	Contractor personnel employed to perform functions pertaining to the CA or RA shall be subject to all the requirements of this CP including Section 5.3 and subsections thereof.
5.3.8	Documentation Supplied to Personnel	The CA or RA shall make available to its personnel applicable CPs, CPS, RPS, technical documentation, relevant system manuals, system operations documents, operations procedures documents and any relevant statutes, policies or contracts required to fulfilling their role responsibilities.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CA, CSA, CMS and RA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, a paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with retention period for archive, Section 5.5.2.

5.4.1 Types of Events Recorded

All security auditing capabilities of the CA, CSA, CMS and RA operating systems, and application Components required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. An "X" in a table cell indicates that the respective component (CA, CSA, CMS, RA) shall record the indicated type of auditable event. A "-" in a table cell indicates that the respective Component need not record the indicated type of auditable event. An "N/A" in a table cell indicates the event is not applicable. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;
- A success or failure indicator for the event, and
- The identity of the entity that caused the event.

Table 5 - Auditable Events

AUDITABLE EVENT				
SECURITY AUDIT	**CA**	**CMS**	**CSA**	**RA**
Any changes to the audit parameters (e.g., audit frequency, type of event audited)	X	X	X	X
Any attempt to delete or modify the audit logs	X	X	X	X
Obtaining a third-party time-stamp	N/A	N/A	N/A	N/A
IDENTITY PROOFING	**CA**	**CMS**	**CSA**	**RA**
Successful and unsuccessful attempts to assume a role	X	X	X	X
The value of maximum number of authentication attempts is changed	X	X	X	X
Maximum number of authentication attempts occur during user log in	X	X	X	X
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X	X
An administrator changes the type of authenticator (e.g., from a password to a biometric)	X	X	X	X
LOCAL DATA ENTRY	**CA**	**CMS**	**CSA**	**RA**
All security-relevant data that is entered in the system	X	X	X	X
REMOTE DATA ENTRY	**CA**	**CMS**	**CSA**	**RA**
All security-relevant messages that are received by the system	X	X	X	X
DATA EXPORT AND OUTPUT	**CA**	**CMS**	**CSA**	**RA**
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X	X

AUDITABLE EVENT				
KEY GENERATION	**CA**	**CMS**	**CSA**	**RA**
Whenever the component generates a Key (not mandatory for single session or one-time use symmetric Keys)	X	X	X	X
PRIVATE KEY LOAD AND STORAGE	**CA**	**CMS**	**CSA**	**RA**
The loading of Component Private Keys	X	X	X	X
All access to Certificate subject Private Keys retained within the CA for Key recovery purposes	X	X	N/A	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION, AND STORAGE	**CA**	**CMS**	**CSA**	**RA**
All changes to the trusted component Public Keys, including additions and deletions	X	X	X	X
SECRET KEY STORAGE	**CA**	**CMS**	**CSA**	**RA**
The manual entry of secret Keys used for authentication	X	X	X	X
PRIVATE AND SECRET KEY EXPORT	**CA**	**CMS**	**CSA**	**RA**
The export of private and secret Keys (Keys used for a single session or message are excluded)	X	X	X	X
CERTIFICATE REGISTRATION	**CA**	**CMS**	**CSA**	**RA**
All Certificate requests	X	X	N/A	X
CERTIFICATE REVOCATION	**CA**	**CMS**	**CSA**	**RA**
All Certificate Revocation requests	X	X	N/A	X
CERTIFICATE STATUS CHANGE APPROVAL	**CA**	**CMS**	**CSA**	**RA**
The approval or rejection of a Certificate status change request	X	X	N/A	N/A
COMPONENT CONFIGURATION	**CA**	**CMS**	**CSA**	**RA**
Any security-relevant changes to the configuration of a component system	X	X	X	X
ACCOUNT ADMINISTRATION	**CA**	**CMS**	**CSA**	**RA**
Roles and users are added or deleted	X	X	-	-
The access control privileges of a user account or a role are modified	X	X	-	-
CERTIFICATE PROFILE MANAGEMENT	**CA**	**CMS**	**CSA**	**RA**
All changes to the Certificate Profile	X	X	N/A	N/A
CERTIFICATE STATUS AUTHORITY MANAGEMENT	**CA**	**CMS**	**CSA**	**RA**
All changes to CSA profile (e.g., OCSP profile)	N/A	N/A	X	N/A
REVOCATION PROFILE MANAGEMENT	**CA**	**CMS**	**CSA**	**RA**
All changes to the Revocation profile	X	N/A	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	**CA**	**CMS**	**CSA**	**RA**
All changes to the Certificate Revocation List profile	X	N/A	N/A	N/A

AUDITABLE EVENT				
MISCELLANEOUS	**CA**	**CMS**	**CSA**	**RA**
A message from any source received by the CA requesting an action related to the operational state of the CA	X	-	-	-
Appointment of an Individual to a Trusted Role	X	X	X	X
Appointment of an Individual to a multi-person Role	X	X	-	N/A
Installation of the Operating System	X	X	X	X
Installation of the PKI Application	X	X	X	X
Installation of Hardware KSMs	X	X	X	X
Removal of KSMs	X	X	X	X
System Startup	X	X	X	X
Logon attempts to PKI application	X	X	X	X
Receipt of hardware / software	X	X	X	X
Attempts to set passwords	X	X	X	X
Attempts to modify passwords	X	X	X	X
Back up of the internal CA database	X	X	-	-
Restoration from back up of the internal CA database	X	X	-	-
File manipulation (e.g., creation, renaming, moving)	X	-	-	-
Posting of any material to a Repository	X	-	-	-
Access to the internal CA database	X	-	X	-
All Certificate compromise notification requests	X	X	N/A	X
Loading KSMs with Certificates	X	X	N/A	X
Shipment of KSMs	X	X	N/A	X
Zeroizing KSMs	X	X	N/A	X
Re-Key of the Component	X	X	X	X
CONFIGURATION CHANGES	**CA**	**CMS**	**CSA**	**RA**
Hardware	X	X	X	-
Software	X	X	X	X
Operating System	X	X	X	X
Patches	X	X	X	-
Security Profiles	X	X	X	X
PHYSICAL ACCESS / SITE SECURITY	**CA**	**CMS**	**CSA**	**RA**
Personnel Access to room housing to component	X	X	-	-
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	-

AUDITABLE EVENT				
Known or suspected violations of physical security	X	X	X	X
ANOMALIES	**CA**	**CMS**	**CSA**	**RA**
Software error conditions	X	X	X	X
Software check integrity failures	X	X	X	X
Receipt of improper messages	X	X	X	X
Misrouted messages	X	X	X	X
Network attacks (suspected or confirmed)	X	X	X	X
Equipment failure	X	X	-	-
Electrical power outages	X	X	-	-
Uninterruptible Power Supply (UPS) failure	X	X	-	-
Obvious and significant network service or access failures	X	X	-	-
Violations of Certificate Policy	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X
Resetting Operations System clock	X	X	X	X

5.4.2 Frequency of Processing Log

Audit logs from the CA, CSA, CMS, and RA shall be reviewed at least once every thirty days. At a minimum, a statistically significant set of security audit data generated by the Component since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. The analysis shall document and explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below. The Individual who removes audit logs from the component shall comply with the role separation requirements of Section 5.2.4. The Individual who removes audit logs from a CA, CSA, or CMS system shall be an official different from the Individuals who, in combination, command the Private Signing Key of that system.

For RA, a System Administrator other than the RA Administrator shall be responsible for managing the audit logs.

5.4.4 Protection of

Component system configuration and operating procedures shall ensure

	Security Audit Data	that: • Only CA Auditors, CSA Auditors and CMS Auditors may have read access to the logs; • Only authorized people may archive audit logs; and • Audit logs are not modified. The Individual performing audit log archive need not have modify access, but procedures shall be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion may require modification access). Audit logs shall be moved to a safe, secure storage location separate from the location where the data was generated.
5.4.5	Security Audit Data Backup Procedures	Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site on a monthly basis.
5.4.6	Security Audit Collection system (internal vs. external)	The audit log collection system may or may not be external to a component. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the PMA (or comparable policy management entity) shall be notified, and a determination shall be made to suspend the component operation until the problem is remedied.
5.4.7	Notification to Event-Causing Subject	This CP imposes no requirement to provide notice that an event was audited to the Individual, Organization, Device, or application that caused the auditable event.
5.4.8	Vulnerability Assessments	The Auditor shall perform routine assessments for evidence of malicious activity and vulnerability self-assessments of security controls. Security audit data shall be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors shall check for continuity of the security audit data.

5.5 Records Archival

CA, CSA, CMS, and RA archive records shall be sufficiently detailed to establish the proper operation of the component or the validity of any Certificate (including those Revoked or expired) Issued by the CA. All entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.

5.5.1	Types of Records Archived	At a minimum, the following data shall be recorded for archive across all Assurance Levels:

Table 6 - Data to Be Archived

Data To Be Archived	CA	CSA	CMS	RA
CA accreditation (if applicable)	X	-	-	-
Certificate Policies	X	X	X	-
Certification Practice Statement	X	X	X	X
Contractual Obligations	X	X	X	X
Other agreements concerning CA/CSA/CMS/RA operations	X	X	X	X
System and equipment configuration	X	X	X	X
Modifications and updates to system or configuration	X	X	X	X
Certificate requests	X	-	X	X
All Certificates Issued or published	X	-	X	-
Record of Re-Key (of CA/CSA/CMS/RAs KSM)	X	X	X	X
Security audit data (as specified in Section 5.4.1)	X	X	X	X
Revocation requests	X	-	X	X
Subscriber identity authentication data (per Section 3.2)	X	-	X	X
Subscriber agreements	X	-	X	X
Documentation of receipt and Acceptance of Certificates	X	-	X	X
Documentation of receipt of Subscriber's KSM	-	-	X	X
Documentation of receipt of KSMs (CA/CSA/CMS/RA)	X	X	X	X
All CRLs issued and/or published	X	X	-	-
OCSP Requests and Responses	-	X	X	-
Other data or applications to verify archive contents	X	X	X	X
Compliance Auditor reports	X	X	X	X
Remedial action taken as a result of violations of physical security	X	X	X	X

5.5.2 Retention Period for Archive

The minimum retention periods for archive data shall be no less than 10 years and 6 months.

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

5.5.3 Protection of Archive

Only authorized Individuals shall be permitted to add to or delete from the archive. The archived records may be moved to another medium when authorized by the Auditor. For the CA, CSA, and CMS, the authorized Individuals are CA, CSA, or CMS Administrators. For the RA, authorized Individuals are persons other than the RA Administrator

		(e.g., Information Assurance Officer or IAO). The contents of the archive shall not be released except as determined by the PMA, CA, or as required by law and in accordance with Sections 9.3 & 9.4 of this CP. Records and material information relevant to use of, and reliance on the Certificates Issued by CAs governed by this policy shall be archived. Archive media shall be stored in a safe, secure storage facility separate from the component (CA, CSA, CMS, or RA) with physical and procedural security controls equivalent or better than those for component.
5.5.4	Archive Backup Procedures	This CP does not require backup of archived records. If a CA or RA chooses to backup archived data, the CPS, RPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.
5.5.5	Requirements for Time-stamping of Records	CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.
5.5.6	Archive Collection System (internal or external)	The applicable CPS or RPS shall describe the archive collection system.
5.5.7	Procedures to Obtain and Verify Archive Information	Procedures detailing how to create, verify, package, transmit, and store the archive information, shall be published in the applicable CPS or RPS. The contents of the archive shall not be released except as determined by the applicable PMA or as required by law. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents.

5.6 Key Changeover

To minimize risk from compromise of a CA's signature Private Key, that Key may be changed often; from that time on, only the new Key shall be used for Certificate signing. The older, but still valid, Certificate will be available to verify old signatures until all of the Certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs or OCSP Certificates, then the old Key shall be retained and protected.

CAs Cross-Certified with the US FBCA or other bridges shall be able to continue to interoperate with the bridge after the bridge performs a Key rollover, whether or not the bridge DN is changed.

CAs either shall establish Key rollover Certificates as described above or shall obtain a new CA Certificate for the new Public Key from the Issuers of their current Certificates. As an example, a CA in a hierarchical PKI may obtain a new CA Certificate from its superior CA rather than establish Key rollover Certificates.

All Certificates and corresponding Keys shall have maximum Validity Periods not to exceed the requirements in Section 6.3.2.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If a CA or CSA detects a potential hacking attempt or other form of compromise, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA or CSA Key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA or CSA needs to be rebuilt, only some Certificates need to be Revoked, and/or the CA or CSA Key needs to be declared compromised.

The CA and applicable PMA(s) shall be notified if any of the following cases occur:

- 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 CA Certificate Revocation is planned.

CA operations shall be reestablished as quickly as possible in accordance with procedures set forth in the CA'S CPS.

RA Systems and CMSs shall have incident handling procedures that are approved by the PMA of the operating Organization. If the RA System or CMS is suspected of compromise, all RA Certificates and PIV-I Content Signing Certificates Issued to the RA System or CMS shall be suspended. If the RA System or CMS is compromised, all RA Certificates and PIV-I Content Signing Certificates Issued to the RA System or CMS shall be Revoked. The damage caused by the RA System or CMS compromise shall be assessed by both the operating entity PMA and the IdenTrust PMA, and all Subscriber Certificates that may have been compromised shall be Revoked. Subscribers shall be notified of such Revocation. The CMS shall be reestablished as soon as practical through Issuance of a new RA Certificate required for operation upon approval of the IdenTrust PMA.

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

CAs shall maintain backup copies of hardware, system, databases, and Private Keys in order to rebuild the CA capability in case of software and/or data corruption. When computing resources, software, and/or data are corrupted, the CAs shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored;
- If the CA Signature Keys are not destroyed, CA operation shall be reestablished, giving priority to the ability to generate Certificate status information within the CRL issuance schedule specified in Section 4.9.7; and

- If the CA Signature Keys are destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA Key Pair.

If a 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 been Issued Certificates by the CA shall be securely notified immediately. This will allow other CAs to protect their Subscribers' interests as Relying Parties. The CA shall reestablish Revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. If Revocation capability cannot be established in a reasonable time-frame, the CA shall determine whether to request Revocation of its Certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all Subscribers that use the CA as a Trust Anchor to delete the Trust Anchor.

5.7.3 CA Private Key Compromise Procedures

If a CA's Signature Keys are compromised, lost, or suspected to be compromised:

1. All cross certified CAs shall be securely notified at the earliest feasible time (so that entities may Issue CRLs revoking any Cross-Certificates Issued to the CA);
2. A CA Key Pair shall be generated by the CA in accordance with procedures set forth in the applicable CPS;
3. New CA Certificates shall be requested in accordance with the initial Registration process set elsewhere in this CP;
4. If the CA can obtain accurate information on the Certificates it has Issued and that are still valid (i.e., not expired or Revoked), the CA may re-issue (i.e., renew) those Certificates with the notAfter date in the Certificate as in original Certificates; and
5. If the CA is the Root CA, it shall provide the Subscribers the new Trust Anchor using secure means.

The CA governing body shall also investigate what caused the compromise or loss, and what measures shall be taken to preclude recurrence.

If a CSA Key is compromised, all Certificates Issued to the CSA shall be Revoked, if applicable. The CSA will generate a new Key Pair and request new Certificate(s), if applicable. If the CSA provides Certificate status services for a Trust Anchor, the Relying Parties will be provided the new Trust Anchor in a secure manner (so that the Trust Anchor integrity is maintained) to replace the compromised Trust Anchor.

If a RA, RA Administrator, or LRA Signature Keys are compromised, lost, or suspected to be compromised:

1. The Certificate shall be immediately Revoked;
2. A new Key Pair shall be generated in accordance with procedures set forth in the applicable CPS;

3. A new Certificate shall be requested in accordance with the initial Registration process set elsewhere in this CP;
4. All Certificate Registration requests approved by the RA, RA Administrator, or LRA since the date of the suspected compromise shall be reviewed to determine legitimacy; and
5. For those Certificates requests or approval than cannot be ascertained as legitimate, the resultant Certificates shall be Revoked and their subjects (i.e., Subscribers) shall be notified of Revocation.

5.7.4	Business Continuity Capabilities After a Disaster	In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request that its Certificates be Revoked. The CA shall follow steps 1 through 5 in Section 5.7.3 above.

5.8 CA or RA Termination

In the event of termination of a CA, the CA shall request all Certificates Issued to it be Revoked. In the event of a CA termination, the IdenTrust PMA shall provide notice to all cross certified CAs prior to the termination.

- A CA, CMS, CSA, RA and LRA shall archive all audit logs and other records prior to termination.
- A CA, CMS, CSA, RA, and LRA shall destroy all its Private Keys upon termination.
- CA, CMS, CSA, RA, and LRA archive records shall be transferred to the IdenTrust PMA.
- If the IGC Root CA is terminated, the IdenTrust PMA shall use secure means to notify Subscribers to delete all Trust Anchors representing the CA.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1	Key Pair Generation	When a FIPS 140-1/2 module is used, the module shall be validated and shall be used in FIPS approved mode.
6.1.1.1	CA Key Pair Generation	Cryptographic keying material for all CAs shall be generated in FIPS 140 Level 3 (or higher) validated hardware KSMs using FIPS approved methods. Cryptographic keying material for all CSAs and CMSs shall be generated in FIPS 140 Level 2 (or higher) validated hardware KSMs using FIPS approved methods. Key Generation procedures shall be documented in the respective CPS or RPS, and generate auditable evidence that the documented procedures were followed, and were witnessed and attested to by an independent third party. CA and CSA, Key Pairs shall be generated under two person control. Key Pair generation shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. The Key Pair generation process shall be validated by an independent third party by witnessing the Key Generation or by examining the signed and documented record of the Key Generation. Cryptographic keying material for RA, CMS and LRA Keys shall be generated in FIPS 140 Level 2 (or higher) validated hardware KSMs. Cryptographic keying material for the PIV-I Content Signing Certificate shall be generated in FIPS 140 Level 2 (or higher) validated hardware KSMs. Activation of the CMS Master Key shall require hardware assurance authentication by Individuals in Trusted Roles. Key diversification operations by the CMS shall also occur on the CMS hardware KSM. The diversified Keys shall only be stored in hardware KSMs that support PIV-I hardware assurance or commensurate. CMS Master Key and diversified Keys shall be protected from unauthorized disclosure and distribution. Card management shall be configured such that only the authorized CMS can manage Issued cards.
6.1.1.2	Subscriber Key Pair Generation	Subscriber Key Pair Generation may be performed by the Subscriber, CA, or RA. If the CA or RA generates Key Pairs, the requirements for Key Pair delivery specified in Section 6.1.2 shall also be met. Key Generation shall be performed using a FIPS approved method as specified in Section 6.2.1 of this CP. For PIV-I Hardware and PIV-I Card Authentication Assurance levels,

		other requirements explained in Section 11 of this CP apply.
6.1.2	Private Key Delivery to Entity	If Subscribers generate their own Key Pairs, then there is no need to deliver Private Keys, and this section does not apply. When CAs, RAs, or CMSs generate Keys on behalf of the Subscriber, then the Private Key shall be delivered securely to the Subscriber. Private Keys may be delivered electronically or may be delivered on a KSM. In all cases, the following requirements shall be met: • For Group Certificates, any entity receiving and holding Private Key(s) of a Signature Certificate on behalf of a Subscriber shall meet the requirements for control of Private Keys as stated in Section 3.2.3.3. • Other than for Group Certificates, any entity that generates a Private Key for the Signature Certificate of a Subscriber shall not retain any copy of the Private Key after delivery to the Subscriber; • The Private Key shall be protected from activation, compromise, or modification during the delivery process; • The Subscriber shall acknowledge receipt of the Private Key, typically by having the Subscriber use the related Certificate; • Delivery shall be accomplished in a way that ensures that the correct tokens and Activation Data are provided to the correct Subscribers; • For hardware KSMs, accountability for the location and state of the module shall be maintained until the Subscriber accepts possession of it; • For electronic delivery of Private Keys, the Key material shall be encrypted using a cryptographic algorithm and Key size at least as strong as the Private Key; • Activation Data shall be delivered using a separate secure channel; and • For shared Key applications, Organizational identities, and network Devices, see also Section 3.2. The CA, RA, or CMS operator shall maintain a record of the Subscriber acknowledgement of receipt of the KSM.
6.1.3	Public Key Delivery to Certificate Issuer	Public Keys shall be delivered to the Certificate Issuer in a way that binds the Applicant's verified identification to the Public Key being certified. This binding shall be accomplished using means that are at least as secure as the security offered by the Keys being certified. The binding shall be accomplished using cryptographic, physical, procedural, and other appropriate methods. The methods used for Public Key delivery shall be stipulated in the CPS or RPS.

6.1.4	CA Public Key Delivery to Relying Parties	When a CA updates its Key Pair, the CA shall distribute the new Public Key in a secure fashion. The new Public Key may be distributed in a self-signed Certificate, in a Key rollover Certificate, or in a new CA Certificate obtained from the Issuer(s) of the current CA Certificate(s). Self-signed Certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods for self-signed Certificate delivery include: • The CA loading a self-signed Certificate onto tokens delivered to Relying Parties via secure mechanisms; • Secure distribution of self-signed Certificates through secure Out-of-Band mechanisms; • Comparison of the hash of the self-signed Certificate against a hash value made available via authenticated Out-of-Band sources (note that hashes posted in-band along with the Certificate are not acceptable as an authentication mechanism); and • Loading Certificates from web sites secured with a currently valid Certificate of equal or greater Assurance Level than the Certificate being downloaded. Other methods that preclude substitution attacks may be considered acceptable. Key rollover Certificates are signed with the CA's current Private Key, so secure distribution is not required. CA Certificates are signed with the issuing CA's current Private Key, so secure distribution is not required.
6.1.5	Key Sizes	For the IGC Root CA, CA's subject Public Keys in such Certificates shall be at least 2048 bits RSA or at least 224 bits for ECDSA. Public Keys in all self-signed Certificates generated after 12/31/2010 that expire after 12/31/2030 shall be at least 3072 bits for RSA or at least 256 bits for ECDSA. CAs that generate Certificates and CRLs under this policy shall use Signature Keys of at least 2048 bits for RSA or at least 224 bits for ECDSA. All Certificates, except self-signed Certificates, that expire after 12/31/2030 shall be signed with Keys of at least 3072 bits RSA, or at least 256 bits for ECDSA. CAs that generate Certificates and CRLs under this policy shall use SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating Digital Signatures. Signatures on Certificates and CRLs that are Issued after

		12/31/2030 shall be generated using, at a minimum, SHA-256. CSSs shall sign OCSP Responses using the same signature algorithm, Key size, and hash algorithm used by the CA to sign CRLs. End-entity (Subscriber or Device) Certificates shall contain Public Keys that are at least 2048 bits RSA, or 224 bits for elliptic curve algorithms. The following special conditions also apply: • End-entity Certificates that expire after 12/31/2030 shall contain Public Keys that are at least 3072 bits RSA, or 256 bits for elliptic curve algorithms. • All end-entity Certificates associated with PIV-I Assurance Levels shall contain Public Keys and algorithms that conform to [NIST SP 800-78]. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric Key, and at least 2048 bit RSA or equivalent for the asymmetric Keys. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric Key, and at least 3072 bit RSA or equivalent for the asymmetric Keys after 12/31/2030.
6.1.6	Public Key Parameters Generation and Quality Checking	Public Key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186. Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186.
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage field)	The use of a specific Key is determined by the key usage extension in the X.509 Certificate. Public Keys that are bound into Certificates shall assert digitalSignature or keyEncipherment, but not both. With the exception of Device Certificates, “dual use” Certificates asserting both digitalSignature and keyEncipherment shall not be Issued by CAs operating under this CP. Subscriber Certificates shall assert key usages based on the intended application of the Key Pair. In particular, Certificates to be used for digital signatures (including authentication) shall set the digitalSignature and/or nonRepudiation bits. Certificates to be used for Key or data encryption shall set the keyEncipherment and/or dataEncipherment bits. Certificates to be used for key agreement shall set the keyAgreement bit.

		Group Certificates shall not assert nonrepudiation. CA Certificates shall set two key usage bits: cRLSign and/or keyCertSign. Where the subject signs OCSP responses, the Certificate may also set the digitalSignature and/or nonRepudiation bits. PIV-I Content Signing Certificates shall include an extended key usage of id-fpki-pivi-content-signing. All Subscriber Certificates issued with a DirectTrust policy OID shall assert a Basic Constraint of CA=FALSE and may assert an extended key usage not in conflict with the Certificate primary key usages.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The minimum requirements for HSMs are (higher levels may be used):

- FIPS 140 Level 3 or higher hardware HSMs for CA systems.
- FIPS 140 Level 2 or higher hardware HSMs for CSA and CMS systems.
- FIPS 140 Level 2 or higher hardware HSMs for RA systems

The relevant standard for Cryptographic Modules (KSMs) is FIPS PUB 140, Security Requirements for Cryptographic Modules.

The minimum requirements for KSMs are (higher levels may be used):

- FIPS 140 Level 2 or higher hardware KSMs for LRAs.
- FIPS 140 Level 2 or higher hardware KSMs for Certificates with an Assurance Level of Basic Hardware, Medium Hardware, Medium Device Hardware or PIV-I Hardware Certificates.
- For Custodian Key Stores for Rudimentary Assurance Certificates, FIPS 140 Level 1 (Hardware or Software) is required and for Custodian Key Stores for all other Assurance levels, FIPS 140 Level 2 or higher hardware KSMs are required.
- FIPS 140 Level 1 or higher KSMs (Hardware or Software) for Certificates with an Assurance Level of Basic Software, or Medium Device Certificates.

For PIV-I Assurance Levels, additional requirements for PIV-I cards detailed in Section 11 also apply.

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 shall be implemented 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 (n out of m) Multi-person Control	A single person shall not be permitted to activate or access the Private Key of a CA, CSA or PIV-I Content Signing Certificate. Access to Private Keys of CA, CSA, and PIV-I Content Signing Certificates backed up for disaster recovery shall be under the same multi-person control as the original CA, CSA, and PIV-I Content Signing Key and as described in Section 5.2.2 of this CP.
6.2.3	Private Key Escrow	Under no circumstances shall the Private Key of a CA Certificate be escrowed. Private Keys used to support non-repudiation services shall not be escrowed. Subscriber Private Keys used to support services associated with digitalSignature and nonRepudiation bits shall not be escrowed. Private Keys of Encryption Certificates may be escrowed in accordance with Section 4.12.1.
6.2.4	Private Key Backup	
6.2.4.1	Backup of CA Private Signing Key	Backup of Private Keys of CA Certificates is required to facilitate disaster recovery. Private Keys shall be backed up under the same multi-person control as used to generate and protect the original Private Key, as described in Section 5.2.2. At least one copy of the Private Key of the CA Certificate shall be stored off site. All copies of the Private Key shall be accounted for and protected in the same manner as the original. Procedures for Private Key backup of CA Certificates shall be identified in the CA'S CPS. Refer to section 6.2.4.4 for additional details.
6.2.4.2	Backup of Subscriber Private Signing 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 CP. Procedures for backup of Private Keys of RA system Certificates shall be identified in the CA'S CPS, or RA'S RPS. Private Keys of LRA Signing Certificates shall not be backed up. Private Keys of Signing Certificates Issued to Subscribers on hardware KSMs shall not be backed up. Private Keys of Signing Certificates Issued to Subscribers on software KSMs may be backed up as long as they remain under the Subscriber's control. Such Private Keys shall not be stored in plain text form outside the KSM. Storage shall ensure security controls consistent with the protection provided by the Subscriber's KSM.

6.2.4.3	Backup of Certificate Holder's Key Management Private Keys	Backed up Private Keys of Subscriber Encryption Certificates shall not be stored in plain text form outside the KSM. Storage shall ensure security controls consistent with the protection provided by the Subscriber's KSM.
6.2.4.4	Backup of CSA Private Key	Private Keys of CSA Certificates may be backed up on a KSM approved for CSAs. The backup shall be performed under the same control as the CSA Key activation. A single copy of the Private Key shall be stored at the CSA location. A second copy shall be kept at the CSA backup location. All copies of the CSA Private Key shall be accounted for and protected in the same manner as the original. Procedures for backup of CSA Private Keys shall be identified in the CA'S CPS.
6.2.4.5	Backup of PIV-I Content Private Signing Key	Private Keys of PIV-I Content Signing Certificates shall be backed up under the same multi-person control as for initial Issuance. A single backup copy of the Private Key shall be stored at or near the content signing system location. A second backup copy shall be kept at a backup location. Procedures for backup of the Private Keys of PIV-I Content Signing Certificates shall be included in the appropriate CPS and shall meet the multiparty control requirements of Section 5.2.2.
6.2.4.6	Backup of Device Private Keys	Private Keys of Devices may be backed up or copied, but shall be held under the control of the Device's Primary Machine Operator or other authorized administrator. Backed up Private Keys shall not be stored in plain text form outside the KSM. Storage shall ensure security controls consistent with the protection provided by the Device's KSM.
6.2.5	Private Key Archival	Private Keys of Signature Certificates shall not be archived. For Private Keys of Encryption Certificates, no stipulation.
6.2.6	Private Key Transfer Into or From a Cryptographic Module	CA, CSA, RA system and CMS Private Keys shall be generated in and remain in a KSM meeting the storage requirements for such Keys as described in Section 6.2.1. At no time shall CA, CSA and CMS Private Keys exist in plain text outside the KSM. CA, CSA, RA system and CMS Private Keys may be backed up in accordance with Section 6.2.4.1. Subscribers of Certificates Issued to hardware KSMs shall not export Private Keys of Signature Certificates. Subscribers of Certificates Issued to software KSMs may use the secure export/import capability in the latest versions of the browsers to transfer Keys and Certificates via the PKCS#12 protocol. Private or symmetric Keys used to encrypt other Private Keys for transport shall be protected from disclosure.
6.2.7	Private Key	No stipulation beyond that specified in FIPS 140.

	Storage on Cryptographic Module	
6.2.8	Method of Activating Private Keys	CA, CSA and PIV-I Content Signing Key activation requires multiparty control as specified in Section 5.2.2. Subscribers shall be authenticated to the KSM before the Activation of any Private Key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs, or biometrics. Entry of Activation Data such as passwords and PINs shall be protected from disclosure (i.e., the data shall not be displayed while it is entered). For PIV-I Card Authentication, Medium Device Software and Medium Device Hardware Certificates, user activation of the Private Key is not required. The Device may be configured to activate its Private Key without requiring its Primary Machine Operator or authorized administrator to authenticate to the KSM, provided that appropriate physical and logical Access Controls are implemented for the Device and its KSM. The strength of the security controls shall be commensurate with the level of threat in the Device's environment, and shall protect the Device's hardware, software, and the KSM and its Activation Data from compromise.
6.2.9	Methods of Deactivating Private Keys	KSMs that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the KSM shall be deactivated (e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS). Hardware KSMs shall be removed and stored in a secure container or environment when not in use.
6.2.10	Methods of Destroying Private Keys	Individuals in Trusted Roles shall destroy CA, CSA, CMS, RA, and LRA Private Keys when they are no longer needed. Subscriber Private Keys shall be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are Revoked. This may be achieved by executing a "Zeroize" command. Physical destruction of the KSM 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 — The Public Key is archived as part of the Certificate archive process

6.3.2 Certificate Operational Periods and Key Pair Usage Periods — The following table provides the maximum Private Key Certificate Validity Periods for CA, CSA, CMS, RA, LRA, Subscriber Certificates, and Cross-Certificates.

Table 7 - Private Key Certificate Validity Periods

Key Type	Private Key Usage Period	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
Identity, Signing, and Card Authentication Certificates Issued to Individuals	3 years	3 years
Encryption Certificates Issued to Individuals	No restriction	3 years
Group Signing Certificates	3 years	3 years
Group Encryption Certificates	No restriction	3 years
Device	3 years	3 years
LRA	3 years	3 years
Bridge Cross Certificate	10-20 years	3 years
* Cross-Certificate Key Pair usage is dictated by whether the Key belongs to the Subordinate or Root CA 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. CAs shall not Issue Subscriber Certificates that extend beyond the expiration date of their own Certificates and Public Keys.		

6.4 Activation Data

6.4.1 Activation Data Generation and — The Activation Data used to unlock Private Keys, in conjunction with any other access control, shall have an appropriate level of strength for the Keys or data to be protected. Activation Data may be user selected. Activation Data shall meet the requirements of FIPS 140 Level 2. If the

	Installation	Activation Data shall be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated KSM. Where a CA, CSA, or RA uses passwords as Activation Data for the CA Signing Key, at a minimum the Activation Data shall be changed upon corresponding Re-Rey.
6.4.2	Activation Data Protection	Activation Data used to unlock Private Keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be either: • Memorized, • Biometric in nature, or • Recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CPS.
6.4.3	Other Aspects of Activation Data	Activation Data for Trusted Roles KSMs shall be changed every three months to decrease the likelihood that it is discovered. For PIV-I Certificates, the Activation Data may be reset only 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 shall be conducted by a Registration Agent or a Trusted Agent.

6.5 Computer Security Controls

6.5.1	Specific Computer Security Technical Requirements	The following computer security functions shall be provided by the operating system used by the CA, CSA, CMS, RA, and LRA: • Authenticated logins; • Discretionary Access Control; • Security audit capability; • Access control restrictions to CA services based on authenticated identity and PKI roles; • Privilege management to limit users to their PKI roles; • Enforce separation of duties for PKI roles; • Require I&A of PKI roles and associated identities; • Prohibit object re-use or require separation for CA random access memory; • Residual information protection;

- Trusted path for user I&A;
- Domain separation enforcement;
- Operating system self-protection;
- Use of cryptography for session communication and database security;
- Self-test security related CA services (e.g., check the integrity of the audit logs); and
- Recovery mechanisms for Keys and system failure

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

The computer system shall be configured only the minimum required accounts and network services. The CA, CSA and CMS shall not permit remote login from external networks.

6.5.2	Computer Security Rating	CA and CSA shall operate systems that have received security evaluations from NIAP, TPEP, or other comparable information-assurance ("IA") evaluation programs.

6.6 Life Cycle Technical Controls

6.6.1	System Development Controls	CAs and RAs shall maintain the following documentation: • Installation Qualification plans, procedures/scripts/data, Acceptance criteria, and results; and • Operational Qualification plans, procedures/scripts/data, Acceptance criteria, certifications, and test results. The following specific requirements shall be met as part of the system development process: • CAs and RAs shall use software, whether off-the-shelf or custom-built, that has been designed and developed under a formal, documented development methodology; • Hardware and software procured shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase); • Hardware and software that is developed specifically for the CA or RA shall be developed in a controlled environment, and the development process shall be defined and documented. The

CA or RA shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment. This requirement does not apply to off-the-shelf hardware or software;

- Where open source software has been utilized, the CA or RA shall demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management;
- All hardware and software shall be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location;
- The PKI platform (server hardware, operating system software, and PKI application software) shall be dedicated to performing PKI functions. There shall be no non-PKI applications installed on the PKI platform. Connected or associated hardware Devices, network connections, or component software that are not part of the PKI platform are exempt from this requirement;
- Proper care shall be taken to prevent malicious software from being loaded. Applications required to perform the PKI operation shall be obtained from sources authorized by local policy; and
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

CA, CSA, CMS, and RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

6.6.2	Security Management Controls	The configuration of the CA, CSA, CMS and RA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CA, CSA, CMS and RA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of CA, CSA, CMS and RA systems. The CA, CSA, CMS, and RA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The CA, CSA, CMS and RA software integrity shall be verified continually.
6.6.3	Life Cycle Security Ratings	No stipulation.

6.7 Network Security Controls

The Root CA shall operate offline. Remote access to the Root CA shall not be allowed.

CAs, CSAs, CMSs, RAs, and LRAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls, and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of PKI services.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Time Stamping

All CA, CSA, CMS and RA components shall regularly synchronize with a time service such as National Institute of Standards and Technology ("NIST") Atomic Clock or NIST Network Time Protocol ("NTP") Service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's Certificate;
- Revocation of a Subscriber's Certificate;
- Posting of CRL updates; and
- OCSP or other CSA responses.

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as listed in Section 5.4.1.

7 CERTIFICATE, CARL/CRL, AND OCSP Profiles

7.1 Certificate Profile

7.1.1	Version Number(s)	CAs shall Issue X.509 v3 Certificates (populate version field with integer "2").
7.1.2	Certificate Extensions	Critical private extensions shall be interoperable in their intended community of use. Certificates Issued by CAs under this CP shall comply with the IGC Certificate Profiles document, published as a companion document to this IGC-CP. IGC Certificate Profiles are subject to change and new versions will be published from time to time. CAs will be notified of IGC Certificate Profiles changes and shall comply with new IGC Profiles versions within (90) days of publication. CA and Subscriber Certificates may include any extensions as specified by RFC 5280 in a Certificate, but shall include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the Certificate and CRL profiles defined in this CP and the IGC Profiles. Conforming Certificates shall include all required extensions.

7.1.3 Algorithm Object Identifiers

Certificates Issued under this CP shall use the following algorithms and OIDs for signatures, and for identifying the subject Public Key information:

Table 8 - Algorithms and OIDs for Signatures

Algorithm	OID
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-Sha1	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) sha1(1)}
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 }

Table 9 - Algorithms and OIDs for Identifying 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}

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

All DNs in the Issuer and Subject fields are consistent with the X.500 standard and further constrained by RFC 5280 and each relative DN shall have only one value.

Table 10 - CA Subject Name Form

USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
Required	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
Required	O	1	CA name
Optional	C	1	Country name (e.g. "US")

Table 11 - Subject Name Form (non-CA)

USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
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. Multiple additional OUs may be included as needed to support individual customer PKI requirements.
Required	O	1	Subject Organization name (e.g., "O=ABC Inc") or "Unaffiliated" if no Organization affiliation.
Optional	C	1	Country name (e.g., "US")

Table 122 - 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"
	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.

Table 13 - 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.
	Optional	OU	0…N	As needed
	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.

When multiple values exist for an attribute in a DN, the DN shall be encoded so that each attribute value is encoded in a separate relative DN.

7.1.5 Name Constraints

CAs may assert critical or non-critical name constraints beyond those specified in IGC Certificate Profiles subject to the requirements above.

CAs may obscure a Subscriber Subject Name to meet local privacy regulations as long as such name is unique and traceable to a corresponding un-obscured name. Issuer names may not be obscured. CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats.

7.1.6 Certificate Policy Object Identifier (CP OID)

CA and Subscriber Certificates Issued under this CP shall assert one or more of the OIDs listed in Section 1.2.2. For example:

> When a Participant CA asserts a certificate policy OID, it may also assert all lower Assurance Level certificate policy OIDs. If a CA Issues a PIV-I Hardware Certificate, it may assert Medium Software or Medium Hardware.

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 also be included, as defined in the IGC-CPS document and/or IGC Certificate Policies document.

7.1.7 Usage of Policy Constraints Extension

CAs shall adhere to the certificate formats described in this CP.

7.1.8 Policy

Certificates Issued by CA's may contain policy qualifiers identified in RFC

	Qualifiers Syntax and Semantics	5280.
7.1.9	Processing Semantics for the Critical Certificate Policies Extension	Processing semantics for the critical CP extension shall conform to X.509 certification path processing rules.

7.2 CRL Profile

The CRL Profile is specific in IGC Profiles.

7.2.1	Version Number(s)	CAs shall Issue X.509 version two (v2) CRLs (populate version field with integer "1").
7.2.2	CRL and CRL Entry Extensions	CRLs shall comply with the CRL extension profiles specified in IGC Profiles.

7.3 OCSP Profile

OCSP Requests and responses shall be in accordance with RFC 6960. IGC Profiles specify the OCSP Request and response formats.

7.3.1	Version Number(s)	The version number for request and responses shall be version one (1).
7.3.2	OCSP Extensions	Responses shall support the nonce extension.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

CAs, CMSs and RAs shall have a compliance audit mechanism in place to ensure that the requirements of this CP, the applicable CPS and/or RPS, and provisions of any relevant Memorandum of Agreement ("MOA") are being implemented and enforced. CAs shall specify the relevant MOAs in their CPS.

8.1 Frequency of Audit or Assessments

CAs, CMSs and RAs including any subordinate CAs, CMSs or RAs, shall be subject to a periodic compliance audit, which is no less frequent than once per year.

8.2 Identity/Qualifications of Assessor

The auditor shall demonstrate competence in the field of compliance audits for security and PKIs, and shall be thoroughly familiar with requirements that the IdenTrust PMA imposes on the Issuance and management of Certificates Issued under this CP. The compliance auditor shall perform such compliance audits as a primary responsibility.

The IdenTrust PMA has the right to require periodic and 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 their respective RPS. The IdenTrust PMA shall state the reason for any aperiodic compliance audit.

8.3 Assessor's Relationship to Assessed Entity

For CAs, the compliance auditor 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.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a component operates in accordance with this CP, the CA CPS, any applicable RPS, other applicable CPs, and any relevant MOAs specified in the component CPS or RPS.

Components other than CAs may be audited fully or by using statistical sampling. 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

The IdenTrust PMA and other relevant PMAs may determine that a CA or RA is not complying with its obligations set forth in this CP, the CA CPS, the RA'S RPS, or the relevant MOAs. When such a determination is made, the relevant PMAs may suspend operation of a noncompliant CA or RA it controls. When the compliance auditor finds a discrepancy between how a component operates, and the requirements of this CP, the applicable CPS, or applicable RPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the responsible party;
- The responsible party, if not IdenTrust, shall immediately notify the IdenTrust PMA of the discrepancy; and
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP, the applicable CPS or RPS and relevant MOAs, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the IdenTrust PMA may decide to Revoke the CA, halt temporarily operation of the affected CA or RA, or take other actions it deems appropriate.

8.6 Communications of Results

On an annual basis, the IdenTrust PMA shall submit an audit compliance package to the Federal PKI Policy Authority. This package shall be prepared in accordance with the "Compliance Audit Requirements" document and includes an assertion from the IdenTrust PMA that all PKI components have been audited - including any components that may be separately managed and operated. The package shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1	Certificate Issuance or 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	Certificate access fees shall not be charged for IGC Certificates.
9.1.3	Revocation or Status Information Access Fees	CAs shall not charge access fees for standard CRL or OCSP Certificate status information. CAs may charge access fees for specialized OCSP services.
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 shall maintain reasonable levels of insurance coverage or demonstrate sufficient balance sheet to address all foreseeable liability obligations to entities described in Section 1.3 of this CP.
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 CP.
9.2.3	Insurance or Warranty Coverage for End-Entities	No stipulation.

9.3 Confidentiality of Business Information

Subject to any stipulations regarding the confidentiality of such information included in any applicable MOA between the US FBCA and IdenTrust, , CAs, RAs, LRAs, and Trusted Agents shall keep confidential all such labeled information they receive as part of fulfilling their responsibilities under this CP.

9.4 Privacy of Personal Information

All Subscribers' identifying information as defined by local privacy regulations shall be protected from unauthorized disclosure. Any sensitive information shall be explicitly identified in a CA CPS or RA'S RPS. All information stored electronically on the component equipment and not in the Repository, and all physical records shall be handled as sensitive. Access to this information shall be restricted to those with an official need-to-know in order to perform their responsibilities as defined in this CP, and such

information shall not be disclosed to any third party unless authorized by this CP, by agreement, by order of a court of competent jurisdiction, or as required by law, government rule or regulation. Requirements for notice and consent to use private information shall be defined in the respective CPS and/or privacy policy.

Certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., LDAP, HTTP).

CAs, RAs, LRAs, and Trusted Agents shall disclose a privacy policy to all entities that submit Subscriber identifying information to CAs and RAs.

9.5 Intellectual Property Rights

Neither IdenTrust, nor any Participant CA, nor any RA shall knowingly violate any intellectual property rights held by others.

This CP 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 CA'S CPS shall define restrictions of use of the intellectual property within the CPS. A RA'S RPS shall define restrictions of use of the intellectual property within the RPS.

A Private Key shall be treated as the sole property of the legitimate holder of the Certificate containing the corresponding Public Key.

9.6 Representations and Warranties

9.6.1 CA Representation and Warranties

CAs shall represent and warrant that they shall conform to the stipulations of this document, including:

- Providing a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming their practices and procedures to the stipulations of the approved CPS;
- Ensuring that Registration information is accepted only from RAs or LRAs who understand and are obligated to comply with this policy;
- 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 shall represent and warrant that they shall conform to the provisions and stipulations of any applicable MOA and Cross-certification agreements.

For PIV-I Assurance Levels, CAs shall maintain an agreement with Subscribing Organizations concerning the obligations pertaining to authorizing affiliation with Subscribers of PIV-I Certificates.

A CA that 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 shall represent and warrant to the CA at the time it approves a Certificate for Issuance that:

- It approved Issuance of the Certificate in accordance with this CP, the CA CPS and the RA'S RPS;
- 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 representations and warranties, RAs represent and warrant that they shall conform to and comply with the stipulations of this CP, the CA CPS and the RA'S RPS, and shall ensure that their LRAs and Trusted Agents 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 Certificates that have been Issued to the RA, LRA or TA and cancellation of registration authorization and registration responsibilities.

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 shall warrant and represent to CA and the RA (if any) that:

- All information provided by it (and its 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.
- Protect its Private Keys from compromise (including if employing a Custodian, or authorized third party who has implemented a Custodial Subscriber Key Store and uses secure processes against potential compromise).

9.6.1 In addition to the above, for Device Certificates, that Organization names, FQDNs or other information used to identify Devices as provided for in Section 3.1.2 above 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.

In addition to these representation and warranties, Subscribers shall represent and warrant that they conform to and comply with the stipulations of this CP, the CA'S CPS and any applicable RA'S RPS, including that they will:

- Accurately represent themselves in all communications with the PKI;
- Protect their Private Keys at all times, RA'S RPS as may be stipulated in their Certificate Acceptance agreements, and local procedures;
- Promptly notify 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 the CA CPS and any applicable RA RPS;
- 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 CP.

For Device Certificates, a Sponsor shall designate an Individual who will perform the role of a Primary Machine Operator and shall be responsible for carrying out Applicant and Subscriber duties in relation to the Device Certificate associated with the Device. Such Primary Machine Operator shall also assume the obligations of the Applicant and Subscriber for the Certificate associated with the Device. The Primary Machine Operator assuming the obligations of Applicant for a Certificate associated with a Device shall sign a Subscribing Organization Authorization Agreement agreeing to the requirements above in this Section 9.6.3.

For all end entity certificate Assurance Levels except for Basic, the Applicant shall sign a Subscribing Organization Authorization Agreement agreeing to all applicable requirements above in this Section 9.6.3 before

being Issued the Certificate and becoming a Subscriber.

For Basic Assurance Level Certificates, Applicants are required to acknowledge his or her obligations respecting protection of the Private Key and use of the Certificate before being Issued the Certificate and becoming a Subscriber.

9.6.4 Relying Party Representations and Warranties

Any time that a Relying Party uses or otherwise relies on a Certificate, he or she shall 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 the CA's 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;
- 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;
- Establish trust in the Certificate using certification path validation procedures described in [RFC 5280], prior to reliance; and
- Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the Digital Signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades may invalidate Digital Signatures and shall be avoided.

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 Repository Representations and Warranties

See Section 2.1.1

9.6.5.2 CSA Obligations

A CSA that provides Revocation status and/or complete validation of Certificates represents and warrants that it shall conform to the stipulations of CA's CPS and this CP, including:

- Providing this CA's CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of CA's CPS and this 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 that is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5 of this CP.

9.6.5.3	Subscribing Organization Representations and Warranties	Subscribing Organizations shall represent and warrant that they will: • Authorize the affiliation of Subscribers with the Organization; and • Immediately inform the Participant CA of any severance of affiliation with any current Subscriber.

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 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 NONINFRINGEMENT 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 CSA will meet particular requirements or be error free; (ii) that any Certificate, Repository or CSA will be available, uninterrupted, accessible, timely or secure; (iii) that any defects will be corrected, or that a Certificate, Repository or CSA 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 any Participant CA shall be set forth in the applicable agreement(s) between IdenTrust and the Participant CA.

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 CP, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

A CA may limit its liability for each Certificate Type as set forth in its CPS. A CPS may exclude liability for any Certificate that is Issued and managed in accordance with this CP and the CPS or in instances where a Subscriber or Relying Party has not complied with the terms and conditions of use for the Certificate.

9.9 Indemnities

Unless agreed upon in a separate agreement, neither IdenTrust, its Participant CAs nor their agents (e.g., RA, Trusted Agents, etc.) assume financial responsibility for improperly used Certificates.

A CA's agreement between itself and other entities (such as Cross Certification Bridge Authority) shall

specify additional indemnification terms between the CA and entity (such as indemnification of the Cross Certification Bridge Authority). Additionally, a CAs CPS may provide further indemnification terms.

9.10 Term and Termination

9.10.1	Term	This CP and any amendments hereto shall become effective upon publication in the Repository. This CP as amended from time to time shall remain in force until it is replaced by a new version.
9.10.2	Termination	Termination of this CP is at the discretion of IdenTrust. A CA's termination of their CPS is at the discretion of the CA.
9.10.3	Effect of Termination and Survival	The following sections of this CP shall survive termination or expiration of this CP: 2.1, 2.2, 5.4, 5.5, 6.2-6.4, 6.8, 9.2-9.4, 9.7-9.10, and 9.13-9.16.

9.11 Individual Notices and Communications with 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 CP 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 CP (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 to 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, Suite 450, Salt Lake City, UT 84116, which such communication will be deemed effective when delivered as evidenced by written confirmation of receipt as recorded by the courier.

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 CP will be reviewed by IdenTrust from time to time. Errors, updates, or suggested changes to this document should be communicated to helpdesk@IdenTrust.com. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.1	Procedure for Amendment	Updated CP versions are posted on IdenTrust's web site at https://secure.identrust.com/certificates/policy/igc/index.html. Changes to this CP become effective upon publication of an amended version of the CP in the Repository.
9.12.2	Notification Mechanism and Period	IdenTrust, at its discretion, will notify affected PKI Participants via email or via IdenTrust's web site of CP changes. PKI Participants may file comments regarding changes that materially or adversely affect the PKI Participant's operations within 15 days of original notice. All comments must be written and signed in ink or digitally signed. Decisions with respect to CP changes and the effective date of any new CP version are at the sole discretion of IdenTrust.
9.12.3	Circumstances Under Which an OID Must be Changed	If a change in this CP is determined by the IdenTrust PMA to change the level of assurance provided from the currently specified OID for a particular type of Certificate, then the revised version of this CP will also contain a revised OID for that type of Certificate.

9.13 Dispute Resolution Provisions

Provisions for resolving disputes between IdenTrust, Participant CAs and other parties shall be set forth in the applicable agreements between the parties.

Provisions for resolving disputes between Participant CAs and other relevant entities shall be set forth in the applicable agreements between the parties.

9.14 Governing 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 CP, 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 Participants, no matter where they are located.

This governing law provision applies only to this CP. Agreements incorporating the CP 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 CP separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

9.15 Compliance with Applicable Law

This CP 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	Except where specified by other contracts, this CP 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 CP.
9.16.2	Assignment	Except where specified by other contracts, Participants may not assign any of their rights or obligations under this CP or applicable agreements without the written consent of IdenTrust.
9.16.3	Severability	In the event that a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP shall remain valid.
9.16.4	Waiver of Rights	No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CP are for convenience only and cannot be used in interpreting this CP.
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: ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH THE PKI SERVICE PROVIDER HAS NO CONTROL; FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT THE FAULT OR NEGLIGENCE OF THE PKI SERVICE PROVIDER.

9.17 Other Provisions

None

10 DIRECTORY INTEROPERABILITY PROFILE

10.1 Protocol

Each CA shall implement a directory system that provides at least HTTP access to published Certificates and CRLs. In addition, LDAP may be implemented and if so, LDAP referrals shall be supported.

10.2 Authentication

Each CA directory system shall permit "none" authentication to read Certificate and CRL information. Each CA shall be free to implement authentication mechanisms of its choice for browse and list operations. Any write, update, add entry, delete entry, add attribute, delete attribute, change schema etc., shall require password over SSL or stronger authentication mechanism.

10.3 Naming

When a LDAP Repository is used:

- Certificates shall be stored under the directory entry for the Subject Name that appears in the Certificate;
- The issuedByThisCA element of CrossCertificatePair shall contain the Certificate(s) Issued by a CA whose name the entry represents; and
- All CRLs shall be stored under the directory entry of the CA that published the CRL.

10.4 Object Class

When a LDAP Repository is used:

- Entries that describe CAs shall be defined by the OrganizationUnit structural object class;
- All CA entries shall belong to the pkiCA cpCPS auxiliary object classes;
- Entries that describe Individuals (human entities) shall be defined by the inetOrgPerson class, which inherits from other classes: person, and OrganizationalPerson; and
- These entries shall also be a member of pkiUser auxiliary object class.

10.5 Attributes

When a LDAP Repository is used:

- CA entries shall be populated with the caCertificate, crossCertificatePair, CertificateRevocationList, and cPCPS attributes, as appropriate; and
- End entity entries shall be populated with userCertificate attribute containing encryption Certificate. Signing Certificates do not need to be published to the PKI LDAP Repository.

11 INTEROPERABLE SMART CARD DEFINITION

IGC PIV-I enables 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. IGC PIV-I fully maps to the PIV-I specification as defined by the U.S. Federal Government. This section defines the specific requirements of an IGC PIV-I Smart Card. It relies heavily on relevant specifications from the National Institute of Standards and Technology ("NIST").

1. Smart Card platform shall be from the GSA's FIPS 201 Evaluation Program Approved Product List ("APL") and shall use the PIV application identifier ("AID").
2. Smart Card shall contain a Private Key and associated identity Certificate asserting IGC PIV-I Hardware assurance or an IGC PIV-I Hardware assurance mapped CP OID.
3. Smart Card shall contain a Private Key and associated card authentication Certificate asserting IGC PIV-I Card Authentication or an IGC PIV-I Card Authentication mapped CP OID.
4. Smart Card may contain Private Key and associated Digital Signature Certificate asserting IGC PIV-I Hardware assurance or an IGC PIV-I Hardware mapped CP OID.
5. Smart Card may contain Private Key and associated encryption Certificate asserting IGC PIV-I Hardware assurance or an IGC PIV-I Hardware mapped CP OID.
6. Smart Card shall 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 Card Issued under IGC PIV-I policies and all data objects on it shall be in accordance with SP 800-73..
8. Biometrics on the Smart Card shall also comply with Section 4.4 of FIPS 201-1 and SP 800-76.
9. Card holder Unique Identifier ("CHUID") shall also comply with Section 4.2 of FIPS 201-1. The Federal Agency Smart Credential Number ("FASC-N") shall be modified as define in Section 3.3 of SP800-73-3. FASC-N shall be constructed using Agency Code equal to 9999, System Code equal to 9999, and Credential Number equal to 999999. CHUID shall contain a 16-byte Global Unique Identifier ("GUID").
10. The CMS-signed objects such as fingerprint and photograph shall contain GUID as entry UUID attribute in place of FASC-N as pivFASC-N attribute.
11. Smart Card shall be visually distinct from the US Federal PIV Card. At a minimum, images or logos on an IGC PIV-I Smart Card shall not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201].
12. The Smart Card physical topography shall include, at a minimum, the following items on the front of it:
    a) Card holder facial image;
    b) Card holder full name;
    c) Organizational affiliation, if it exists; otherwise the Issuer of the card; and
    d) Card expiration date.
13. Smart Card shall have an expiration date not to exceed 6 years of issuance.
14. Smart Card expiration shall not be later than the expiration of the IGC PIV-I Content Signing

Certificate on the card, which shall conform to the Content Signing Certificate Profile specified in IGC Profiles.

15. The IGC PIV-I Content Signing Certificate and corresponding Private Key shall be managed within a trusted CMS in accordance with the requirements specified in this document.
16. At issuance, the RA shall activate and release 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 Card may support activation by the CMS to support card personalization and post-issuance card update. To activate the Smart Card for personalization or update, the CMS shall perform a challenge response protocol using cryptographic Keys stored on the Smart Card in accordance with [SP800-73]. When Smart Cards are personalized, card management Keys shall be set to be specific to each Smart Card. That is, each Smart Card shall contain a unique card management Key. Card management Keys shall meet the algorithm and Key size requirements stated in [SP 800-78].

12 REFERENCES

The following documents were referenced in development of this CP. Document versions cited were current at the date of adoption unless otherwise cited.

RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (Nov. 2003) http://www.ietf.org/rfc/rfc3647.txt
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 5322	Internet Message Format (Oct. 2008) http://tools.ietf.org/html/rfc5322.txt (replaces RFC 2822)
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (May 2008) http://www.ietf.org/rfc/rfc5280.txt
RFC 4122	A Universally Unique Identifier (UUID) URN Namespace (Jul. 2005) http://www.ietf.org/rfc/rfc4122.txt
RFC 3379	Delegated Path Validation and Delegated Path Discovery Protocol Requirements (Sept. 2002) http://www.ietf.org/rfc/rfc3379.txt
RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP) (Sept. 2005) http://www.ietf.org/rfc/rfc4210.txt
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (June 1999) http://www.ietf.org/rfc/rfc2560.txt?number=2560
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
W3C Recommendation	XML Key Management Specification, ver. 2 (XKMS 2.0) (Jun. 2005) http://www.w3.org/TR/xkms2
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)

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.