IdenTrust Global Common Certificate Policy

Version 1.6.0

October 24, 2025

Table of Contents

1 INTRODUCTION

This IdenTrust Global Common (IGC) Certificate Policy (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 CP will be reviewed and updated, 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.

1.1 OVERVIEW

This CP defines requirements for 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 CP are defined in Section 1.6.

1.1.1 Certificate Policy (CP)

Certificates issued under this CP contain a registered Certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a Certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance established by this CP which must be available to Relying Parties. Each Certificate issued by IdenTrust under the CP will assert the appropriate level of assurance in the Certificate Policies extension.

1.1.2 Relationship Between the IGC CP and the IGC CPS

This CP states the requirements for issuance and management of Certificates by the IdenTrust CA and requirements for operation. The IGC Certification Practices Statement (CPS) states how IdenTrust establishes and implements the requirements.

1.1.3 Relationship Between the IGC CP and other CPs

The relationship between this CP and other cross-certified CPs is asserted in the policy Mappings extension for CA Certificates issued by IdenTrust or in any Certificates issued to an IdenTrust CA that are requested by IdenTrust. This extension must include all relevant policy mappings and indicate that these policies are equivalent to each other.

1.1.4 Scope

This CP aligns with requirements as specified the following CP documents:

- X.509 Certificate Policy for the Federal Bridge Certification Authority v3. 8 dated August 2025
- DirectTrust Certificate Policy v2.0 dated October 7, 2020

1.1.5 Interaction with PKIs External to the Federal Government

No stipulation.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the IGC Certificate Policy approved for publication on TBD, by the IdenTrust Policy Management Authority (PMA). The following table contains subsequent revisions:

IGC Certificate Policy 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 the IGC Certificate Profiles.
1.3	July 15, 2015	The following sections have been modified primarily to meet business requirements for IGC Certificates: o 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. o Section 1 to add Card Authentication and Identity Certificate Policies (OIDs) for Basic Hardware and Medium Hardware Assurances. o Section 3.2.3.3 to add requirements for Group Certificates. o Section 4.12.1 add Key escrow and recovery policy. o Section 6.2.6 to clarify Private Key transfer requirements for software and hardware KSMs. o Section 6.3.2 to provide more Certificate granularity. o Section 6.4.2 to allow backup of RA Private Signing Keys. o Section 8 to better align audit requirements with current US FBCA CP audit requirements. o Section 9.11 regarding Participant communications. o In addition, RA requirements clarified and corrections to terms, formatting and spelling errors have been made throughout. o This version 1.3 was approved by IdenTrust PMA but not published pending auditor approval in regard 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	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: o Basic Hardware o Medium Hardware o 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.

Version	Date	Summary of Changes/Comments
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.
1.4.8	March 17, 2019	• Updated Section 6.5.1 Specific Computer Security Technical Requirements to clarify language pertaining to remote access to the CA System. • Updated Section 6.5.2 Computer Security Rating to sync with requirements of related governing CP documents. • Updating document to remove specific references to audits required on an annual basis and to refer to Section 8 where a table of annual audits is recorded. This will allow one update to be made to the document when audit procedures change, instead of need to make multiple updates throughout the document. • Updating format to align with RFC 3647 and the FBCA CP. Some sections were initially omitted because they pertained only to the Federal Bridge CA; however, to ensure that the document format is fully aligned, these sections have been reinserted.
1.4.9	May 29, 2019	Aligning with FBCA CP v2.34 dated Oct 4, 2018: o To remove all references to SSL Certificate issuance. o General cosmetic and clean up to grammar, etc. o Added references to VME and hypervisor. o Modified requirements for suspension periods.
1.5	August 8, 2019	Additional cosmetic and formatting clean up.
1.5.1	January 31, 2020	• Modifications to align with FBCA CP v2.35 to add allowance for the FBCA to be operated in an off-line status effective as of April 15, 2019: o 4.9.7 CRL Issuance Frequency. o 4.9.12 Special Requirements Related to Key Compromise. o 5.4.2 Frequency of Processing Log. • 6.3.2 Certificate Operational Periods and Key Usage Periods. • Added definition for Hypervisor. • Removed reference to dataEncipherment from section 6.1.7 - Key Usage Purposes (as per X.509 v3 key usage field). • Additional cosmetic clean up.
1.5.2	April 15, 2020	• Revised language referencing the FBCA, FPKIPA, FPKIPM, etc. per review conducted by the FPKIPA in 2019 audit review. • Changes made in Sections 1, 2, 4 and 6. • Revised language specific to DNs naming. • Changes made in Sections 3.1.1 and 3.1.2 • Updated language to clarify remote identity proofing (unsupervised and supervised). • Updated Definitions and Section 3.2.3.1 Authentication of Human Subscribers.
1.5.3	March 1, 2021	Added and or modified language as recommended by the FPKIPA as a result of comparison to the Federal Bridge Certificate Policy to this IGC Certificate Policy. • Removed specific references to FPKI and replaced with more generic terms, as this CP complies with multiple governing CP documents. • Removed reference to Entity CA and replaced with IdenTrust. Entity CA is an FPKI term and IdenTrust is the Entity CA as represented in the CP. • Added language in various sections to indicate that any UUID used in a PIV-I Certificate may not be the card serial number. • Section 1.2.2.1 IGC OIDs: Updated table to correctly reference all active

Version	Date	Summary of Changes/Comments
		OIDs • Section 1.3.4 Subscribers: Removed redundant language specific to Primary and Secondary Machine Operators • Section 2.1.1 IdenTrust Repository Obligations: updated language related to LDAP to indicate that encrypted LDAP is used for communications. • Section 3.1.2 Need for Names to Be Meaningful: added language to indicate that the UUID used to ensure name uniqueness is appended to the commonName (CN) and should not be included as a value in an organizationalUnit (OU) attribute. • Section 3.2.3.1 Authentication of Human Subscribers: removing language referring to remote identity proofing. • Section 3.2.3.3.2 Group Software Certificates: modified language to be more explicit and removed some irrelevant text. • Section 3.2.3.4 Authentication of Devices: removed language allowing for remote identity proofing for Device Certificates. • 3.2.3.4.2 Authentication of Secondary Machine Operators: added language to indicate that Secondary Machine Operators are not named in a Device Certificate. • Section 4.3.1.1 CA Certificates: added new requirement for CA Certificates to be checked for accuracy before providing to the requesting entity. • Section 4.4.3 Notification of Certificate Issuance by the CA to Other Entities: added new requirement to provide advance notice to the FPKI prior to issuance of a new CA Certificate. • Section 4.5.2 Relying Party Public Key and Certificate Usage: revised language to shift responsibility for compliance with the CP/CPS to the Relying Party and from IdenTrust. • Section 4.9.3 Procedure for Revocation Request: added language indicating that IdenTrust allow for revocation of Certificates. • Section 4.9.7 CRL Issuance Frequency and Section 4.9.12 Special Requirements Related to Key Compromise: removed references to Rudimentary and High Assurance as IdenTrust does not issue these types of Certificates. • Section 4.12 Key Escrow: removed language pertaining to Key Escrow and Key recovery is not presently offered under IGC. • Section 5.1 Physical Controls: adding explicit language regarding protection of the CA and definition of remote access to the CA. • Section 5.2.1.2 Certification Status Authority (CSA) Roles: added definitions for CSA Agent and CSA Operator which are equivalent to the CA Agent and CA Operator. • Section 5.4.2 Frequency of Processing Log: removed Rudimentary and High Assurance from the table in this section as IdenTrust does not offer these Certificate types. • Section 5.7.1.1 CA Incident: added new requirements for notifications pertaining to a CA compromise. • Section 5.7.2 Computing Resources, Software, and/or Data are Corrupted: added new requirements specific to notifications if a CRL cannot be issued. • Section 5.8 CA and RA Termination: added requirements regarding notification in the event of CA termination. • Section 6.3.2 Certificate Operational Periods and Key Usage Periods: removed language specific to FPKI and removed references to Code Signing Certificates which are not offered by IdenTrust under IGC • Section 6.8 Time Stamping: added language clarifying when manual adjustments may be made to synchronize time.

Version	Date	Summary of Changes/Comments
		• Section 7.1.3 Algorithm Object Identifiers: removed reference to SHA1 algorithms.
1.5.4	April 14, 2021	Alignment of new SAFE Identity CP 1.0 and DirectTrust V2.0 policy documents. Updated Trusted Roles to clarify PKI responsibilities.
1.5.5	March 1, 2022	• 1.2.1 Alphanumeric Identifier-Updated version references. • 1.2.2.1 Assurance Levels-Separated into subsections. • 1.2.2.1.1 Basic Assurance Certificates-Moved content into subsection. • 1.2.2.1.2 Non-Human Certificates-Moved content into subsection. • 1.2.2.1.3 Medium Hardware and PIV-I Certificates-Moved content into subsection. • 1.3 PKI Entities-Aligning language in CP to CPS content. • 1.3.1.3 Participant CAs-Updated section number. • 1.3.1.4 IdenTrust Policy Management Authority (PMA)-Updated section number. • 1.3.1.5 Certificate Status Servers/Authority (CSS/CSA)-Updated section number. • 1.3.2.1 External RAs-Added subsection. • 1.3.5.3.1 Primary Machine Operator-Moved content into subsection. • 1.3.5.3.2 Secondary Machine Operator-Moved content into subsection. • 1.5.4.1 RPS Approval Procedures-Added new content to address RPS approval process. • 2.2.3 Interoperability-Updated section number. • 3.1.1.1 Human (non-PIV-I)-Added requirement regarding use of UUID to ensure name uniqueness. • 3.1.1.3 PIV-I Certificates-Added subsection. • 3.1.1.3.1 PIV-I (Except for Card Authentication)-Added subsection. • 3.1.1.3.3 PIV-I Content Signing-Added subsection. • 3.1.1.4 Device-Added subsection. • 3.1.1.5 Subordinate CAs-Added subsection. • 3.1.1.6 Root CA-Added subsection. • 3.1.1.7 Cross-Certifying Bridge CA-Added subsection. • 3.1.5 Uniqueness of Names-Added subsection. • 3.1.5.1 Subscriber Certificates-Added subsection. • 3.1.5.2 Subject Identifier (subjectID)-Added subsection. • 3.1.5.3 Unique Identifier (UID)-Added subsection and requirement that PIV-I card number cannot be used for UUID. • 3.1.5.4 Device Certificates-New content regarding Device Certificates. • 3.2.3.1.1 Basic Identity -Added subsection. • 3.2.3.1.2 Medium (all)-Added subsection. • 3.2.3.1.3 PIV-I Hardware-Added subsection. • 3.2.3.1.5.2 Mobile Phone Verification-Added subsection. • 3.2.3.1.7.2.1 Collection of Identity Data from an Antecedent In-Person Appearance-Updated section number. • 3.2.3.1.7.2.2 Records Retention-Updated section number. • 3.3.1 Identification and Authentication for Routine Re-Key-Added subsection. • 3.3.1.1 Basic and Medium (all policies) - Added subsection. • 3.3.1.2 PIV-I - Added subsection. • 3.3.1.3 LRAs - Added subsection. • 3.3.1.4 SubCAs, RAs and the Cross-Certifying Bridge CA-Added subsection • 4.1.2.1 Establishment of Identity-Clarified language pertaining to RA Certificate Requests.

Version	Date	Summary of Changes/Comments
		• 6.2.1.1 Custodial Subscriber Key Stores-Removed first paragraph requirement for periodic Activation Data change in CP. • 6.2.10.1 Methods of Destroying Private Keys for Subscribers-Added subsection to CP. • 6.2.10.2 Methods of Destroying Private Keys for CA, CSA, CMS, and RA System-Added subsection to CP. • 6.2.3.3 Escrow of Subscriber Private Signature Keys-Split RA content out of Subscriber content and renumbered Section in CP. • 6.2.3.4 Escrow of Subscriber Private Encryption and Dual Use Keys-Split RA content out of Subscriber content and renumbered Section in CP. • 6.2.4 Private Key Backup-Renumbered section to realign in CP. • 6.2.4.2 Backup of RA Private Signature Key-Renumbered section to realign in CP. • 6.2.4.3 Backup of Subscriber Private Signature Key-Renumbered section to realign in CP. • 6.2.8.1 Method of Activating Private Keys for Subscribers-Added subsection to CP. • 6.2.8.2 Method of Activating Private Keys For PIV-I-Added subsection to CP • 6.2.8.3 Method of Activating Private Keys for CA, CSA, RA, and CMS-Added subsection to CP. • 6.5.1 Specific Computer Security Technical Requirements-Added clarifying content regarding equipment configurations. • 7.1.1.1 Serial Numbers-Added subsection. • 7.1.3.1 Signature Algorithm OIDs-Updated and numbered table • 7.1.3.2 Subject Public Key Information-Updated and numbered table • 7.1.3.3 Elliptic Curve Public Key-Updated and numbered table • 7.1.4 Name Forms-Updated and numbered table • 9.12.1 Procedure for Amendment - Updated URL to https://www.identrust.com/support/documents/igc-standard • Reference to High Assurance Level-Removed section and content. • Reference to Rudimentary Assurance Level-Removed section and content.
1.5.6	March 31, 2023	• Updates based on the FBCA Policy v3.0 in these sections: o Overall updates from “Shall” to “Must” or actionable task o 1.3.7 added “Other Participants”. o 1.4.2. Added reference to “id-fpki-certpcy-pivi-cardAuth”. o 2.2.1, 2.4, 4.3.1.3, and 4.4.2 Updated PIV-I Authentication and Card Authentication Certificates not to be distributed via public repositories. o 2.3 Updated Frequency of Publication within 30 days. o 3.1.1.1 Added Group Certificates issuance under non-PIV-I Subscribers. o 3.1.2 Common Name updates. o 4.4.3 Added notification of CA Certificate issuance to other entities within 24 hours. o 4.6.6, 4.7.6, and 4.8.6 Removed text referenced in 4.4.2. o 4.9.7 CRL updates from 31 to 35 days. o 4.9.9 Added CRL and OCSP details. o 5.3.3 Updated details for Training Requirements. o 5.3.5 Updated details for Job Rotation Frequency. o 5.4.2 Updated frequency of Processing Log from 60 to 30 days. o 5.5.1 Updated Types of Events Archived table. o 5.7 added statement for Security Incidents. o 5.7.1.1 Updated CA Incident Reporting.

Version	Date	Summary of Changes/Comments
		o 6 Moved statement in 6.1 to footer area. o 6.2.7 Added details for Private Key Storage on Cryptographic Module. o 6.3.2 Update IGC PIV-I Container Signer Certificate lifetime from 8 to 9 years. o 6.5.2 Added Computer Security Rating statement. o 6.6.3 Updated from "No stipulation" adding details to Life Cycle Security Controls. o 6.7 Added the last 2 paragraphs for Network Security Controls. o 6.8 Added Timestamping details o 7.1.1.1 Updated Serial Number details from at least 20-bits to at least 60-bits entropy referencing pseudo -random generator. o 7.1.3.1 Updated table 13 with Sha384 and sha-512 algorithms. o 7.1.6 Added reference to PIV-I Card Authentication and PIV-I Content Signing Certificates. o 9.2.3 Updated from "No stipulation" adding reference to 9.2.1. o 9.3.3 Added reference to applicable agreements. o 9.17 Added references to Other Provisions. • Moved the Revision History table to this Section 1.2 per RFC 3647 • 1.2.2.4, 1.3.1.2, 1.6.1, 1.6.2, 4.1, 7.1.4, and 12 Removed SAFE Identity references as no longer offered by IdenTrust • Removal of deprecated OIDs in Section 1.2.2.2 • 1.6.1 Added/Updated definitions: "Key", "Out-of-Band", "Two-Person-Control". • 1.6.2 added acronyms: AES, AIA, AID, APL, CIO, CISA, CN, FIPS, FPKI, FPKIPA, GSA, HSM, HTTP, IEFTF, ITAR, ITU, ITU-T, MOA, NACI, NACLC, PII, SIA, S/MIME, and SP. • 7.3.2 Updated OCSP extension requirement. • 9.11 Added missing sub-headers. • 10 – removed as supplicated in Appendix A. • Section 11 removed as the referenced documents are in section 1.1.4 Scope.
1.5.7	August 18, 2023	• Updates based on the FBCA 2021-2022 audit feedback mapping the same sections of the FBCA CP with the IGC CP/CPS and on the FBCA CP versions 3.1 and 3.2: o 1.1.5 Added missing section o 1.3.1.1 thru 1.3.1.5 added missing sections o 1.3.2.1 thru 1.3.2.2 added missing sections o 1.3.6 thru 1.3.7.2, Added missing sections o 2.1, Added first paragraph o 3.1.1, 3.1.1.1, 3.1.1.2, Updates to match the CP o 3.5 thru 3.5.5, Added missing sections o 4.12.1.2.2 thru 4.1.12.3.5, Added missing sections o 5.1.2.5 thru 5.1.2.7, Added missing sections o 5.2.1.3 thru 5.2.1.3.2, Added missing sections o 5.4.1/5.5.1, updated types of events recorded/archived o 5.7.3.2, Added missing section o 6.1.1.3 and 6.1.1.4, Added missing sections o 6.3.2, updated certificate operational periods o Appendix C, D, and E, Added • 1.2.2.2.6, DirectTrust OIDs updates • 4.12.3 thru 4.12.4 added missing sections • 5.2.1, Added Development Operations and Software Engineer Trusted Roles • 5.2.1.8.7 Added Software Engineer Trusted Role

Version	Date	Summary of Changes/Comments
		• 5.2.1.8.8 Added Development Operations Trusted Role • 5.2.4, Added Development Operations and Software Engineer Trusted Roles • 5.5 Added text from the CPS
1.5.8	September 15, 2023	• Updated some section titles
1.5.9	September 23, 2024	• Updated the section numbering through the document where needed. • 1.2.2 Removed Table 1 language and moved to CPS • 1.2.2.1 Added Assurance Level language • 1.2.2.1.3 Added Medium Software Certificate section • 1.2.2.2 Removed OID's • 1.3.6 Added key escrow and recovery language • 1.3.7 Added key escrow and recovery language • 1.3.8.1 Added role clarification language • 1.3.10 Removed language from the CP and added it to the CPS • 1.3.11.1 Removed language as is not public facing • Updated Assurance Level definition • 3.1.1.1 Removed redundant language • 3.1.2 Added Human Subscribers • 3.1.3 Added CA language • 3.1.5 Added additional CA language • 3.1.6 Added PMA language • 3.1.6.1 Removed section and moved to 3.1.6 • 3.2.3 Added FPKI requirement • 3.2.3.1 Removed redundant language • 3.2.3.1 Updated requirement language • 3.2.3.1.1 Added requirement language • 3.2.3.1.2 Added requirement language • 3.2.3.4 Removed language from the CP and added it to the CPS • 3.5 Added key escrow and recovery language • 4.1.2 Added FPKI Requirement • 4.2.1 Removed language from the CP and added it to the CPS • 4.2.2 Removed language from the CP and added it to the CPS • 4.2.3 Updated requirement • 4.3.1 Added FPKI requirement • 4.5.1 Removed language from the CP and added it to the CPS • 4.7.1 Added subscriber and participant language • 4.8.2 Added more specification • 4.8.3 Added Requirement language • 4.9.7.1 Updated requirement • 4.9.16 Added Mechanism language • 5.1 Updated more specific Physical Control language • 5.1.4 Updated requirement • 5.1.6 Removed language from the CP and added it to the CPS • 5.1.7 Added more specific language • 5.2.1 Added language to Trusted role section • 5.2.1.2 Added section • 5.2.1.3 Added section • 5.3.1 Updated section title • 5.3.6 Updated language • 5.4.5 Added FPKI Language • 5.4.6 Added FPKI Language

Version	Date	Summary of Changes/Comments
		• 5.4.8 Added FPKI Language • 5.7 Added FPKI Language • 5.7.1 Removed language and moved to section 5.7 • 6.1.1 Added FPKI Language • 6.1.1.1 Added FPKI Language • 6.1.1.1.1 Added cryptographic language • 6.1.6 Added validation language • 6.1.7 Added PIV-I language • 6.2.3 Added FPKI Language • 6.2.3.1 Removed section • 6.2.3.2 Removed section • 6.2.5 Added FPKI Language
1.6.0		• Added Hyperlinks to all section references throughout the CP document • 1.1.4 Updated Bridge date • 1.2.2.2 Updated the PIV-I, Medium Device Software & Medium Device Hardware OID's to include (2.16.840.1.101.3.2.1.3.47) as called out in audit Added 2.16.840.1.113839.0.100.37.1 and 2.16.840.1.113839.0.100.38.1 with a comment "To be deprecated" as called out in audit. • 1.3.2 Updated section title to be in-line with the Bridge, updated some language • Added section 1.3.6.1 Key Escrow Database as instructed by FPKI • Added section 1.3.6.2 Data Decryption Server as instructed by FPKI • Added section 1.3.6.3 Key Recovery Agent as instructed by FPKI • Added section 1.3.6.4 Key Recovery Official as instructed by FPKI • Added section 1.3.7.1 Internal Third-Party Requestor as instructed by FPKI • Added section 1.3.7.2 External Third-Party Requestor as instructed by FPKI • Updated Custodian definition • Added Key Recovery Agent definition • Added Key Recovery Official definition • 3.1.1.1 Updated language and added additional bullet points, to align with the Bridge • Removed wording and added to CPS • 3.2.3.1.3 Added bullet for Supervised Remote in-person Proofing • 3.2.3.4.2 Updated language • 3.2.4 Updated language • 3.3.1.1 Updated and Removed language to align with the Bridge • Added section 3.5.1 KRA Authentication as instructed by FPKI • Added section 3.5.2 KRO Authentication as instructed by FPKI • Added section 3.5.3 Subscriber Authentication as instructed by FPKI • Added section 3.5.4 Third-Party Requestor Authentication as instructed by FPKI • Added section 3.5.5 Data Decryption Server Authentication as instructed by FPKI • 4.1.2 Updated language • 4.3.1.1 Removed section • 4.3.1.2 Removed section • 4.3.1.3 Removed section • 4.4 Added this section • 4.6.3 Updated Language • 4.8 Updated language • 4.8.3.1 Removed language and added to CPS

Version	Date	Summary of Changes/Comments
		• 4.12 Added language • Added section 4.12.1 as instructed by FPKI • Added section 4.12.1.1 as instructed by FPKI • 4.12.2 Updated language • Added section 4.12.2.1 as instructed by FPKI • Added section 4.12.2.2 as instructed by FPKI • Added section 4.12.2.2.1 as instructed by FPKI • Added section 4.12.2.2.2 as instructed by FPKI • Added section 4.12.2.2.3 as instructed by FPKI • Added section 4.12.2.2.4 as instructed by FPKI • Added section 4.12.2.3 as instructed by FPKI • Added section 4.12.2.3.1 as instructed by FPKI • Added section 4.12.2.3.2 as instructed by FPKI • Added section 4.12.2.3.3 as instructed by FPKI • Added section 4.12.2.3.4 as instructed by FPKI • Added section 4.12.2.3.5 as instructed by FPKI • Removed section 4.10.3 • Removed section 4.10.3.1 • 5.2.1 Updated & Removed language and added to CPS • Added section 5.2.1.3.1 • Added section 5.2.1.8 • 5.2.2 Updated language • 5.3.5 Updated Language • 5.7.3.5 Updated Language • 5.7.3.6 Updated Language • 5.8 Updated language • 6.1.1.1 Updated language • 6.1.1.1.1 Updated language • 6.1.1.1.2 Updated language • 6.1.3 Updated language • 6.1.4 Updated language • 6.2.1 Updated language • 6.2.9 Updated language • 6.3.2 Updated language • 6.5.2 Removed language and added to CPS

1.2.1 Alphanumeric Identifier

The alphanumeric identifier (i.e., the title) for this CP is the "IdenTrust Global Common Certificate Policy, Version 1.6.0" dated October 2025.

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. See Table 1 below.

Certificates Issued under this CP must assert one or more of the Certificate Policy OIDs in *Table 1* ***CP Certificate Names, Assurance Levels, Types and Certificate Policy OIDs,*** below. For each named Certificate, one or more Certificate Types may be Issued, depending on customer requirement and use case.

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 SubCAs that are signed under this CP. In this case, Certificate policy OIDs

are detailed in the CPS, the Certificate Profile and the specific CP correlated to the SubCA signed under this policy.

Certificates may use additional OIDs to assert affiliations, compliance, intended usages or other purposes. All IGC specific Certificate policy OIDs in Table 1 refer to the most current versions of the CPS, the IGC Certificate Profiles and any other IGC related policy documents. All OIDS that are designated in cross-certified CP documents are provided in the CPS and incorporated into the IGC Certificate Profiles.

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

1.2.2.1 Assurance Levels

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

1.2.2.1.1 Basic Assurance Certificates

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 may be asserted to allow Relying Parties an ability to distinguish Certificate storage type. Basic Hardware and Basic Software Certificates are Assurance Level of Basic.

1.2.2.1.2 Non-Human Certificates

Any Certificate issued to a Device must assert the OID or OIDs associated in *Table 1* ***CP Certificate Names, Assurance Levels, Types and Certificate Policy OIDs***, with a single "Certificate Name" listed among the following "Certificate Names":

- IGC Medium Device Software,
- IGC Medium Device Hardware,
- IGC PIV-I Content Signing.

All other policies defined in this CP are reserved for human Subscribers.

1.2.2.1.3 Medium Software Certificates

Unless otherwise specified, requirements stated for Medium Software Certificates are identical to Basic Assurance Certificates, except for identity proofing, re-key and activation data.

1.2.2.1.4 Medium Hardware and PIV-I Certificates

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 CMS for the purpose of signing PIV-I card security objects.

1.2.2.2 IGC OIDs Table

The following table provides all IGC OIDs:

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

Certificate Name	Assurance Level	Certificate Type	IdenTrust Policy OID	Federal Bridge Policy OID
IGC Basic Software	Basic	Signing Certificate	2.16.840.1.113839.0.100.2.1	2.16.840.1.101.3.2.1.3.2
		Signing Certificate	2.16.840.1.113839.0.100.2.3	
		Encryption Certificate	2.16.840.1.113839.0.100.2.2	

Certificate Name	Assurance Level	Certificate Type	IdenTrust Policy OID	Federal Bridge Policy OID
		Encryption Certificate	2.16.840.1.113839.0.100.2.4	
IGC Basic Hardware	Basic	Signing Certificate	2.16.840.1.113839.0.100.2.5	2.16.840.1.101.3.2.1.3.2
		Encryption Certificate	2.16.840.1.113839.0.100.2.6	
		Card Authentication Certificate	2.16.840.1.113839.0.100.2.7	
		Identity Certificate	2.16.840.1.113839.0.100.2.8	
IGC Medium Software	Medium Software	Signing Certificate	2.16.840.1.113839.0.100.3.1	2.16.840.1.101.3.2.1.3.3
		Encryption Certificate	2.16.840.1.113839.0.100.3.2	
		Group Organization Signing Certificate	2.16.840.1.113839.0.100.3.3	
		Group Organization Encryption Certificate	2.16.840.1.113839.0.100.3.4	
		Group Address Signing Certificate	2.16.840.1.113839.0.100.3.5	
		Group Address Encryption Certificate	2.16.840.1.113839.0.100.3.6	
IGC Medium Software CBP	Medium Software CBP	Signing Certificate	2.16.840.1.113839.0.100.14.1	2.16.840.1.101.3.2.1.3.14
		Encryption Certificate	2.16.840.1.113839.0.100.14.2	
IGC Medium Hardware	Medium Hardware	Signing Certificate	2.16.840.1.113839.0.100.12.1	2.16.840.1.101.3.2.1.3.12
		Encryption Certificate	2.16.840.1.113839.0.100.12.2	
		Card Authentication Certificate	2.16.840.1.113839.0.100.12.3	
		Identity Certificate	2.16.840.1.113839.0.100.12.4	
IGC Medium Hardware CBP	Medium Hardware CBP	Signing Certificate	2.16.840.1.113839.0.100.15.1	2.16.840.1.101.3.2.1.3.15
		Encryption Certificate	2.16.840.1.113839.0.100.15.2	
		Card Authentication Certificate	2.16.840.1.113839.0.100.15.3	
		Identity Certificate	2.16.840.1.113839.0.100.15.4	
IGC PIV-I Hardware	PIV-I Hardware	Identity Certificate	2.16.840.1.113839.0.100.18.0	2.16.840.1.101.3.2.1.3.18
		Signing Certificate	2.16.840.1.113839.0.100.18.1	
		Encryption Certificate	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	2.16.840.1.101.3.2.1.3.19
IGC PIV-I Content Signing	PIV-I Content Signing	PIV-I Content Signing Certificate	2.16.840.1.113839.0.100.20.1	2.16.840.1.101.3.2.1.3.20 2.16.840.1.101.3.2.1.3.47
IGC Medium Device Software	Medium Device Software	To be deprecated Device Certificate	2.16.840.1.113839.0.100.37.1 2.16.840.1.113839.0.100.37.2	2.16.840.1.101.3.2.1.3.37
IGC Medium Device Hardware	Medium Device Hardware	To be deprecated Device Certificate	2.16.840.1.113839.0.100.38.1 2.16.840.1.113839.0.100.38.2	2.16.840.1.101.3.2.1.3.38

1.2.2.3 DirectTrust OIDs

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

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

Certificate Name	Assurance Level	Certificate Type	IdenTrust Policy OID	DirectTrust OID
Covered Entities (CE) IGC Medium Software	Medium Software	Group Organization Signing Certificate	2.16.840.1.113839.0.100.3.3	1.3.6.1.4.1.41179.2.1 (CE) 1.3.6.1.4.1.41179.0.2.0 (CP) 1.3.6.1.4.1.41179.1.5 (IAL2 Assurance)
		Group Organization Encryption Certificate	2.16.840.1.113839.0.100.3.4	
		Group Address Signing Certificate	2.16.840.1.113839.0.100.3.5	
		DirectTrust Address Signing		
		Group Address Encryption Certificate	2.16.840.1.113839.0.100.3.6	
		DirectTrust Address Encryption		
Business Associates (BA) IGC Medium Software	Medium Software	Group Organization Signing Certificate	2.16.840.1.113839.0.100.3.3	1.3.6.1.4.1.41179.2.2 (BA) 1.3.6.1.4.1.41179.0.2.0 (CP) 1.3.6.1.4.1.41179.1.5 (IAL2 Assurance)
		Group Organization Encryption Certificate	2.16.840.1.113839.0.100.3.4	
		Group Address Signing Certificate	2.16.840.1.113839.0.100.3.5	
		DirectTrust Address Signing		
		Group Address Encryption Certificate	2.16.840.1.113839.0.100.3.6	
		DirectTrust Address Encryption		
Healthcare Entities (HE) IGC Medium Software	Medium Software	Group Organization Signing Certificate	2.16.840.1.113839.0.100.3.3	1.3.6.1.4.1.41179.2.3 (HE) 1.3.6.1.4.1.41179.0.2.0 (CP) 1.3.6.1.4.1.41179.1.5 (IAL2 Assurance)
		Group Organization Encryption Certificate	2.16.840.1.113839.0.100.3.4	
		Group Address Signing Certificate	2.16.840.1.113839.0.100.3.5	
		DirectTrust Address Signing		
		Group Address Encryption Certificate	2.16.840.1.113839.0.100.3.6	
		DirectTrust Address Encryption		
Patients IGC Medium Software	Medium Software	Group Organization Signing Certificate	2.16.840.1.113839.0.100.3.3	1.3.6.1.4.1.41179.2.4 (Patients) 1.3.6.1.4.1.41179.0.2.0 (CP) 1.3.6.1.4.1.41179.1.5 (IAL2 Assurance)
		Group Organization Encryption Certificate	2.16.840.1.113839.0.100.3.4	
		Group Address Signing Certificate	2.16.840.1.113839.0.100.3.5	
		DirectTrust Address Signing		

Certificate Name	Assurance Level	Certificate Type	IdenTrust Policy OID	DirectTrust OID
		Group Address Encryption Certificate	2.16.840.1.113839.0.100.3.6	
		DirectTrust Address Encryption		
Non-Declared Entities (ND) IGC Medium Software	Medium Software	Group Organization Signing Certificate	2.16.840.1.113839.0.100.3.3	1.3.6.1.4.1.41179.2.5 (ND) 1.3.6.1.4.1.41179.0.2.0 (CP) 1.3.6.1.4.1.41179.1.5 (IAL2 Assurance)
		Group Organization Encryption Certificate	2.16.840.1.113839.0.100.3.4	
		Group Address Signing Certificate	2.16.840.1.113839.0.100.3.5	
		DirectTrust Address Signing		
		Group Address Encryption Certificate	2.16.840.1.113839.0.100.3.6	
		DirectTrust Address Encryption		

Valid DirectTrust OIDs not currently used in IGC Certificate end-entity profiles:

- 1.3.6.1.4.1.41179.1.1,
- 1.3.6.1.4.1.41179.1.2; and
- 1.3.6.1.4.1.41179.1.4

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.

1.3.1 PKI Authorities

1.3.1.1 Federal Chief Information Officers Council

No stipulation.

1.3.1.2 Federal PKI Policy Authority (FPKIPA)

No stipulation.

1.3.1.3 Federal PKI Management Authority (FPKIMA)

No stipulation.

1.3.1.4 FPKI Management Authority Program Manager

No stipulation.

1.3.1.5 IdenTrust Policy Management Authority (PMA)

The PMA shall oversee the adoption of this CP and the administration of this CP with CAs, RAs, Certificate Status Authorities, and other PKI Participants.

The PMA must also be responsible for approving the cross-certification of other policies to this CP.

1.3.1.6 IdenTrust Global Common PKI Participants

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

1.3.2 Certification Authority (CA)

IdenTrust is the Principal Certificate Authority and may issue Certificates that are cross-certified under other Certificate Policies.

A 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. This CA operates as a root under this policy. SubCA Certificates are Issued by the IGC Root CA. Certificates are Issued to Subscribers by SubCAs.

The IGC Root CA, may also issue SubCA Certificates to well-established 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 IGC CPS. A Participant CA is prohibited from issuing CA Certificates to any entity other than for the purpose of Cross-certification. There must 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 SubCA Certificate has been Issued to IdenTrust or a Participant CA. In other words, the CA Private Keys of all SubCAs must be in the custody of IdenTrust. The IGC Root CA and all SubCAs 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 SubCAs are required to be in custody of IdenTrust on behalf of that party. The IGC Root CA and all SubCAs that are part of the IGC PKI are referred to herein as Certification Authorities or "CAs."

This CPS is an assertion of the Certificate policies that IdenTrust, Participant CAs, RAs and others implement, and they are bound by and must 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 Financial Responsibility*.

1.3.2.1 IdenTrust Cross-Certified Certification Authority (CA)

IdenTrust designates at least one CA within its PKI to receive a cross-certificate from the FBCA, referred to in this CP as the Entity cross-certified CA. In addition, this CP may refer to CAs that are "subordinate" to the Entity cross-certified CA.

IdenTrust must ensure that no CA under its PKI shall have more than one trust path to the FBCA.

1.3.2.2 Federal Bridge Certification Authority (FBCA)

The FBCA is operated by the FPKIMA and is authorized by the FPKIPA to create, sign, and issue public key certificates. As operated by FPKIMA, the FBCA is responsible for all aspects of the issuance and management of a certificate including:

- The certificate manufacturing process,
- Publication of certificates,

- Revocation of certificates,
- Re-key of FBCA signing material, and
- Ensuring that all aspects of the FBCA services and FBCA operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of the "X.509 Certificate Policy for the Federal Bridge Certification Authority".

1.3.3 Card Management System (CMS)

The CMS manages smart card token content. In this policy the context regarding CMS requirements are generally associated with the PIV-I policies; however, an External RA may also use the CMS to request Smart card credentials that are not PIV-I, as noted in specific sections of this CP. 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 meets the requirements described in this CP, including requirements stated in Appendix B. A CMS must not be issued any Certificates that express the PIV-I Hardware or PIV-I Card Authentication policy OID.

1.3.4 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. 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 must 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 must be accomplished in a secure manner ensuring confidentiality and integrity.

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

1.3.4.1 External RAs

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

1.3.5 Certificate Status Servers/Authority (CSS/CSA)

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 must provide an OCSP-based CSS.

1.3.6 Key Recovery Authorities

While IdenTrust supports the escrow of encryption keys for enterprise entities who may need it, the recovery of escrowed keys is the responsibility of the enterprise entity via CMS.

1.3.6.1 Key Escrow Database

The KED is defined as the function, system, or subsystem that maintains the key escrow repository and responds to key registration requests. The KED also responds to key recovery requests from two or more KRAs or self-recovery by a current subscriber.

1.3.6.2 Data Decryption Server

A DDS is an automated system that has the capability to obtain subscriber private keys from the KED or another DDS for data monitoring or other purposes (e.g., email inspection). DDSs do not provide keys to Subscribers or other Third-Party Requestors. A DDS has access to escrowed key management keys and must meet all security requirements of the KED as outlined in this policy.

Implementation of a DDS is optional based on organizational operations.

1.3.6.3 Key Recovery Agent

A KRA is an individual who is authorized, as specified in the applicable Practice Statement (KRPS or CPS), to recover an escrowed key. The KRAs have high level, sensitive access to the KED and are considered Trusted Roles (see Section 5.2.1). KRAs can recover large numbers of keys, the number and location of KRAs should be closely controlled.

A KRA performs the following functions:

- Confirm validity and completeness of requests,
- Recover copies of escrowed keys; and
- Distribute copies of recovered keys to Requestor, with protection as described.

KRAs may conduct requestor identity verification and authorization validation when KROs are not used.

1.3.6.4 Key Recovery Official

Organizations may opt to appoint a Key Recovery Official (KRO) to support key recovery requestor identity verification and authorization validation tasks; however, a KRO is not a Trusted Role.

A KRO's responsibilities are to perform the following functions: 9

- Verify a Requestor's identity and authorization as stated by this policy,
- Assist authorized requestors in building key recovery requests,
- Utilize secure communication for key recovery requests to and responses from the KRA; and
- Participate in the distribution of escrowed keys to the Requestor, ensuring that it occurs as described by the associated practice statement (CPS or KRPS).

1.3.7 Key Recovery Requestors

While IdenTrust supports the escrow of encryption keys for enterprise entities who may need it, the recovery of escrowed keys is the responsibility of the enterprise entity via CMS.

1.3.7.1 Internal Third-Party Requestor

An Internal Third-Party Requestor is any Requestor who is in the Subscriber's supervisory chain or is otherwise

authorized to obtain the Subscriber's key for the Issuing Organization (i.e., the organization on behalf of which the CA issues certificates to subscribers).

1.3.7.2 External Third-Party Requestor

An External Third-Party Requestor is someone (e.g., investigator) outside the Issuing Organization with a court order or other legal instrument to obtain the decryption private key of the Subscriber.

1.3.8 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).

1.3.8.1 Custodian

A Custodian is an organization 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 (authorized third party), who is appointed by the Custodial entity (organization) is typically referred to as the Information System Security Officer (ISSO).

1.3.9 Affiliated 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 must be indicated with the presence of a DN in the subject field in the Certificate. Certificates expressing affiliation must be Revoked in accordance with Section *4.9 Certificate Revocation and Suspension* when the affiliation is terminated.

1.3.9.1 Local Registration Authority (LRA)

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 Personnel Controls*. 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.

1.3.9.2 Trusted Agent (TA)

Trusted Agents (TA) 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 must 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.

4. All activities of the Trusted Agent must be performed in accordance with the CP and CPS of the applicable CA. The duties to be performed by the Trust Agent include:
5. Performance of in-person identification of Applicants,
6. Collection of copies of supporting identity documentation,
7. Delivery of said documentation and/or supporting electronic input to the LRA for the applicable CA or RA; and
8. 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 must 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.

1.3.9.3 Machine Operators

Where Certificates are Issued to Devices, there must 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 CPS.

1.3.10 Relying Parties

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 Relying Party Public Key and Certificate Usage.* 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.

1.3.11 Other Participants

1.3.11.1 Certificate Policy Management Authority (PMA)

The PMA for this Policy is the IdenTrust Policy Management Authority, which administers Policy decisions.

1.3.11.2 Certificate Policy Manufacturing Authority (CMA)

The Issuing CA will remain ultimately responsible for the manufacture of IGC Certificates. However, the Issuing CA may subcontract manufacturing functions to third party CMAs who agree to be bound by this Policy.

1.3.11.3 Repositories

The Issuing CA will perform the role and functions of the Repository. The Issuing CA may subcontract the performance of the Repository functions to a third-party Organization that agrees to fulfill the functions of a Repository, and who agrees to be bound by this Policy, but the Issuing CA remains responsible for the performance of those services in accordance with this Policy.

1.3.11.4 PKI Sponsors

Individuals who are employed by the Sponsoring Organization or by an authorized agent who has express authority to represent the Organization but is not the Subscriber. The Sponsoring Organization must verify that PKI Sponsors are individuals that:

(i) sign and submit, or approve a request for a Certificate issued to an Electronic Device on behalf of the Organization, and/or
(ii) (ii) sign and submit a Certificate Agreements on behalf of the Organization, and/or
(iii) (iii) acknowledge and agree to the Certificate Terms of Use on behalf of the Organization when the Organization is an Affiliate of the CA.

1.3.11.5 Trusted Agents

Authorized entities acting as representatives of Affiliated Organizations to verify the Applicant's or PKI Sponsor's identification during the registration process. Trusted Agents must not have automated interfaces with CAs.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

The IdenTrust CA's appropriate Certificate shall be described in the 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 architecture that provides facilities for interference with encrypted communications, including, but not limited to:
    a. (a) active eavesdropping or
    b. (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.
iv. Certificates that map to id-fpki-certpcy-pivi-cardAuth must be used only to authenticate the hardware token containing the associated private key and must not be interpreted as authenticating the presenter or holder of the token.

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: policy@IdenTrust.com

1.5.3 Person Determining 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 must submit a CPS to the IdenTrust PMA for approval. The IdenTrust PMA must determine whether a CPS complies with this policy. The CA must meet all the CP requirements and receive written approval of the CPS from the IdenTrust PMA prior to commencing operations.

1.5.4.1 RPS Approval Procedures

All External RA Organizations must submit an RPS document to the IdenTrust PMA for approval. The IdenTrust PMA must determine whether the RPS complies with the ICP and CPS. The External RA receives written approval of the RPS from the IdenTrust PMA prior to being granted approval to operate.

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. 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

Term	Definition
Accept or Acceptance	Acceptance is a Subscriber act that triggers the Subscriber's rights and obligations with respect to the Certificate under this CP, and the 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 described 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 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.
Affiliated Certificate	A Certificate that is issued to an individual and the organization with which that individual is affiliated.
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.

Term	Definition
Assurance Level	Assurance Level is the strength and security of the authentication and the level of confidence the system has, depending on the type of credentials used, the number of authentication factors and the strength of the cryptographic transactions.
Authenticator Assurance Level (AAL)	A category describing the strength of the authentication process, per NIST SP-800-63B standards.
Authorizing Official	An Authorizing Official is an Individual designated in a written agreement within a CA, or RA who can appoint and authorize other Individuals to act as LRAs or Trusted Agents for that Organization.
Business Associate	A Business Associate (BA) helps Covered Entities carry out health care activities and functions under a written business associate contract or other arrangement with the Business Associate that establishes specifically what the Business Associate has been engaged to do and requires the Business Associate to comply with the requirements to protect the privacy and security of protected health information.
CA Certificate	The CA Certificate is an IdenTrust issued 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 must ensure that all CMSs meet the requirements described in this CP. The CMS must not issue any Certificates that express Assurance Levels of PIV-I Hardware or PIV-I Card Authentication.
Certificate	A Certificate is a computer-based record or electronic message that: (i) identifies the CA issuing it; (ii) names or identifies its subject (see Distinguished Name); (iii) contains the Public Key of the Subject; (iv) identifies the Certificate's Validity Period; (v) is Digitally Signed by a CA; and (vi) has the meaning ascribed to it in accordance with the legal infrastructure in which the Certificate is used (e.g., the CP, contractual agreements, and other system rules governing the course of dealing, usage and trade practice). A Certificate includes not only its actual content but also all documents expressly referenced or incorporated within.
Certificate Chain	A Certificate Chain is an ordered series of Certificates connecting a Subscriber's Certificate to the Root Certificate. Successive and superior CA and SubCA Certificates up to the Root Certificate connect superior Certificates (which may be self-signed) in a Certificate Chain. For Subscribers under this CP, a self-signed Root Certificate is Issued in compliance with this Policy.
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.

Term	Definition
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, • Group Domain-Bound Certificate; and • Group Address Certificate. Certificate Types are assigned unique Certificate policy OIDs and are listed in Table 1 by Certificate name and Assurance Level.
Certification Authority (CA)	A Certification Authority (CA) is an Organization that attests to the binding between an identity and cryptographic Key Pair. Certification Authority is more fully defined in Section 1.3.2.
Certification Practice Statement (CPS)	A Certification Practice Statement is a statement of the practices that a CA employs in creating, issuing, managing, and~~,~~ revoking Certificates in conformance with a particular CP.
Client (application)	A Client is a system entity, usually a computer process acting on behalf of a human user, which makes use of a service provided by a server.
Client-authenticated SSL/TLS-Encrypted Session	A Client-authenticated SSL/TLS-Encrypted Session is a session securely communicated through use of the Secure Sockets Layer and Transport Layer cryptographic protocols. For Client-authenticated SSL/TLS-Encrypted Sessions described 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 CMS 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 2 PKIs. The Cross Certificate is the Certificate Issued by 1 PKI to another PKI for Cross-certification.
Cryptographic Service Provider	A Cryptographic Service Provider is an independent software module or set of programs (e.g., an application program interface, or "API") used with a given Device to provide a concrete implementation of a set of cryptographic algorithms to be used for authentication, encoding, encryption and other cryptographic functions.
Cryptographic Module	A Cryptographic Module is the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Custodian	A Custodian is an organization or authorized third party 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.
Custodial Subscriber Key Store	A Custodial Subscriber Key Store holds keys for a number of Subscriber Certificates in one location.

Term	Definition
Data Decryption Server (DDS)	An automated system that obtains subscriber private keys from the Key Escrow Database or another Data Decryption Server in order to support decryption of data entering and leaving the Enterprise. An example of such data is e-mail.
Device	A Device is a non-human Subscriber of a Certificate. Examples of Devices include but are not limited to routers, firewalls, servers, and other Devices capable of securely handling Private Keys and properly implementing PKI technologies.
Device Certificate	A Device Certificate is a Certificate Issued to a Device and can be managed by a Machine Operator, Custodian, etc.
Digital Signature/Digitally Sign	A Digital Signature is the result of or mathematical transformation of a document or message through use of cryptography. To Digitally Sign a message is the act of applying a Digital Signature. A Relying Party in receipt of a document or message with a Digital Signature can accurately determine: (i) whether the transformation was created using the Private Key corresponding to the Public Key; and (ii) whether the message or document has been altered since the transformation was made.
Direct Project	The Direct Project is an initiative from the Office of the National Coordinator (ONC) for Health Information Technology that created a set of standards and services that, with a policy framework, enables simple, routed, scalable, and secure message transport over the Internet between known participants.
Directory Information Tree	A Directory Information Tree is data represented in a hierarchical structure containing the Distinguished Names (DNs) of directory service entries.
DirectTrust	DirectTrust.org, Inc. (DirectTrust) is a non-profit and competitively neutral entity operated by and for participants in the Direct community and other communities involved in electronic health information exchange that benefit from leveraging a healthcare-centric PKI. The Direct Project developed the original Direct Ecosystem Community Certificate Policy Version 0.9 in accordance with its consensus process.
DirectTrust Accredited Trust Anchor Bundle (ATAB)	The ATAB has as participants Health Information Service Providers (HISPs), Certificate Authorities (CAs), and Registration Authorities (RAs) that have achieved accreditation through either the DirectTrust HISP Accreditation Program for HISPs or the DirectTrust-EHNAC Trusted Agent Accreditation Program (DTAAP-CA/RA) for CA/RAs.
DirectTrust Certificates	DirectTrust Certificates are those Certificates that are Issued for use within Direct as defined in the Direct Project Applicability Statement for Secure Health Transport and more specifically by the DirectTrust Certificate Policy. DirectTrust Certificates may be Issued under this CP asserting IGC OIDs and OIDs belonging to DirectTrust, asserting compliance with DirectTrust CP.
Distinguished Name (DN)	A Distinguished Name is a unique name-identifier for the Issuer or the Subject of a Certificate so that he, she, or it can be located in a directory. For example, a DN might contain the following attributes: common name (cn), email address (e) or (mail), Organization name (o), Organizational unit (ou), locality (l), state (st) and/or country (c).
Domain Bound Certificate	A Domain Bound Certificate is a Certificate that contains a Health Domain Name in the form of a dNSName in the subjectCommonName and subjectAlternativeName extensions of the Certificate.
Encryption Certificate	An Encryption Certificate is a Certificate Issued to a Subscriber that can be only used for encryption services.
Enrollment Work Station (EWS)	An Enrollment Work Station is the customer side computer application that interfaces with the CMS to accomplish Certificate registration.
Fast Healthcare Interoperability Resources (FHIR)	FHIR is a draft standard describing data formats and elements and an application programming interface for exchanging electronic health records. The standard was created by the Health Level 7 International health-care standards organization.
Government Entity	A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Term	Definition
Group Address Certificate	A Group Address Certificate is a Group Certificate that contains a Health Endpoint Name in the Certificate subject. Group Address Certificates may be held by a third party that controls and manages access to the Private Key of the Certificate. See Section 3.2.3.3.2
Group Address Encryption Certificate	A Group Address Encryption Certificate is a Group Address Certificate that can be only used for encryption services.
Group Address Signing Certificate	A Group Address Signing Certificate is a Group Address Certificate that can only be used to create a Digital Signature.
Group Certificate	A Group Certificate can be either a Group Domain-Bound Certificate or a Group Address End-Entity Certificate.
Group Domain-Bound Certificate	A Group Domain-Bound Certificate is a domain bound Device Certificate that contains a Health Domain Name in the Certificate subject. Group Domain-Bound Certificates may be held by a third party that controls and manages access to the Private Key of the Certificate. See Section 3.2.3.3.1.
Group Domain-Bound Encryption Certificate	A Group Domain-Bound Encryption Certificate is a Group Domain-Bound Device Certificate that can be only used for encryption services.
Group Domain-Bound Signing Certificate	A Group Domain-Bound Signing Certificate is a Group Domain-Bound Device Certificate that can only be used to create a Digital Signature.
Government Agency	A Government Agency is an agency, unit, department, division, or other subdivision of any governmental authority of any jurisdiction.
Healthcare Entity	A Healthcare Entity (HE) is an entity involved in healthcare, that has agreed to protect private and confidential patient information consistent with the requirements of HIPAA although it is not a Covered Entity or Business Associate as defined under HIPAA at 45 CFR 160.103.
Health Information Service Provider (HISP)	A Health Information Service Provider (HISP) is an entity that processes Direct-compliant messages to and from Direct addresses, each of which is bound to a Direct-compliant X.509 digital Certificate. Acting in the capacity of an agent for the Subscriber, the HISP may hold and manage Private Keys associated with a DirectTrust Certificate on behalf of the Subscriber.
Health Domain Name	A Health Domain Name is a string conforming to the requirements of RFC 1034 and identifies the organization that assigns the Health Endpoint Names. Example: direct.sunnyfamilypractice.example.org. A Health Domain Name must be a fully qualified domain name, and should be dedicated solely to the purposes of health information exchange.
Health Endpoint Name	A Health Endpoint Name is a string conforming to the local-part requirements of RFC 5322. Health Endpoint Names express real-world origination points and endpoints of health information exchange, as vouched for by the organization managing the Health Domain Name. Example: johndoe (referring to in individual), sunnyfamilypractice, memoriallab (referring to organizational inboxes), diseaseregistry (referring to a processing queue).
Hypervisor	Computer software, firmware or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or virtual machine monitor.
ID Form	The ID Form a document incorporated into the Subscriber Agreement and is a document that, among other things (a) is used by the Applicant to provide personally identifying information as part of the Registration process, (b) must be signed by the Applicant, and (c) contains a declaration of identity by the Applicant.
Identification and Authentication (I&A)	Identification and Authentication is the process of affirming that a claimed identity is correct by comparing the claims offered by an Applicant with previously proven information. I&A requirements for this CP are fully described in Section 3.
Identity Assurance Level (IAL)	A category that conveys the degree of confidence that the Applicant's claimed identity is their real identity, per NIST SP-800-63A standards.

Term	Definition
Identity Certificate	An Identity Certificate is a Certificate Issued to a Subscriber that can be used to authenticate the Subscriber by a Relying Party.
Identity Verification Provider (IVP)	An Identity Verification Provider is an Organization that provides affirmation of identity and claims made by an Applicant in support of I&A. IVPs are considered authoritative and must able to demonstrate through policy and audit that the data is accurate and maintained with appropriate integrity, privacy, and confidentiality.
IdenTrust subjectID	An IdenTrust subjectID is included in the subjectDN field of Certificates as an (ou) attribute and, for Certificates where use includes authentication of the subject of the Certificate, is also utilized as a User Principal Name (UPN) structure in the subjectAlternativeName extension of the Certificate. The IdenTrust subjectID in any given Certificate issued by the IdenTrust CA is to be unique among IdenTrust subjectIDs operational within the PKI.
IdenTrust SubjID	Has the same meaning as IdenTrust subjectID.
Individual(s)	An Individual is a natural person and not a juridical person or legal entity.
Information System Security Officer (ISSO)	The Information System Security Officer is an individual who is responsible for establishing and maintaining the enterprise vision, strategy, and program as it relates to information systems security, to ensure information assets are adequately protected. The ISSO will play a role in authenticating the Subscriber application when a custodian-managed Group Certificate is issued under this policy.
Issue / Issuance	To Issue, or Issuance is the act performed by a CA in creating a Certificate, listing as Issuer itself or, alternately, listing as Issuer a name which the CA has obtained a license to use for such purpose. Issuance also involves notifying the Applicant of Certificate contents, that the Certificate has been created and that the Certificate is available for Acceptance.
Issuer	An Issuer is the Organization that owns a CA Private Key used to Digitally Sign Certificates and (a) is named (or uses a name to which it owns or has licensed for such purpose) as the Issuer in the Issuer DN field in a Certificate.
Issuing Certification Authority (Issuing CA)	An entity authorized by the PMA to issue and sign Certificates in accordance with the CPS and this CP.
Key	A general term used throughout this CP to encompass any one of the defined Keys mentioned in these general definitions section.
Key Compromise	Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
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 2 mathematically related Keys consisting of a Public Key and its corresponding Private Key. Key Pair properties ensure that: (i) 1 Key can be used to encrypt a message that can only be decrypted using the other Key; and (ii) even knowing 1 Key, it is computationally infeasible to discover the other Key.
Key Recovery Agent (KRA)	An individual authorized to interface with the key escrow database in conjunction with one or more other key recovery agents) to cause the key escrow database to carry out key recovery requests, as specified by this policy.
Key Recovery Official	An individual authorized to authenticate and submit key recovery requests to the Key Recovery Agent on behalf of requestor, as specified by this policy.
Key Recovery Policy (KRP)	A key recovery policy is a specialized form of administrative policy tuned to the protection and recovery of key management private keys (i.e., decryption keys) held in escrow. A key recovery policy addresses all aspects associated with the storage and recovery of key management Certificates.

Term	Definition
Key Storage Module (KSM)	A Key Storage Module is secure software or a hardware Cryptomodule used to store Private Keys and to perform private key operations such as Digital Signature generation. KSM is used in this policy to refer to Cryptomodules used by a Subscriber in daily operations. KSM is inclusive of software and hardware Cryptomodules as well as different form factors such as smart cards or USB tokens. See also Cryptographic Module.
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.
NPI Number	A National Provider Identifier or NPI is a unique 10-digit identification number issued to health care providers in the United States by the Centers for Medicare and Medicaid Services (CMS).
Non-Declared Entity	A Non-Declared Entity (ND) is an entity that has not asserted it will protect personal health information with privacy and security protections that are equivalent to those required by HIPAA and is not a Patient / Consumer.
Object Identifier (OID)	An Object Identifier is a unique numeric identifier registered under the ISO registration standard to reference a specific object or object class. OIDs are used within this 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. Out-of-band communications must protect the confidentiality and integrity of the data
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.

Term	Definition
Participant CA	A Participant CA is a legal entity that is Issued a Sub-CA Certificate by the IGC Root CA. A Participant CA is operated and managed by IdenTrust. The Participant enters into an Agreement with IdenTrust, which requires that IdenTrust operate the Participant CA and requires the Participant CA to follow and adhere to the provisions of this CP and the relevant CA 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
Registrar	A Registrar is the person performing the in-person confirmation of the Subscriber's identification. Some restrictions based on the specific IGC Certificate Assurance Level apply to the type of Registrar who can perform identification. Registrars who are eligible to perform in-person identification under this CP are: • LRAs • TAs • Licensed Notary or other person certified by a Government Agency who is certified as being authorized to confirm identities (e.g., a driver's license bureau employee, a Dept. of State consular office employee, a court clerk, or a county clerk).

Term	Definition
Registration	Registration is the process of receiving or obtaining a request for a Certificate from an Applicant, and collecting and entering the information needed from that Applicant to include in and support I&A and the Issuance of a Certificate.
Registration Agent	A Registration Agent is an Individual appointed directly by a CA or RA. A Registration Agent may also be an LRA or Trusted Agent appointed by a CA or RA or may also be a Licensed Notary or other official of a Government Agency. A Registration Agent assists CAs and RAs by providing in-person I&A in accordance with Section 3.
Registration Authority (RA)	A Registration Authority (RA) is an Organization that is responsible for collecting and confirming an Applicant's identity and any other information provided by Applicant for inclusion in a Certificate. Registration Authority is more fully defined in Section 1.3.3.
Registration Authority Agreement	A Registration Authority Agreement is an agreement entered into between an Organization and a CA authorizing the Organization to act as a Registration Authority for the CA, and detailing the specific duties and obligations of the RA, including but not limited to the procedures for conducting appropriate I&A on Applicants.
Registration Practices Statement (RPS)	The Registration Practices Statement (RPS) describes the registration practices of an External Registration Authority in performance of duties and obligations to fulfill the requirements of the IdenTrust Global Common Certificate Policy.
Relying Party	A Relying Party is an Organization, Subscriber, Device, or any entity that relies upon the information contained within a Certificate and upon Certificate status received from a CSA. Relying Party is more fully described in Section 1.3.8.
Repository	A Repository is an online system maintained by or on behalf of a CA for storing and retrieving Certificates and other information relevant to Certificates and Digital Signatures, including CPs, CPSs and information relating to Certificate validity or Revocation.
Requestor	A Requestor is an authorized agent of an Organization who invites an Individual to apply for an Affiliated Certificate.
Revocation or Revoke a Certificate	Revocation is the act of making a Certificate ineffective permanently from a specified time forward. Revocation is affected 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.
Secondary Machine Operators List	The Secondary Machine Operators List is a list of individuals who are designated by a Primary Machine Operator to act in the role of Secondary Machine Operator. Initial list of individuals so designated must be made in the Subscribing Organization Authorization Agreement prior the submission of the completed and fully executed Subscribing Organization Authorization Agreement to the CA in connection with an application Registration process for the relevant Device Certificate. Then after, from time to time, the Primary Machine Operator may submit an updated list to the CA as provided in the Subscribing Organization Authorization Agreement, and each such updated list, once recorded by the CA, must supersede the version of the list recorded by the CA prior to such updated list being recorded. The CA must record submitted to the CA in the Subscribing Organization Authorization Agreement as part of the Registration process in the CA database. Any updated lists provided to the CA by the Primary Machine Operator as provided for in the Subscribing Organization Authorization Agreement will be recorded by the CA by adding such updated list to the archived documents associated with the relevant Device Certificate account record.
Separation-of-Duties/Multi-party Control	Separation-of-Duties or Multi-party Control are procedures or techniques whereby no single Individual possesses the equipment or authorization to view, alter, or otherwise have access to sensitive or confidential information in a particular PKI. Tasks are separated into multiple subtasks and distributed to more than 1 Individual, requiring the participation of 2 or more Individuals to complete the task. The purpose of Separation-of-Duties and Multi-party Control is to reduce risk of PKI compromise.

Term	Definition
Server-Authenticated SSL/TLS-Encrypted Session	Server-authenticated SSL/TLS-Encrypted Sessions as described in the CP are those sessions in which a Subscriber or Client is directed to a specified secure URL (https://). The SSL-enabled client software confirms the identity of the IdenTrust secure server by validating the Certificate presented by the server. The subsequent session established is encrypted through use of the Secure Sockets Layer and Transport Layer Security cryptographic protocols.
Signing Certificate	A Signing Certificate is a Certificate Issued to a Subscriber that can be used to create Digital Signature to establish integrity of content.
Sponsor	A Sponsor is an Organization that authorizes Issuance of a Certificate to an Individual or a Device. (e.g., an employee's supervisor who authorizes the Issuance of a Certificate to the employee, or the head if an information systems department that authorizes Issuance of a Device Certificate to specific device). The Sponsor is responsible for either supplying or confirming Certificate attribute details to the CA or RA; and is also responsible for informing the CA or RA if the 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	An SSL / TLS Certificate is a Certificate Issued to a Device that is utilized to establish an encrypted session between a Client and a server. SSL/TLS Certificates are not issued under the IGC policy.
Subject Name or Subject Distinguished Name	See Distinguished Name.
Subordinate CA (SubCA)	A Subordinate CA is an Organization Issued a SubCA 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 the CP and this CP when performing RA functions.
Subscriber	A Subscriber is an end-entity Individual (Human Subscriber) or Device (Non-Human Subscriber) to whom or to which a Certificate is Issued. Subscribers may use Certificates for purposes indicated by the Certificate Type. Where Certificates are Issued to Devices, there must be an Individual (Primary Machine Operator) who is responsible for carrying out Subscriber duties.
Subscriber Agreement	The Subscriber Agreement is a legally binding contract that provides terms and conditions applicable to a Certificate that is applied for by an Applicant and, if Issued, Issued to that Applicant as the Subscriber of that Certificate.
Subscribing Organization	A Subscribing Organization is an Organization that authorizes affiliation with Subscribers. Subscribing Organization is more fully described in Section 1.3.7.
Subscribing Organization Authorization Agreement	The Subscribing Organization Authorization Agreement is completed by and submitted in conjunction with Registration for some types of Certificates.
Suspension or Suspend a Certificate	Suspension is the act of making a Certificate ineffective temporarily from a specified time forward. Suspension is affected by notation or inclusion in a set of Suspended Certificates (e.g., inclusion in a CRL).
System Transaction	The successful execution of all of the following components and steps: (i) Creation of a Digital Signature; (ii) Verification that the Subscriber's Digital Signature was created by the Private Key corresponding to the Public Key in the Certificate; and (iii) Verification that the Certificate was valid by using OCSP and the RFC 5280 certification path validation process as required by this CP and the CPS.
Trust Anchor	See Root Certificate.
Trusted Agent (TA)	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.

Term	Definition
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.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of 2 authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.
User Principal Name (UPN)	A User Principal Name is an attribute used in PKI, the format of such attribute being an Internet-style login name for a user based on the Internet standard RFC 822.
Virtual Machine Environment	An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine in a platform-independent environment. It consists of a host (virtual machine) and isolation kernel (hypervisor) and provides functionality needed to execute entire operating systems. At this time, allowed VMEs are limited to Hypervisor type virtual environments. Other technology, such as Docker Containers, is not permitted.
Validity Period	Validity Period is the intended term of validity of a Certificate, beginning with the notBefore date asserted in the Certificate and ending with the notAfter date asserted in the Certificate.
Zeroize	Zeroize is to erase electronically stored data by altering or deleting the contents of the data storage and overwriting with binary zeros so as to prevent the recovery of the data.

1.6.2 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AIA	Authority Information Access
AID	Application Identifier
APL	Approved Products List
ASN.1	Abstract Syntax Notation (version 1)
ATAB	Accredited Trust Anchor Bundle (DirectTrust)
BA	Business Associate
CA	Certification Authority
CHUID	Card Holder Unique Identifier
CE	Covered Entity
CIS	Certificate Information System
CMS	Card Management System
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority (interchangeable with CSS)
CSS	Certificate Status Server (interchangeable with CSA)
DDS	Data Decryption Server
DN	Distinguished Name – See Subject Name/Subject Distinguished Name
DNS	Domain Name System
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
EWS	Enrollment Work Station

Acronym	Definition
FIPS	Federal Information Processing Standard
FASC-N	Federal Agency Smart Credential Number
FBCA	U.S. Federal Bridge Certification Authority
FHIR	Fast Healthcare Interoperability Resource
FPKI	Federal Public Key Infrastructure
FPKIPA	Federal PKI Policy Authority
GSA	General Services Administration
HE	Healthcare Entity
HIPAA	HIPAA is the federal Health Insurance Portability and Accountability Act of 1996.
HISP	Healthcare Information Services Provider
HSM	Hardware Security Model
HTPP	Hypertext Transfer Protocol
IEFT	Internet Engineering Task Force
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
ITAR	International Traffic in Arms Regulation
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
IVP	Identity Verification Provider
KRP	Key Recovery Policy
KSM	Key Storage Module
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MOA	Memorandum of Agreement
NACI	National Agency Check with Written Inquiries
NACLC	National Agency Check with Law Enforcement Check
ND	Non-Declared Entity
NPI	National Provider Identifier OID
OCSP	Online Certificate Status Protocol
OOB	Out-of-Band
OTC	One Time Code
OTP	One Time Password
PII	Personally Identifiable Information
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
SIA	Subject Information Access
S/MIME	Secure Multipurpose Internet Mail Extension
SP	Special Publication
SSL/TLS	Secure Sockets Layer and Transport Layer Security

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

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The publicly accessible repository system must be designed and implemented to provide 99% availability overall and limit scheduled downtime to 0.5% annually.

2.1.1 IdenTrust Repository Obligations

CAs must operate repositories available over the internet to support their PKI operations for its own and all Relying Party populations.

Mechanisms used for posting information into a Repository must include:

- Hypertext Transfer Protocol (HTTP) or Directory Server Systems that provide access through encrypted Lightweight Directory Access Protocol (LDAP);
- 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 service availability and information as described in Section *4 Certificate Life-Cycle Operational Requirements*.

2.2 PUBLICATION OF CERTIFICATE INFORMATION

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

2.2.1 Publication of Certificates and Certificate Status

CA and Subscriber Certificates must only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties.

PIV-I Authentication and Card Authentication Certificates are not distributed via public repositories.

2.2.2 Publication of CA Information

The IdenTrust PMA must publish information concerning the IGC PKI necessary to support its use and operation. The CP and CPS must be publicly available on the IdenTrust web site:

https://www.identrust.com/support/documents/igc-standard.

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 Directory interoperability Profile*.

2.3 Time or Frequency of Publication

This CP and any subsequent changes must be made publicly available within 30 days of approval. CA Certificates must be published to the Repository within 7 days of Issuance. Certificates of Subscribers may be published to a publicly available Repository to the locations specified in the CA's CPS. CRLs must be published within 24 hours of issuance to the locations specified in the CA's CPS upon issuance.

2.4 Access Controls on Repositories

Any CA Repository information not intended for public dissemination or modification must be protected. Access to information in a CA's Repositories must 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 must make CA Certificates and CRLs published by the CA and CA Certificates Issued to the CA available to Relying Parties.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

A CA must only generate and sign Certificates that contain a non-null subjectDN complying with the X.501 standard. Certificates may also include other name forms in the subject alternative name field provided the field is marked as non-critical. This CP does not restrict the types of names that can be used.

Table *3 Level of Assurance Naming Requirements* (below) summarizes the naming requirements that apply to each level of assurance for this CP.

Table 3 - Level of Assurance Naming Requirements

Level	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 (All Policies) 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 must clearly indicate the Organization administering the CMS.

3.1.1.1 Subject Names

Certificates issued to Subscribers must include distinguished names that are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs).

A Device Subscriber name must be a unique name for the device and must not take the form of a Human Subscriber name.

Role-based and group certificates may be issued under any non-PIV-I human Subscriber policy.

- Role-based certificates identify a specific role on behalf of which one or more Subscribers are authorized to act rather than the Subscriber's name. Where the organization is implicit in the role, it may be omitted. Where the role alone is ambiguous, the organization must be present in the DN.
- The subjectName DN in a group certificate must not imply that the subject is a single individual, e.g., by inclusion of a human nme form.
- PIV-I Card Authentication subscriber certificates, use of the Subscriber's common name is prohibited, instead, the serialNumber = UUID is required.
  - For PIV-I cardAuth certificates with an Affiliated Organization:

    serialNumber=UUID, ou=Affiliated Organization Name {Base dn}

  - For PIV-I cardAuth certificates with no Affiliated Organization:

    serialNumber=UUID, ou=Unaffiliated, ou=entity CA's Name {Base dn}

- The UUID must 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"). The UUID may not be the serial number of the PIV-I card.
- For PIV-I Hardware Certificates asserting no affiliation, the subjectDN must contain the value "Unaffiliated" in the last Organizational unit (ou) attribute or for certificates asserting affiliation, the certificate must contain the Subscribing Organization name in the Organizational unit (ou) attribute. If the Organization does not have a specific need to include an Organizational unit (ou), the organization name may also be used for the value in the (ou).
  - For PIV-I Hardware certificates with no Affiliated Organization:

    cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name, (Base DN)

  - For PIV-I Hardware certificate with an Affiliated Organization

    cn=Subscriber's full name, ou=Affiliated Organization, (Base dn)

3.1.1.2 Subject Alternative Names

PIV-I Hardware and PIV-I Card Authentication certificates must include a subject alternate name extension, containing a UUID value encoded as a URI as specified in Section 3 of [RFC 4122].

PIV-I Card Authentication certificates must not include any other name in the subject alternative name extension.

Subscriber certificates that contain id-kp-emailProtection in the EKU must include a subject alternative name extension that includes a rfc822Name.

For Device Subscriber certificates that assert serverAuth in the Extended Key Usage, wildcard domain names are permitted in the dNSName value only if all sub-domains covered by the wildcard fall within the same application, cloud service, or system boundary within the scope of the sponsoring organization.

3.1.2 Need for Names to Be Meaningful

Names must identify the person or object to which they are assigned in a meaningful way. CA's must ensure an affiliation exists between the Subscriber and any Organization identified by any component of any name in its Certificate.

When DNs are used, the common name must represent the Subscriber in a way that is easily understandable for humans.

- For Human Subscribers, this will typically be a legal name.
- For equipment, this may be:
  a) FQDNs, IP addresses,
  b) program component identifiers,
  c) serial numbers or other (Subject Name) expressed similar identifiers within the Subject Common Name (cn) of the subjectDN of the Device Certificate.
- For non-PIV-I Certificates Issued to Individual Subscribers, that have no organizational affiliation, the subjectDN must contain the value “Unaffiliated” in the Organization (o) attribute. In the case of an affiliated Certificate Issued to an Individual Subscriber the subjectDN must contain the Subscribing Organization name in the Organization (o) attribute.

When UUID is required in the subject Distinguished Name, it must be appended to the Subscriber’s name and included in the Common Name (cn) attribute. Alternative methods of establishing uniqueness of names may be utilized providing that the format of attributes used to ensure uniqueness are compliant with the requirements of the FPKI profile document and RFC 5280 and have been approved by the IdenTrust PMA.

If UUID is included in a PIV-I Certificate, the UUID must not represent the PIV-I card serial number. When included in a Certificate, the UUID must be expressed using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").

Names must never be misleading.

When DNs are used, they must accurately reflect Organizational structures. When DNs are used, the common name must observe name space uniqueness requirements. When User Principal Names (UPNs) are used, they must be unique within the Participant CA namespace and accurately reflect Organizational structures.

Each CA must only Issue Certificates with Subject Names from within a name-space approved by the IdenTrust PMA. Unless approved by IdenTrust PMA, CAs must not certify other CAs.

When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous Certificates as defined in Section *3.1.3 Anonymity or Pseudonymity of Subscribers*. The Subject Name in IdenTrust CA Certificates match the issuer CA name in Subscriber Certificates issued by the IdenTrust CA, as required by RFC 5280.

3.1.3 Anonymity or Pseudonymity of Subscribers

CA Certificates must not contain anonymous or pseudonymous identities.

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

CAs may issue role-based or group certificates that identify subjects by their organizational roles. Each identified role or group must meet name space uniqueness requirements.

3.1.4 Rules for Interpreting Various Name Forms

DNs in Certificates must be interpreted using the X.501 series of specifications and ASN.1 syntax. If present, e-mail names in the Subject Alternative Name field must be interpreted using RFC 5322. 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.501 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 must be interpreted using RFC 4122.

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

3.1.5 Uniqueness of Names

CAs must enforce name uniqueness. When other name forms are used, name uniqueness must also be ensured for certificates issued by that CA. For distinguished names, name uniqueness is enforced for the entire name rather than a particular attribute (common name).

It is recommended that the CA's CPS must define the following:

- What name forms must 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 2 people be provided unique names?).

3.1.6 Recognition, Authentication, and Role of Trademarks

An Issuing CA must not knowingly use trademarks in names unless the subject has the right 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.

The IdenTrust PMA must 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 1 or more employees as LRAs. CAs and RAs may also enroll Trusted Agents to perform I&A in accordance with this Section.

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 must 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 must 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 CA certificates, Subscriber and Group Certificates in the name of Subscribing Organizations must include the Organization name, address, and documentation of the Organizations existence. The RA must 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 Group Certificates: When performing Identification and Authentication of the Applicant of

a Group 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

For each certificate issued, the CA must authenticate the identity of the individual requestor.

Subscriber certificates may be issued on the basis of an electronically authenticated request, using a valid signature or authentication certificate and associated private key, with the following restrictions:

- The assurance level of the new certificate must be the same or lower than the assurance level of the certificate used to authenticate the request,
- Identity information in the new certificate must match the identity information from the signature or authentication certificate,
- The expiration date of the new certificate shall not exceed the next required initial identity authentication date associated with the certificate used to authenticate the request.
- The next required initial identity authentication date remains unchanged in the event of a new certificate issuance based on electronic authentication.

3.2.3.1 Authentication of Human Subscribers

For Applicants, the CA, RA, and/or associated Registration Agents (either CA, RA, LRA or TA) must 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 must depend upon the Assurance Level of the Certificate level and must be addressed in the CA'S CPS or RA's RPS. The documentation and authentication requirements must vary depending upon the level of assurance.

For all Medium Assurances and PIV-I Assurances, identity must be established no more than 90 days before initial Issuance of the Certificate.

A Registration Agent must 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 must 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 during the in-person identity proofing event, 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 must be Revoked.

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

Assurance Level	Requirement
For All Levels Except PIV-I	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 represents.
Basic Assurance Level	Identity is established by in-person proofing before a Registration Authority or Trusted Agent; or verified through automated means where the applicant provides identity data points including name, date of birth, address and other personal information.
Medium Assurance Level	• Identity is established by in-person proofing before a Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities.
For PIV-I Certificates	The following biometric data must be collected during the identity proofing and Registration process, and must be formatted in accordance with [NIST SP 800-76-2]: • 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 must be collected each time a card is Issued; and Two electronic fingerprints to be stored on the card for automated authentication during card usage.

3.2.3.1.1 Basic Identity

Identity verification shall be achieved through in-person confirmation or through an automated process and carried out by a Registrar or Trusted Agent. They will verify the identity information provided by the Applicant, including ID number and account number, by conducting record checks with relevant agencies, institutions, credit bureaus, or similar databases. This process ensures that the name, Date of Birth (DoB), address, and other personal information provided by the Applicant match the records and are adequate for identifying a distinct individual.

3.2.3.1.2 Medium (all)

To establish identity, it is necessary to undergo in-person identity proofing conducted by a Registrar or Trusted Agent. Meeting the in-person identity proofing requirement can be fulfilled through a trust relationship established between the Registration Agent and the Applicant, based on a prior in-person encounter as explained below. The required credentials for this process include 1 Picture I.D. issued by the Federal Government, or one picture ID compliant with the REAL ID Act, or 2 Non-Federal Government I.D.s, 1 of which must be a picture I.D. (such as a Non-REAL ID Act compliant Driver's License). Any credentials presented should be valid and have not expired.

3.2.3.1.3 PIV-I Hardware

PIV-I identity must be verified in accordance with the requirements specified for issuing PIV in Section 2.7 of [FIPS 201] For PIV-I, the use of an in-person antecedent is not applicable.

To establish identity, it is necessary to undergo in-person proofing conducted by a Registration Agent, if in-person proofing is unable to be conducted, supervised remote proofing can be performed only as defined per *NIST SP 800-63A*

- In-person identity proofing - The required credentials for this process consist of 2 original identity source documents. These identity source documents must be selected from the list of acceptable documents provided in Form I-9, OMB No. 1115-0136, which is the Employment Eligibility Verification form. At least 1 of the documents must be a valid State or Federal Government-issued picture identification (ID). The use of an in-person antecedent is not applicable in this case.
- Supervised Remote in-person Proofing – The requirements associated with supervised remote identity proofing are described in *NIST SP 800-63A*, Digital Identity Guidelines, Enrollment and Identity Proofing section 5.3.3. In addition, the supervised remote process for PIV-I policies must have the capability of capturing an approved biometric. Additional required credential documents for this process are identical to those of In-person proofing (above). For supervised remote in-person proofing, a TA or LRA must conduct and witness every step of the process along with validating all required documents being presented.

Registration forms and agreements must be fulfilled by Applicants as described in the CPS Section 3.2.3.1.3.2

3.2.3.1.4 Appeal or Redress of Denied Application

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

3.2.3.1.5 Electronic Verification of Email and Mobile Phone

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

3.2.3.1.6 Who May Perform In-Person Identification

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

The CPS must define the roles and responsibilities of individuals who act as Registrars under this CP.

3.2.3.1.7 Antecedent In-Person Identity Proofing Process

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

1. Meet the thoroughness (rigor) of the in-person event,
2. Provide supporting ID proofing artifacts or substantiate the Applicant through a relationship; and
3. 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. Applicants 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. Subscribers 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 1 other trusted party.

An antecedent process requires various actors, roles, responsibilities, and activities

See Appendix C.

3.2.3.1.8 ID Proofing Relationships

- The Individual performing the identity proofing, IVP or Sponsor of the Applicant must have a contractual relationship with the CA or RA represented by the Registration Agent.
- Sponsor or IVP must have an established relationship with Subscriber. The relationship must be sufficient 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 must contain a description of the relationship with Applicant describing the initial identity proofing or qualifications and the on-going relationship.

3.2.3.1.9 Records Retention

All Participants must store and exchange private information in a confidential and tamper proof manner, also protecting from unauthorized access.

3.2.3.1.9.1 Verification of Applicant Data from an Antecedent In-Person Identity Proofing

- The RA must record the date of the antecedent in-person identity proofing event.
- The RA must obtain any historical artifacts from the Antecedent Event.

3.2.3.1.10 Binding the Certificate Request to the Identity

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

- A Sponsor for the Applicant must provide the RA with initial contact information, (e.g., name, email address, phone number, Subscribing Organization).
- The PKI must use the Sponsor provided information to contact the Applicant.
- Applicants, using a prescribed method, must initiate the credential process by identifying themselves through a series of initial questions. At least 1 question must be derived from private information occurring through the course of the in-person Antecedent Event. This identity binding process must not be repeated in the event of failure.
- If successful, Applicant progresses to a second phase of questions. This on-line verification process must be a set of additional (non-repetitive) questions. The system must score the responses and determine the probability that the claim is or is not fraudulent.

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

Role-based Certificates identify a specific role on behalf of which the 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 must 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. Multiple Group Certificate Types are defined under this CP and have differing authentication requirements, see the following sub-sections:

3.2.3.3.1 Group Domain-Bound 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 Affiliated Certificates. Authentication requirements are:

- Organization authentication as described in Section *3.2.2 Authentication of Organization Identity*.
- Authentication of a human Sponsor for the Certificate in accordance with Section *3.2.3.1 Authentication of Human Subscribers* 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 reliable means of communication; and,
- The Device associated with Group Device Certificates must also be verified according to Section *3.2.3.4Authentication of Devices*.

3.2.3.3.2 Group Certificates

Group Certificates assert Organization and the Group Name in the subjectName DN. Group Certificates are Affiliated Certificates. Authentication requirements are:

- Organization authentication as described in Section *3.2.3.2 Authentication of Human Subscribers for Role-based Certificates*.
- Verification of authorization of the Group Certificate Sponsor and the Subscribing Organization with an authoritative source within the Subscribing Organization (e.g., corporate, legal, IT, HR, or other appropriate organizational sources) using reliable means of communication.

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

- Group Signing Certificates must not assert non-repudiation.
- The Organization responsible for management of the Group Certificate(s) must 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 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,
- The list of those holding the shared Private Key must 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 must 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.

3.2.3.3.3 Verification of NPI Number

When a National Provider Identifier (NPI) Number is included in a Certificate, it MUST be verified against the NPI Registry provided by the Centers for Medicare & Medicaid Services (CMS). The RA MUST utilize the Applicant-provided NPI number to retrieve the Applicant's record from the NPI Registry and confirm that the data elements returned are consistent with the information provided in the application.

3.2.3.3.4 Authentication of Subscribers for Group Certificates

Group Certificates (e.g., authorized third party) assert the Custodian and may contain the Organization. Authentication requirements are:

- Issuer CA or RA must also record the information identified in Section *3.2.3.1 Authentication of Human Subscribers* 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 must be responsible for ensuring control of the Private Key, including maintaining a list of any Group Certificate 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; and
- The Custodian (e.g., authorized third party), ISSO or equivalent must 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.

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 must 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.

These Certificates must 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 must 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 must describe procedures to ensure that Device Certificate accountability is maintained.

3.2.3.4.1

There are 2 Machine Operator roles—a Primary Machine Operator and a Secondary Machine Operator.

3.2.3.4.1.1 Primary Machine Operator

A Primary Machine Operator is named as such under the Subscribing Organization Authorization Agreement entered into in connection with a Device and such Primary Machine Operator represents the Device that is named as Certificate subject in a Certificate issued in connection with such Subscribing Organization Authorization Agreement; provided, however, with respect to revocation and suspension requests, only a Primary Machine Operator may represent a Device to the IdenTrust CA.

3.2.3.4.1.2 Secondary Machine Operator

Secondary Machine Operators are designated by being named as such on the List, which is included in the Subscribing Organization Authorization Agreement, by the Primary Machine Operator, during the Device Certificate Registration process and are archived in the CA database as a part of the Device Certificate account.

3.2.3.4.1.3 Machine Operator Authentication

The Primary Machine Operator is responsible for providing the following registration information and providing supporting documentation when requested by the RA:

- Equipment identification – Subscribing Organization's registered domain name/service name (DNS name), Device serial number; FQDN(s); unique software application name; or public IP addresses,
- Equipment or software application Public Keys,

- Equipment or software application authorizations and attributes (if any are to be included in the Certificate); and/or
- Contact information to enable the RA to communicate with the Primary Machine Operator and Subscribing Organization when required.
- Designation of Secondary Machine Operators

The registration information is verified by the LRA. Acceptable methods for performing this authentication of registration information provided by a Primary Machine Operator and ensuring the information has not been tampered with include, but are not limited to:

- Verification of Digitally Signed messages sent from the Primary Machine Operator; and/or
- Registration by the Primary Machine Operator, with In-person identity proofing of Registration of the Device by the Primary Machine Operator, including verification of the identity of the Primary Machine Operator confirmed in accordance with the requirements of Section *3.2.3 Authentication of Individual Identity* of this CP at a level of assurance equal to or higher than that of the Device Certificate being applied for.

3.2.3.4.2 Authentication of Primary Machine Operators

Part of the Device Registration process, the Primary Machine Operator will be named in the Subscribing Organization Authorization Agreement. Identity Verification and affiliation of the Primary Machine Operator must 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 Authentication of Devices,* 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.

Should a Secondary Machine Operators be initially designated in conjunction with the Device, then the Primary Machine Operator is 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.

3.2.3.4.3 Authentication of Secondary Machine Operators

Secondary Machine Operators are allowable for the purpose of managing a Device that has been issued a Device Certificate, they also act as back up to the Primary Machine Operator to manage Certificate Suspension and/or Revocation of the Device Certificate, when needed. The name(s) of Secondary Machine Operator(s) will not be named in the Device Certificate.

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 CPS.

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

3.2.3.4.4 Verification of Authorization by Subscribing Organization

Device Certificate Issuance and affiliation must be authorized by submission of a Subscribing Organization Authorization Agreement.

3.2.3.4.5 Device Issuance

IdenTrust must not Issue Device Certificates to Individual Subscribers without affiliation to a Subscribing Organization. An Individual defined as a sole proprietor of an Organization is eligible with proper verification.

3.2.4 Non-Verified Subscriber Information

All Subscriber Information included in Certificates must be verified.

3.2.5 Validation of Authority

IdenTrust must validate any CA Certificate Requestor's authorization to act in the name of the CA. Additionally, IdenTrust must validate that the CA has been approved by the PMA based on successful compliance analysis of the CA's CPS.

Certificates that assert affiliation must 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.

3.2.6 Criteria for Interoperation

A CA must adhere to the following requirements:

- Operate a PKI that has undergone a successful compliance audit pursuant to Section *8 Compliance Audit and Other Assessments* 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

If 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 must identify itself through use of its current Signature Key or the initial Registration process. If it has been more than 3 years since the Participant CA was identified as required in Section *3.2 Initial Identity Validation*, identity must be re-established through the initial Registration process.

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

3.3.1.1 Subscribers - Basic and Medium (All policies)

Identity may be established using current (unexpired) Signature Keys, however, for Basic Assurance Level Certificates, identity must be re-established through the initial Registration process at least once every **15** years from the time of initial Registration and for a Medium Assurance Level Certificates, identity must be re-established through the initial Registration process at least once every **12** years.

3.3.1.2 Subscribers - PIV-I

Identity may be established using current (unexpired) Signature Key, however, identity must be established through initial Registration process at least once every 12 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

3.3.1.3 LRAs

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

3.3.1.4 SubCAs, RAs and the Cross-Certifying Bridge CA

The I&A process for Re-Keying SubCAs, RAs and Cross-Certifying Bridge CAs is the same as stated above, except that if it has been more than 3 years since identity was established, it must be re-established. Certificate validity is as defined in the table in Section *6.3.2 Certificate Operational Periods and Key Usage Periods*.

3.3.2 Identification and Authentication for Re-Key After Revocation

For Re-Key after Revocation, all Participants must undergo the initial I&A processes specified in Sections *3 Identification and Authentication* and Section 3 sub-sections, also Section *4 Certificate Life-Cycle Operational Requirements* and Section 4 sub-sections of this CP.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

Revocation requests must 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.

3.5 IDENTIFICATION AND AUTHENTICATION FOR KEY RECOVERY REQUESTS

While IdenTrust supports the escrow of encryption keys for enterprise entities who may need it, the recovery of escrowed keys is the responsibility of the enterprise entity via CMS.

3.5.1 KRA Authentication

The KRA must authenticate to the KED or DDS directly or by using a public key certificate issued by the governing organization. When a public key certificate is used, it must be on a FIPS 140 level 2 or higher validated hardware cryptographic module. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered.

3.5.2 KRO Authentication

The KRO must authenticate to the KRA using a public key certificate issued by the governing organization. The assurance level of the certificate must be the same as or greater than that of the certificate whose corresponding private key is being recovered.

3.5.3 Subscriber Authentication

The Subscriber identity must be established as specified in Section 3.3.1 above. Alternatively, if the authentication cannot be verified using the public key certificates issued by the associated PKI and for at least the given certificate policy assurance level, then the identity validation can use the steps outlined in Section 3.2.3.1. For automated self-recovery, the Subscriber must be authenticated to the KED using a valid public key certificate. The assurance level of the Subscriber certificate must be equal to or greater than that of the certificate whose corresponding private key is being recovered.

3.5.4 Third-Party Requestor Authentication

The KRA or KRO must verify the identity and authorization of the Requestor prior to initiating the key recovery request.

Third-Party Requestor identity authentication must be commensurate with the assurance level of the certificate associated with the key being recovered. Identity must be established using one of the following methods:

- Procedures specified in Section 3.2.3 for authentication of an individual identity during initial registration for the specified certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).
- Certificate-based authentication (e.g., digitally signed e-mail or client-authenticated TLS) that can be verified using current, valid (i.e., un-revoked) public key certificates at the requested certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).

3.5.5 Data Decryption Server Authentication

The DDS must authenticate to the KED directly using a public key certificate issued by the associated PKI. The assurance level of the certificate must be the same as or greater than that of the highest assurance level encryption certificates issued by the associated PKI.

The implementation of a DDS is optional see section *1.3.6.2 Data Decryption Server*.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

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

All communications among CAs, RAs, LRAs, Trusted Agents, and Applicants supporting the Certificate application and Issuance process must 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 must be protected using hardware assurance Certificates, or some other mechanism of equal or greater strength). Any electronic transmission of shared secrets must 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 Who Can Submit a Certificate Application

A Certificate application may be submitted to a CA or RA by the Applicant, compliant Custodian (e.g., authorized third party), ISSO or the Subscribing Organization of the Applicant.

4.1.2 Enrollment Process and Responsibilities

All communications among PKI authorities supporting the Certificate application and Issuance process must 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 must require:

- An auditable chain of custody must be in place when information is obtained through one or more information sourced to the CA
- All data received be protected and securely exchanged in a confidential and tamper evident manner and protected from unauthorized access.

4.1.2.1 Establishment of Identity

Requests made by CAs for SubCA Certificates must be submitted to the PMA using the contact provided in Section *1.5.2 Contact Person*. The PMA will evaluate the request for acceptability. At a minimum the CA's CPS must have successfully completed a compliance analysis conducted by either the PMA or an independent party. The PMA must only accept requests from an approved CA.

The Applicant and the CA must 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 Initial Identity Validation*,
- 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.

4.2 CERTIFICATE APPLICATION PROCESSING

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

4.2.1 Performing Identification and Authentication Functions

Upon receiving the Certificate application, the CA or RA must verify the identity of the Applicant in accordance with Sections *3.2 Initial Identity Validation* and *3.3 Identification and Authentication for Re-Key Requests* and their sub-sections of this CP.:

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 must be required to agree to the requirements that they must 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 must be responsible for the Approval or Rejection of certificate applications:

4.2.3 Time to Process Certificate Applications

Certificate applications must be processed, and certificate issued within 90 days of identity verification.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

Upon receiving a certificate request, and before certificate issuance, the CA/RA must verify and/or authenticate the following:

- Verify the identity of the requestor.
- Verify the authority of the requestor and the integrity of the information in the certificate request.
- Verify all attribute information received from a subscriber before inclusion in a certificate.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).
- Make the certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged the obligations described in section *9.6.3 Confidentiality of Business Information*.

See the IGC CPS for more details.

4.3.2 Notification to Subscriber by IdenTrust of Issuance of Certificate

A CA must notify a Subscriber of Certificate Issuance.

4.4 CERTIFICATE ACCEPTANCE

Before effective use of private keys, Subscribers must accept the Subscriber Agreement, and the responsibilities as defined in section *9.6.3 Subscriber Representations and Warranties*.

4.4.1 Conduct Constituting Certificate Acceptance

Failure to object to the Certificate or its contents must constitute Acceptance of the Certificate.

4.4.2 Publication of the Certificate by the CA

As specified in Section *2.2 Publication of Certificate Information*, all CA Certificates must be published in a publicly accessible Repository.

PIV-I Authentication and Card Authentication Certificates must not be distributed via public repositories.

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) must be notified upon Issuance of all CA Certificates. The process or requirement for notifying any other entities (e.g., PMAs of Cross-Certified entities) must be specified in relevant agreements between the IdenTrust PMA or CA and other entities.

For any CA Certificate issued under this policy, IdenTrust will also notify the CA under which the issuing CA Root Certificate is cross-certified, at least 2 weeks prior to the issuance of the new CA Certificate or issuance of new inter-organizational CA cross-certificate. The notification must assert that the new CA cross-certification does not introduce multiple paths to a CA already participating in the associated PKI. In addition, all new artifacts (CA Certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the CA Certificate issuance must be provided to the cross-certified entity, within 24 hours following issuance of the CA Certificate.

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, must protect it from access by unauthorized parties and must use the Private Keys only as specified by the Certificate Policies and keyUsage extensions of the corresponding Certificate. The Subscriber must not use the signature Private Key after the associated Certificate has been Revoked or has expired.

Use of the Private Key must 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 must also be observed. For example, the OCSP Responder Private Key must be used only for signing OCSP Responses.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties should become familiar with their responsibilities as detailed in Section *9.6.4 Relying Party Representations and Warranties* and assume the responsibility to understand 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 must 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 must not be further Re-Keyed, renewed, or modified.

4.6.1 Circumstance for Certificate Renewal

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. In addition, the Validity Period of the Certificate must meet the requirements specified in Section *6.3.2 Certificate Operational Periods and Key Usage Periods*.

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 such as PIV-I must 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

For Certificates where Renewal is allowable, Certificate renewal identity-proofing must be achieved using 1 of the following processes:

- Initial Registration process as described in Section *3.2 Initial Identity Validation*: or
- I&A for Re-Key as described in Section *3.3 Identification and Authentication for Re-Key Requests*, except the old Key can also be used as the new Key.

When certificates are renewed because of CA Key compromise, the CA or RA must verify all certificates issued since the date of the compromise were issued appropriately. If the certificate cannot be verified, then it must not be renewed.

4.6.4 Notification of New Certificate Issuance to Subscriber

A CA must notify Subscribers of Certificate Issuance.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Failure to object to the Certificate or its contents constitutes Acceptance of the Certificate.

4.6.6 Publication of the Renewal Certificate by the CA

As specified in Section *2.2 Publication of Certificate Information*, and *4.4.2 Publication of the Certificate by the CA,* all CA Certificates must be published in a publicly accessible Repository.

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) must be notified upon

Issuance of all CA Certificates. The process or requirement for notifying any other entities (e.g., PMAs of Cross-Certified entities) must be specified in relevant agreements between the IdenTrust PMA or CA and other entities.

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 must identify themselves for the purpose of Re-Keying as required in Section *3.3.1 Identification and Authentication for Routine Re-Key*.

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

4.7.1 Circumstances 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. Subscribers and other PKI Participants should plan on Re-Keying well in advance of the time when a Key Pair or Certificate is scheduled to expire.

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.

Subscribers may request re-key of his or her Valid Certificate.

4.7.3 Processing Certificate Re-Keying Requests

Re-Key requests are processed in the same manner as initial issuance. See Sections *3.2 Authentication of Organization Identity* and *3.3 Identification and Authentication for Re-Key Requests*.

4.7.4 Notification of New Certificate Issuance to Subscriber

A CA must notify Subscribers of Certificate Re-Key Issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Failure to object to the Certificate or its contents must constitute Acceptance of the Certificate.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As specified in Section 2.2 and 4.4.2, all CA Certificates must be published in a publicly accessible Repository.

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) must be notified upon Issuance of all CA Certificates.

In the event a Cross-Certified CA is re-keyed, new Cross-Certificates must 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 must identify itself through use of its current Signature Key or the initial registration process. If it has been more than 3 years since identification of the Cross-Certifying CA as required in Section *3.2 Initial Identity Validation,* identity must be re-established through the initial registration process.

4.8 CERTIFICATE MODIFICATION

A Certificate modification is creating new Certificates with the same or a different key and that has a different serial number, and that it differs in one or more other fields from the old certificate (e.g., a name or email address). For example, a CA may perform Certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree).

After Certificate modification, the old Certificate may or may not be Revoked, but must 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 with a valid certificate may request a Certificate modification. Additionally, CAs, RAs and LRAs may request Issuance of modified Certificates.

4.8.3 Processing Certificate Modification Requests

A modified certificate may use the same or a different subject public key as the original certificate, depending on issuance constraints. However, if the same key is used, certificate operational periods and key lifetimes as defined in Section *6.3.2 Certificate Operational Periods and Key Usage Periods* continue to apply.

For CAs, proof of all subject information changes must be provided to the RA or other designated agent and verified before modified certificate is issued. If the modified certificate is issued with a new (different) public key, the additional requirements specified in Section *4.7.3 Processing Certificate Re-Keying Requests* must also apply.

If an individual's authorizations or privileges change, such that the modified certificate indicates a reduction in privileges and authorizations, the old certificate must be revoked.

4.8.3.1 Processing Modification Requests for Subscriber Certificates

Certificate modification identity-proofing must require proof of all subject information changes to be provided to the RA, LRA, or Trusted Agent and verified before the modified Certificate is Issued. Processing Modification Requests for Subordinate CA Certificates

Requests for modification of a SubCA Certificate must be submitted in written form to the IdenTrust PMA for consideration. Upon approval, the modification request must be processed according to the procedures defined in the CPS Section *4.8 Certificate Modification* and 4.8 sub-sections.

4.8.3.2 Processing Modification Requests for CA Cross-Certificates

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

CA Modification requests are processed according to the CPS Section 4.8.3.3.

4.8.4 Notification of New Certificate Issuance to Subscriber

A CA must notify Subscribers of Certificate Issuance.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Failure to object to the Certificate or its contents must constitute Acceptance of the Certificate.

4.8.6 Publication of the Modified Certificate by the CA

All CA Certificates must be published in a publicly accessible Repository.

PIV-I Certificates must not contain the card serial number in any extension that is 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) must be notified upon Issuance of all CA Certificates. The process or requirement for notifying any other entities (e.g., PMAs of Cross-Certified entities) must be specified in relevant agreements between the IdenTrust PMA or CA and other entities.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

Revocation and Suspension requests must 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.

4.9.1 Circumstances for Revocation

A Certificate must 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 hold 1 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 must require that the Organization must inform the CA of any changes in the Subscriber affiliation. If the Subscribing Organization no longer authorizes the affiliation of a Subscriber, the CA must 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 must Revoke all Certificates affiliated with that Organization.

Whenever any of the above circumstances occur, the associated Certificate must be Revoked and Certificate Revocation status placed on a CRL. Revoked Certificates must be included in all new publications of the Certificate status information until the Certificates expire. Revoked Certificates must appear on at least 1 CRL.

4.9.2 Who Can Request Revocation

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

- 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 named 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

IdenTrust allows Certificate revocation and will Revoke Certificates upon receipt of sufficient evidence of compromise or loss of the Subscriber's corresponding private key.

A request to Revoke a Certificate must 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 must authenticate the request and then Revoke the Certificate.

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

For PIV-I Assurance Levels, CAs must directly or through a delegate collect and destroy PIV-I cards from Subscribers whenever the cards are no longer valid, whenever possible. CAs must 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 must 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 must 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 1 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 2 hours of CRL issuance, Revocation requests must be processed before the next CRL is published. Revocation requests validated within 2 hours of CRL issuance must 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 must 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

CRL issuance encompasses both CRL generation and publication. See the table below for guidelines for issuing frequency of routine CRLs. CRLs may be issued more frequently than specified below.

	Maximum Interval for Routine CRL Issuance	
Assurance Level	**Online**	**Offline**
Basic	24 hours	35 Days
Medium (all policies)	24 hours	35 Days
PIV-I Card Authentication	24 hours	35 Days

CAs may be operated in an offline manner if the CA only issues:

- CA Certificates,
- CSS Certificates (optionally); and
- End user Certificates solely for the administration of the principal CA (optionally).

However, the interval between routine CRL issuance will not exceed 35 days. Such CAs must meet the requirements specified in section *4.9.12 Special Requirements Related to Key Compromise*, for issuing Emergency CRLs.

NOTE: Such CAs will also be required to notify the FPKIMA upon Emergency CRL issuance. This requirement will be included in the MOA between the FPKIPA and the Entity.

The frequency of CRL Issuance is dependent on the type of CRL as defined in the following sub-sections.

4.9.7.1 CRL Issuance Frequency for CAs

SubCA and Participant CAs must generate and publish a CRL no less than once every 24 hours.

4.9.7.2 CRL Issuance Frequency for Root CAs

IdenTrust must publish the CRL for Certificates Issued by the IGC Root CA at least every 35 days.

4.9.7.3 CRL Issuance Frequency for All CAs

All CAs must publish to Repository a new CRL prior to the time specified in the Next Update field of the active CRL. Upon the publishing of a new CRL, the Root CA and Participant CA must remove any and all old CRLs published in the Repository.

4.9.8 Maximum Latency of CRLs

CRLs must be published within four hours of generation. Furthermore, each CRL must be published no later than the time specified in the Next Update field of the previously published CRL for same scope.

4.9.9 Online Revocation / Status Checking Availability

CAs may support on-line Revocation/status checking. For PIV-I Assurance Levels, CAs must support on-line status checking via OCSP using the CA-delegated trust model specified in RFC 6960.

OCSP services must be designed and implemented as to provide 99% availability overall and limit scheduled

downtime to 0.5% annually, with resources sufficient to provide a response time of 10 seconds or less under normal operating conditions.

If on-line Revocation/status checking is supported by a CA, the latency of Certificate status information distributed on-line by the CA or its delegated status responders must meet or exceed the requirements for CRL issuance stated in *4.9.7 CRL Issuance Frequency*.

4.9.10 Online Revocation Checking Requirements

Unless specified in Section *4.9.9 Online Revocation / Status Checking Availability*, 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 must meet the following requirements:

- The alternative method must be described in the CA's approved CPS, and
- The alternative method must provide authentication and integrity services commensurate with the Assurance Level of the Certificate being verified.
- The alternative method must 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 an IdenTrust principal CA private key Compromise or loss, the cross- certificate must be revoked and IdenTrust must publish a CRL must be published as specified in the table below. In the event of a Subscriber Private Key Compromise or loss, a CRL must be published as specified in the table below.

Assurance Level	Maximum Latency for Emergency CRL Issuance
Basic	24 hours after notification
Medium (all policies)	18 hours after notification
PIV-I Card Authentication	18 hours after notification

In the event of a Subscriber Private Key Compromise or loss, a CRL must be published at the earliest feasible time. At a minimum, a CRL must be published according to the requirements in Section *4.9.7 CRL Issuance Frequency*.

4.9.13 Circumstances for Suspension

Suspension must be permitted for all Certificate types Issued by CAs under this CP. 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

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

- 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 must 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 must authenticate the request and then suspend the Certificate.

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

The Maximum limit on a Suspension period must be no longer than 14 days.

In order to mitigate the threat of unauthorized person removing the Certificate from hold, the Subscriber identity must be authenticated:

- In person using initial identity proofing process described in Section *3.2.3 Authentication of Individual Identity*,
- 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
- Using a Client-authenticated SSL/TLS-Encrypted Session using with a Certificate of an equal or higher Assurance Level than the suspended Certificate, 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 must ensure the request is authenticated and verify the Certificate Subject is the same as in the suspended Certificate.

4.10 CERTIFICATE STATUS SERVICES

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

4.10.1 Operational Characteristics

See Sections *4.9.6 Revocation Checking Requirements for Relying Parties*, *4.9.9 Online Revocation/Status Checking Availability*, and *7.3 OCSP Profile*.

4.10.2 Service Availability

Certificate Status Services must 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 Features

Operational features of CRL and OCSP services are described in Section *7 Certificate Profile*.

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 must always be Revoked at the end of subscription.

4.12 Key Escrow and Recovery

Encryption key escrow and key recovery by an RA can be facilitated via the use of CMS on the premise of a third-party RA.

4.12.1 Key Escrow for CMS

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 must be encrypted and protected in a manner that requires involvement of both the CA and RA for Key recovery.

4.12.1.1 Circumstances for Key Recovery

Subscribers and Subscribing Organizations may request recovery of an escrowed Private Key via the CMS. 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.

4.12.2 Key Escrow and Recovery Policy and Practices

Encryption Key escrow and key recovery by an RA via the use of a CMS on the premise of a third-party RA are supported only.

4.12.2.1 Key Escrow Process and Responsibilities

Subscriber private keys (i.e., decryption private keys) associated with a key management certificate must be securely escrowed by the KED. The CA must ensure that the keys are escrowed successfully prior to issuance of the key management certificates. Subscriber private keys must be protected during transit and storage using cryptography at least as strong as the key being escrowed. Subscribers must be notified that the private keys associated with their encryption certificates will be escrowed.

4.12.2.2 Key Recovery Process and Responsibilities

Communications between the various key recovery participants (KED, DDS, KRA, KRO, Requestor, and Subscriber) must be secured from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols must be equal to or greater than that of the keys they protect.

During delivery, escrowed keys must be protected against disclosure to any party except the Requestor.

When any mechanism that includes a shared secret (e.g., a password) is used to protect the key in transit, the mechanism must ensure that the Requestor and the transmitting party are the only holders of this shared secret.

Subscribers may use electronic or manual means to request their own escrowed keys from the KRS. The Subscriber may submit the request to the KED, KRA or KRO. If the request is made electronically, the subscriber must digitally sign the request or authenticate to a recovery service using an associated authentication or signature certificate with an assurance level equal to or greater than that of the escrowed key. Manual requests must be made in person and include proper identity verification by the KRA in accordance with Section 3.2.3.1.

Third-Party Requestors may use electronic or manual means to request the Subscribers' escrowed keys. The Requestor must submit the request to the KRA or KRO. If the request is made electronically, the Requestor must digitally sign the request using a trusted authentication or signature certificate, as determined by the recovering organization, with an assurance level equal to or greater than that of the escrowed key. Manual requests must include proper identity verification by the KRA in accordance with Section 3.2.3.1.

Third party key recovery in and of itself does not require revocation of a subscriber certificate. This does not prohibit Subscribers from requesting revocation of their own certificates for any reason.

4.12.2.2.1 Key Recovery Through KRA

The KRA must provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access requires the actions of at least two KRAs. All copies of escrowed keys must be protected using two-person control procedures during recovery and delivery to the authenticated and authorized Requestor. Split key or password procedures are considered adequate two-person controls, provided they comply with technical controls in Section 6.2.2.

The KRA is not required to notify subscribers of a third-party key recovery

4.12.2.2.2 Automated Self-Recovery

A current Subscriber's escrowed keys may be provided directly to the Subscriber without imposition of two-person control requirements. The KED must only provide escrowed keys to current Subscribers without two-person control upon:

- Verifying that the authenticated identity of the Requestor is the same as the Subscriber associated with the escrowed keys being requested,
- Sending notification to the Subscriber of all attempts (successful or unsuccessful) to recover the Subscriber's escrowed keys that are made by entities claiming to be the subscriber. If the KED does not have information (e.g., an e-mail address) necessary to send notification to the Subscriber of a key recovery request, then the KED must not provide the Subscriber with the requested key material using the automated recovery process
- Ensuring that the escrowed keys are being sent only to the authenticated Subscriber associated with the escrowed keys; and
- Ensuring that the escrowed keys are encrypted during transmission using cryptography of equal or greater strength than provided by the escrowed keys.

4.12.2.2.3 Key Recovery During Token Issuance

When a Subscriber (individual and/or group/role sponsor or member) is issued a new certificate on a hardware token, private key management keys for the Subscriber may be recovered as part of the issuance process as long as the KED uses secure means, such as Global Platform Secure Channel Protocol, to inject the key history onto the hardware token directly.

The hardware token must meet FIPS 140 Level 2 hardware requirements, and the key must be injected into the token such that it is not thereafter exportable.

4.12.2.2.4 Key Recovery by Data Decryption Server

A DDS must be under two-person control, as is required for any CA or KED. A DDS is permitted to automatically recover keys from the KED. The KED must perform the following activities prior to releasing the key:

- Authenticating the Requestor as a legitimate DDS,
- Verifying that the DDS is authorized to recover the escrowed key for the Issuing Organization to which the key belongs,
- Ensuring that the escrowed keys are protected during transmission using cryptography or other means of equal or greater strength than provided by the escrowed keys.

In order to prevent any individual KRA, KRO or another trusted role from accessing subscriber encryption keys, a combination of physical, procedural, and technical security controls must be used to enforce continuous two-person control on the DDSs. The DDSs must be designed to maximize the ability to enforce two-person control technically.

4.12.2.3 Who Can Submit a Key Recovery Application

Subscribers may request recovery of their own escrowed keys. Key recovery may also be requested by internal Third-Party Requestor permitted by the Issuing Organization policy, and by authorized external Third-Party Requestors (e.g., law enforcement personnel with a court order from a competent court).

4.12.2.3.1 Requestor Authorization Validation

The KRA or the KRO, as an intermediary for the KRA, must validate the authorization of the Requestor. KRAs should consult with Issuing Organization management and/or legal counsel, as appropriate.

Issuing Organizations must determine internal notification requirements for External Third-Party key recovery requests and account for situations where the law requires the KED to release the Subscriber's private key without organizational notification.

Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests.

4.12.2.3.2 Subscriber Authorization Validation

Current Subscribers are authorized to recover their own escrowed key material.

4.12.2.3.3 KRA Authorization Validation

The KED must verify that the KRA has appropriate privileges to obtain the keys for the identified Subscriber's organization.

4.12.2.3.4 KRO Authorization Validation

The KED or KRA must verify that the KRO is authorized to request keys for the identified Subscriber.

4.12.2.3.5 Data Decryption Server Authorization Validation

The KED must verify that the DDS recovery request falls within the organizational scope for which the DDS was established. Implementation of a DDS is optional see Section *1.3.6.2 Data Decryption Server*.

4.12.3 Key Encapsulation and Recovery Policy and Practices

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

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

All equipment, including CA equipment and CA cryptographic modules, must be protected from unauthorized access at all times. IdenTrust requires that equipment for CMS, RA Systems and LRA workstations located outside of IdenTrust's physical control be protected from unauthorized access. Operators of such equipment are obligated by contract, this CP and the CPS to implement physical Access Controls that must be implemented to reduce the risk of equipment tampering even when the KSM/cryptomodule is not installed and activated. These security mechanisms must 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 must be implemented which protect the CA, CSA, CMS, and RA hardware and software from unauthorized use. CA, CSA, CMS, and RA KSMs must 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 must be in accordance with that afforded the highest value sensitive business and financial information.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

The CA, CSA, CMS, and RA equipment including remote workstations, must always be protected from unauthorized access. The equipment must be protected from unauthorized access while the KSM is installed and activated. Physical Access Controls must be implemented to reduce the risk of equipment tampering even when the KSM is not installed and activated. These security mechanisms must be commensurate with the level of threat in the equipment environment. The physical security mechanisms for CAs, CSAs, CMSs, and RAs must 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 Control physical access to both the KSM and the computer system; and
- At a minimum, provide 3 layers of increasing security such as perimeter, building, and CA room.

Removable KSMs must 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 must be placed in secure containers. Activation Data must either be memorized or recorded and stored in a manner commensurate with the security afforded the KSM and must not be stored with the KSM.

In addition, LRA equipment must be protected from unauthorized access while LRA's KSM is installed and activated. The LRA must implement physical Access Controls to reduce the risk of equipment tampering even when the KSM is not installed and activated. These security mechanisms must 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 must occur if the facility is to be left unattended. At a minimum, the check must 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 people must be made explicitly responsible for making such checks. When a group of people is responsible, a log identifying the person performing a check at each instance must be maintained. If the facility is not continuously attended, the last person to depart must 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 must be supplied with power and air conditioning sufficient to create a reliable operating environment.

Remote access to CA equipment, that is, access from outside of the IdenTrust network, must be prohibited.

5.1.2.2 Physical Access for RA Equipment

Sec Section 5.1.2.1

5.1.2.3 Physical Access for CSS Equipment

Sec Section 5.1.2.1

5.1.2.4 Physical Access for CMS Equipment

Sec Section 5.1.2.1

5.1.2.5 Physical Access for Key Escrow Database Equipment

IdenTrust does not escrow or recover keys.

5.1.2.6 Physical Access for Data Decryption Server Equipment

IdenTrust does not escrow or recover keys.

5.1.2.7 Physical Access for Key Recovery Equipment

IdenTrust does not escrow or recover keys.

5.1.3 Power and Air Conditioning

The CA, CSA, CMS, Repository, and RA equipment must 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 must be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to support continuity of operations.

5.1.4 Water Exposures

CA, CSA, CMS and RA equipment must be installed such that it is not in danger of exposure to water. Water exposure from fire prevention and protection measures are excluded from this requirement.

5.1.5 Fire Prevention and Protection

Commercial best practices for fire prevention and protection must be used for the CA, CSA, CMS, and RA equipment.

5.1.6 Media Storage

Media must be stored to protect it from accidental damage (water, fire, electromagnetic) and unauthorized

physical access.

5.1.7 Waste Disposal

Sensitive media and documentation used to collect or transmit information described in Section *9.4 Privacy of Personal Information* must be destroyed, such that the information is unrecoverable, prior to disposal.

IdenTrust employees are prohibited from destroying or disposing of potentially important records or information without specific advance management approval.

All other types of sensitive information must be disposed of in a secure fashion.

5.1.8 Off-site Backup

System backups, sufficient to recover from system failure, must be made on a periodic schedule for CA, CMS, and RA systems. Backups must be performed and stored off-site not less than once every 7 days, unless the system is off-line, in which case it must be backed up whenever it is activated or every 7 days, whichever is later. At least 1 full backup copy must be stored at an offsite location (separate from the equipment). Only the latest backup need be retained. The backup must 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 personnel selected to fill these roles must 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 1 person, so that any malicious activity would require collusion.

An auditable record must be created identifying when personnel are added or removed from a trusted role, as well as who added or removed them from the role. The individual who authorized the role assignment, or any series of role assignments over a given period of time, must also be traceable via audit and archive records.

The following roles must be fulfilled by Individuals that have met the requisite requirements for a Trusted Role:

- CA Administrator,
- CA Agent,
- CA Auditor,
- CA Operator,
- CSA Administrator,
- CSA Agent,
- CSA Auditor,
- CSA Operator,
- Software Engineer,
- Development Operations (DevOps),
- CMS Administrator,
- CMS Auditor,
- CMS Operator,
- Key Recovery Agent
- Registration Authority Administrator,

- Local Registration Authority,
- Quality Assurance Personnel

The following sections define these and other Trusted Roles.

5.2.1.1 Certification Authority (CA) Trusted Roles

5.2.1.1.1 CA Administrator

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 SubCA Key management including generation and/or destruction.

CA Administrators do not Issue Certificates to Subscribers.

5.2.1.1.2 CA Agent

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.

5.2.1.1.3 CA Auditor

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.

5.2.1.1.4 CA Operator

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.

5.2.1.1.5 Software Engineer

The Software Engineer role responsibilities are as follows:

- Build/program, software code
- Install, test and debug software code

5.2.1.1.6 DevOps

The DevOps role responsibilities are as follows:

- Provide system infrastructure
- Automate process to support efficient software development
- Deploy tested and approved software applications

5.2.1.2 Registration Authority Trusted Roles

An RA may be considered a Trusted Agent as defined in Section 5.2.1.8 Trusted Agent .

The RA role is highly dependent on implementation and local requirements. The responsibilities and controls for RAs shall be explicitly described in the CPS.

5.2.1.3 Key Recovery Trusted Roles

5.2.1.3.1 Key Recovery Agent (KRA)

A Key Recovery Agent may be considered a Trusted Agent as defined in Section 5.2.1.8 Trusted Agent.

5.2.1.4 Certification Status Authority (CSA) Trusted Roles

5.2.1.4.1 CSA Administrator

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.

5.2.1.4.2 CSA Agent

Within IdenTrust the CA Agent and the CSA Agent are equivalent and interchangeable. See Section *5.2.1.1.2 CA Agent*.

5.2.1.4.3 CSA Auditor

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.

5.2.1.4.4 CSA Operator

Within IdenTrust the CA Operator and the CSA Operator are equivalent and interchangeable. See Section *5.2.1.1.4 CA Operator*.

5.2.1.5 Card Management System (CMS) Roles

5.2.1.5.1 CMS Administrator

The CMS Administrator role responsibilities are as follows:

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

5.2.1.5.2 CMS Auditor

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.

5.2.1.5.3 CMS Operator

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.

5.2.1.6 Registration Authority (RA) Administrator

The RA Administrator responsibilities are:

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

5.2.1.7 Local Registration Authority (LRA)

The LRA responsibilities are:

- 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.

5.2.1.8 Quality Assurance Personnel

As Quality Assurance Personnel roles perform functions that, if not carried out properly, can introduce security problems, whether accidentally or maliciously, controls are in place requiring approval from the Operations Management Personnel role prior to the introduction of code to Staging and Production environments.

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

Quality Assurance Personnel have the following tasks:

- Develop and execute test plans,
- Identify and document defects,
- Conduct Functional, regression, performance and user acceptance testing,
- Collaborate with cross-functional teams including developers, product managers and other stakeholders,
- Maintain testing environments
- Report and track quality metrics
- Lead Change Management from code freeze through Production deployment.

5.2.1.9 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.

5.2.1.10 Other Roles

Other internally defined roles may be implemented to support the CA and/or RA operation.

5.2.2 Number of Persons Required per Task

For Basic Levels of Assurance, only one person is required per task.

For Medium (all policies) or High Levels of Assurance, proper procedural and operational mechanisms must 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 people 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 must 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 1 of the Participants must be an Administrator. All Participants must serve in a Trusted Role as defined in Section *5.2.1 Trusted Roles*. Principles of Separation-of-Duties/Multi-party Control must 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 must 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 must be allowed CMS access only when authenticated using a Certificate that 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 must be specifically designated to the roles defined in Section *5.2.1 Trusted Roles* above. Individuals may assume more than 1 role subject to the following limitations:

- Individuals assigned to 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 must 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 must be identified. The Trusted Roles of these Individuals per Section 5.2.1 must be identified. All individuals filling Trusted Roles must be selected based on loyalty, trustworthiness, and integrity. Trusted Roles are responsible and accountable

for the operation of the CA, CMS, CSA, and RA must be subject to background investigation. Personnel appointed to Trusted Roles (including CA Trusted Roles, CSA Trusted Roles, CMS Trusted Roles, RA Administrator, and LRA) must:

- 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 non-performance 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 must satisfy at least 1 of the following requirements:

- The person must be a citizen of the country where the CA is located,
- For PKIs operated on behalf of multinational governmental Organizations, the person must be a citizen of 1 of the member countries,
- For PKIs located within the European Union, the person must be a citizen of 1 of the member states of the European Union,
- The person must 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) must, 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 must cover at least the last 5 years for each area, except for the residence check which must cover at least the last 3 years. Regardless of the date of the award, the highest educational degree must be verified. Adjudication of the background investigation must be performed by a competent adjudication authority using a process consistent with U.S. Executive Order 12968, 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 must be in accordance with the corresponding formal clearance.

If the person has been in the workforce for less than 5 years, the employment verification must consist of the periods during which the person has been in the workforce. At a minimum, the background check will be refreshed

every 10 years.

The results of these checks must not be released except as required in Sections *9.3 Confidentiality of Business Information* and *9.4 Privacy of Personal Information*.

5.3.3 Training Requirements

Each person performing duties with respect to the operation of the CA, CSA, RA, and LRA must receive comprehensive training regarding such duties. Training must be conducted in the following areas:

- CA/CSA/CMS/RA security principles and mechanisms,
- Use and operation of all PKI associated equipment,
- All PKI hardware and software versions in use on the CA system,
- Stipulations of the applicable Certificate policy documents
- Key recovery system security principles and mechanisms
- All PKI duties an Individual is expected to perform; and
- Disaster recovery and business continuity procedures.

Documentation must 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 must be aware of changes in the CA, CSA, CMS, RA, or LRA operations, as applicable. Any significant change to the operations must have a training (awareness) plan, and the execution of such plan must 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 must be maintained, identifying all personnel who received training, and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

Job rotation is optional, however, if exercised, must be implemented by and with the judgment of management, this 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.

Job rotation must not violate role separation. All access rights associated with a previous role must be terminated.

All job rotations are documented. Individuals assuming an auditor role must not audit their own work from a previous role.

5.3.6 Sanctions for Unauthorized Actions

IdenTrust and the PMA of the Participating CA, must take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions not permitted by this CP, the CPS and any applicable RPS.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the CA or RA must 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 must 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 fulfill their role responsibilities.

5.4 AUDIT LOGGING PROCEDURES

Audit log files must be generated for all events relating to the security of the CA, CSA, CMS, and RA. Where possible, the security audit logs must be automatically collected. Where this is not possible, a logbook, a paper form, or other physical mechanism must be used. All security audit logs, both electronic and non-electronic, must be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section must be maintained in accordance with Section *5.5.2 Retention Period for Archive*. For CAs operated in a virtual machine environment (VME) audit logs must be generated for all applicable events on both the virtual machine (VM) and isolation kernel (i.e., hypervisor).

5.4.1 Types of Events Recorded

All security auditing capabilities of the CA, CSA, CMS and RA operating systems, and application Components required by this CP must be enabled. As a result, most of the events identified in the table must be automatically recorded. An "X" in a table cell indicates that the respective component (CA, CSA, CMS, RA) must 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 must include the following (either recorded automatically or manually for each auditable event):

- The type of event occurred,
- The date and time the event occurred,
- Where events occurred (e.g., on what systems or in what physical locations),
- Source of the event,
- Outcome of the event to include success or failure indicator; and
- The identity of any individual, subjects or objects/entities associated with the event.

Table 4 - Type of Events Recorded

Ref ID	AUDITABLE EVENT	CA	CMS	CSA	RA
1	**SECURITY AUDIT**	**CA**	**CMS**	**CSA**	**RA**
1.a	Any changes to the audit parameters (e.g., audit frequency, type of event audited)	X	X	X	X
1.b	Any attempt to delete or modify the audit logs	X	X	X	X
1.c	Obtaining a third-party timestamp	N/A	N/A	N/A	N/A
2	**IDENTITY PROOFING**	**CA**	**CMS**	**CSA**	**RA**
2.a	Successful and unsuccessful attempts to assume a role	X	X	X	X
2.b	The value of maximum number of authentication attempts is changed	X	X	X	X
2.c	Maximum number of authentication attempts occur during user log in	X	X	X	X
2.d	An administrator unlocks an account that has been locked because of unsuccessful authentication attempts	X	X	X	X
2.e	An administrator changes the type of authenticator (e.g., from a password to a biometric)	X	X	X	X
3	**LOCAL DATA ENTRY**	**CA**	**CMS**	**CSA**	**RA**
3.a	All security-relevant data that is entered in the system	X	X	X	X
4	**REMOTE DATA ENTRY**	**CA**	**CMS**	**CSA**	**RA**
4.a	All security-relevant messages that are received by the system	X	X	X	X

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

Ref ID	AUDITABLE EVENT	CA	CMS	CSA	RA
19	CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	CA	CMS	CSA	RA
19.a	All changes to the Certificate Revocation List profile	X	N/A	N/A	N/A
20	MISCELLANEOUS	CA	CMS	CSA	RA
20.a	A message from any source received by the CA requesting an action related to the operational state of the CA	X	N/A	N/A	N/A
20.b	Appointment of an Individual to a Trusted Role	X	X	X	X
20.c	Appointment of an Individual to a multi-person Role	X	X	N/A	N/A
20.d	Installation of the Operating System	X	X	X	X
20.e	Installation of the PKI Application	X	X	X	X
20.f	Installation of Hardware KSMs	X	X	X	X
20.g	Removal of KSMs	X	X	X	X
20.h	System Startup	X	X	X	X
20.i	Logon attempts to PKI application	X	X	X	X
20.j	Receipt of hardware / software	X	X	X	X
20.k	Attempts to set passwords	X	X	X	X
20.l	Attempts to modify passwords	X	X	X	X
20.m	Back up of the internal CA database	X	X	N/A	N/A
20.n	Restoration from back up of the internal CA database	X	X	N/A	N/A
20.o	File manipulation (e.g., creation, renaming, moving)	X	N/A	N/A	N/A
20.p	Posting of any material to a Repository	X	N/A	N/A	N/A
20.q	Access to the internal CA database	X	N/A	X	N/A
20.r	All Certificate compromise notification requests	X	X	N/A	X
20.s	Loading KSMs with Certificates	X	X	N/A	X
20.t	Shipment of KSMs	X	X	N/A	X
20.u	Zeroizing KSMs	X	X	N/A	X
20.v	Re-Key of the Component	X	X	X	X
21	CONFIGURATION CHANGES	CA	CMS	CSA	RA
21.a	Hardware	X	X	X	N/A
21.b	Software	X	X	X	X
21.c	Operating System	X	X	X	X
21.d	Patches	X	X	X	N/A
21.e	Security Profiles	X	X	X	X
22	PHYSICAL ACCESS / SITE SECURITY	CA	CMS	CSA	RA
22.a	Personnel Access to room housing to component	X	X	N/A	N/A
22.b	Access to a component – logged through a combination of automatic and	X	X	X	N/A

Ref ID	AUDITABLE EVENT	CA	CMS	CSA	RA
	manual logs based on the type of component and type of access				
22.c	Known or suspected violations of physical security	X	X	X	X
23	**ANOMALIES**	**CA**	**CMS**	**CSA**	**RA**
23.a	Software error conditions	X	X	X	X
23.b	Software check integrity failures	X	X	X	X
23.c	Receipt of improper messages	X	X	X	X
23.d	Misrouted messages	X	X	X	X
23.e	Network attacks (suspected or confirmed)	X	X	X	X
23.f	Equipment failure	X	X	N/A	N/A
23.g	Electrical power outages	X	X	N/A	N/A
23.h	Uninterruptible Power Supply (UPS) failure	X	X	N/A	N/A
23.i	Obvious and significant network service or access failures	X	X	N/A	N/A
23.j	Violations of Certificate Policy	X	X	X	X
23.k	Violations of Certification Practice Statement	X	X	X	X
23.l	Resetting Operations System clock	X	X	X	X

5.4.2 Frequency of Processing Log

Audit logs from the CA, CSA, CMS, and RA must be reviewed in accordance with the table listed below. At a minimum, a statistically significant set of security audit data generated by the Component since the last review must 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 must 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 because of these reviews must be documented.

Table 5 – Review Audit Log Criteria

Assurance Level	Review Audit Log
Basic	Only required for cause
Medium (all policies)	At least once every thirty days A statistically significant set of security audit data generated by the CA since the last review must 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
PIV-I Card Authentication	At least once every 30 days A statistically significant set of security audit data generated by the CA since the last review must 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

5.4.3 Retention Period for Audit Logs

Audit logs must be retained onsite for at least 2 months as well as being retained in the manner described below. The Individual who removes audit logs from the component must comply with the role separation requirements of Section *5.2.4 Roles Requiring Separation of Duties*. The Individual who removes audit logs from a CA, CSA, or CMS system must 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 must be responsible for managing the audit logs.

5.4.4 Protection of Audit Logs

Component system configuration and operating procedures must ensure 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 must 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 must be moved to a safe, secure storage location separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures

Security Audit logs and audit summaries must be backed up at least monthly. If audit records are stored locally in the system where the events occur, they must be transferred to a backup environment and protected as described in Section *5.4.4 Protection of Audit Logs*. The backup procedure may be automated or manual but must be sent off-site monthly.

The process for transferring the audit records to the backup environment must be documented.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to a component. Automated audit processes must be invoked at system (or application) startup and cease only at system (or application) shutdown. Audit collection systems must be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). 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) must be notified, and a determination must 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

Routine assessments must be performed for evidence of malicious activity and vulnerability self-assessments of security controls.

Automated vulnerability scans, if executed, should be run no less frequently than required by the risk rating of the component.

The methodology, tools and frequency of the vulnerability assessments must be documented.

Security audit data must 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 must check for continuity of the security audit data.

5.5 RECORDS ARCHIVAL

CA, CSA, CMS, and RA archive records must 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 must comply with their respective records retention policies in accordance with whatever laws apply to those entities.

Key and key recovery as stated in section *4.12.1 Key Escrow and Recovery Policy and Practices*.

5.5.1 Types of Events Archived

At a minimum, the following data must be recorded for archive across all Assurance Levels:

Table 6 - Types of Events 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, authorized or rejected	As specified in Section 5.4.1 Ref ID 11.a			
Revocation requests	As specified in Section 5.4.1 Ref ID 12.a			
Subscriber identity authentication data (per Section 3.2)	X	N/A	X	X
Documentation of receipt and Acceptance of Certificates	X	N/A	X	X
Subscriber agreements	X	N/A	X	X
Documentation of receipt of Subscriber's KSM	N/A	N/A	X	X
Documentation of receipt of KSMs (CA/CSA/CMS/RA)	X	X	X	X
All Certificates Issued or published	X	N/A	X	N/A
Record of Re-Key (of CA/CSA/CMS/RAs KSM)	X	X	X	X
All CRLs issued and/or published	X	X	N/A	N/A
Other data or applications to verify archive contents	X	X	X	X
Compliance Auditor reports, generated by internal reviews and documentation generated during third party audits	X	X	X	X
Any changes to the Audit parameters, e.g., audit frequency, type of	As specified in Section 5.4.1 Ref ID 1.a			
Any attempt to delete or modify the Audit logs	As specified in Section 5.4.1 Ref ID 1.b			

Data To Be Archived	CA	CSA	CMS	RA
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	As specified in Section 5.4.1 Ref ID 6.a			
All access to Certificate subject private keys retained within the CA for key recovery purposes	As specified in Section 5.4.1 Ref ID 7.c			
All changes to the trusted public keys, including Certificates used for trust between the CA and other components such as CMS, RA, etc.	As specified in Section 5.4.1 Ref ID 8.a			
The export of private and secret keys (keys used for a single session or message are excluded)	As specified in Section 5.4.1 Ref ID 10.a			
All records related to certificate status change whether generated directly on the CA or generated by a related external system or process	As specified in Section 5.4.1 Ref ID 13.a			
Appointment of an individual to a Trusted Role	As specified in Section 5.4.1 Ref ID 20.b			
Destruction of cryptographic modules	As specified in Section 5.4.1 Ref ID 20.h			
All Certificate compromise notifications	As specified in Section 5.4.1 Ref ID 20.s			
Remedial action taken as a result of violations of physical security	X	X	X	X
Violations of Certificate Policy	As specified in Section 5.4.1 Ref ID 23.j			
Violations of Certification Practice Statement	As specified in Section 5.4.1 Ref ID 23.k			
OCSP Requests and Responses	N/A	X	X	N/A

5.5.2 Retention Period for Archive

The minimum retention periods for archive data must be no less than 3 years.

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

The CPS and any applicable RPS must describe the method for destruction of out-of-date records.

5.5.3 Protection of Archive

Only authorized Individuals must 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 individuals other than the RA Administrator (e.g., Information Assurance Officer or IAO).

The contents of the archive must not be released except as determined by the PMA, CA, or as required by law and in accordance with Sections *9.3 Confidentiality of Business Information* & *9.4 Privacy of Personal Information* of this CP. Records and material information relevant to use of, and reliance on the Certificates Issued by CAs governed by this policy must be archived. Archive media must 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 must 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 must be accurately timestamped as they are created. The CPS must describe how system clocks used for timestamping are maintained in synchrony with an authoritative time standard.

The time precision must be such that the sequence of events can be determined.

5.5.6 Archive Collection System (Internal or External)

The applicable CPS or RPS must 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, is published in the applicable CPS or RPS.

The archive contents must not be released except as determined by the IdenTrust 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 must be used for Certificate signing. The older, but still valid, Certificate will be available to verify old signatures until all 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 must be retained and protected.

CAs Cross-Certified with the US FBCA or other bridges must 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 must either establish Key rollover Certificates as described above or must 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 must have maximum Validity Periods not to exceed the requirements in Section *6.3.2 Certificate Operational Periods and Key Usage Periods*.

5.7 COMPROMISE AND DISASTER RECOVERY

If a CA or CSA detects a potential hacking attempt or other form of compromise, it must perform an investigation 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 Entity (CA) Private Key Compromise Procedures* must be followed. Otherwise, the scope of potential damage must be assessed 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.

5.7.1 Incident and Compromise Handling Procedures

The CA and applicable PMA(s) must 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,
- Violation or threat of violation to the system,

- Improper usage, malicious or anomalous activity,
- Violations of the CA's CPS or CP
- Successful denial of service attacks of CA components,
- Suspected or detected compromise of a CSS,
- Suspected or detected compromise of an RA.
- 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 must be reestablished as quickly as possible in accordance with procedures set forth in the CA'S CPS.

5.7.1.1 CA Incident

In the event of an incident as described above, the Issuing CA must notify the cross-certified entity within 24 hours of incident discovery, along with preliminary remediation analysis. The notification provided directly to the cross-certified entities must also include detailed measures taken to remediate the incident.

Once the incident has been resolved, the organization operating the CA must provide notification directly to the relevant PAAs which include detailed measures to remediate the incident. The notice must include the following:

- Which CA components were affected by the incident
- The CA's interpretation of the incident
- Who is impacted by the incident
- When the incident was discovered
- A complete list of all Certificates that may have been issued erroneously or are not compliant with the CP/CPS because of the incident
- A statement that the incident has been fully remediated.

The notification must include a preliminary remediation analysis.

5.7.1.2 RA Incident

RA Systems and CMSs must 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 must 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 must be Revoked. The damage caused by the RA System or CMS compromise must be assessed by both the operating PMA and the IdenTrust PMA, and all Subscriber Certificates that may have been compromised must be Revoked. Subscribers must be notified of such Revocation. The CMS must be reestablished as soon as practical through the 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 must maintain backup copies of hardware, system, databases, and Private Keys to rebuild the CA capability in case of software and/or data corruption. When computing resources, software, and/or data are corrupted, the CAs must 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 must be reestablished, giving priority to the ability to generate Certificate status information within the CRL issuance schedule specified in Section *4.9.7 CRL Issuance Frequency*; and
- If the CA Signature Keys are destroyed, CA operation must 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 update field the valid CRL, then all CAs that have been Issued Certificates by the CA must be securely notified within 24 hours. This will allow other CAs to protect their Subscribers' interests as Relying Parties. The CA must 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 timeframe, the CA must determine whether to request Revocation of its Certificate(s). If the CA is a Root CA, the CA must determine whether to notify all Subscribers that use the CA as a Trust Anchor to delete the Trust Anchor.

In the event of an incident as described above, IdenTrust must post a notice on its web page identifying the incident and provide notification to all related parties. See Section *5.7.1 Incident and Compromise Handling Procedures*, for contents of the notice.

5.7.3 Entity CA Private Key Compromise Procedures

5.7.3.1 CA Private Key Compromise Procedures

If a CA's Signature Keys are compromised, lost, or suspected to be compromised the following steps must be performed:

- All cross-certified CAs must be securely notified according to the timelines specified in Section *5.7.1 Incident and Compromise Handling Procedures* (so that entities may Issue CRLs revoking any Cross-Certificates Issued to the CA);
- A CA Key Pair must be generated by the CA in accordance with procedures set forth in the applicable CPS,
- New CA Certificates must be requested in accordance with the initial Registration process set elsewhere in this CP,
- If the CA can obtain accurate information on the Certificates it has Issued and 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
- If the CA is the Root CA, it must provide the Subscribers the new Trust Anchor using secure means.

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

If a CSA Key is compromised, all Certificates Issued to the CSA must 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:

- The Certificate must be immediately Revoked,
- A new Key Pair must be generated in accordance with procedures set forth in the applicable CPS,
- A new Certificate must be requested in accordance with the initial Registration process set elsewhere in this CP,
- All Certificate Registration requests approved by the RA, RA Administrator, or LRA since the date of the suspected compromise must be reviewed to determine legitimacy; and
- For those Certificates requests or approval than cannot be ascertained as legitimate, the resultant Certificates must be Revoked and their subjects (i.e., Subscribers) must be notified of Revocation.

5.7.3.2 KRS Private Key Compromise Procedures

IdenTrust does not escrow or recover keys.

5.7.3.3 CA Private Key Compromise Procedures-Root CA

When Revocation of the Root Certificate is required, in addition to the foregoing procedures, IdenTrust shall immediately notify the PAAs of all Bridges that are Cross-certified and request that the Cross Certificate Issued by those Bridges be Revoked. A new Root CA Key Pair, self-signed Root CA Certificate with new DN, and CRL shall be generated in a Key Generation ceremony consistent with the procedures of Section *6.1.1 Key Pair Generation*.

CAs and RAs are required by contract to facilitate the replacement of the Revoked Root CA Certificate with the new Root CA Certificate in Subscriber and Relying Party applications. IdenTrust shall also notify PKI Participants that the new Root Certificate is available in a secure area of the IdenTrust website (HTTPS) where it can be downloaded in a Server-authenticated SSL/TLS-encrypted session.

Subordinated CAs and Cross-certified CAs shall be asked to submit new Certificate requests.

IdenTrust shall notify all interested parties via email, telephone or written letter sent by courier service. In addition, IdenTrust shall set up an informational secure site (https://) that establishes a Server-side session secured using 1 of its high assurances IdenTrust Root Certificates (e.g., DST Root CA X1 or DST Root CA X3), which are embedded in the most widely distributed commercial browsers.

Cross-Certification of the new Root CA with the Bridges shall proceed in accordance with each specific PKI Cross Certification Process.

5.7.3.4 CA Private Key Compromise Procedures-CSA Key

OCSP Responder Certificates shall be Issued with the nocheck extension (id-pkix-ocsp-nocheck) specifying that OCSP Responder Certificates are not checked by the Relying Party applications for the lifetime of the Certificate (30 days). If the CSA Signing Key has been or is suspected to have been compromised, then the Head of IdenTrust Operations shall convene a meeting of personnel involved in CSA operations to assess the degree and scope of the compromise. If it is determined that Private Keys were compromised, a new OCSP Responder Key Pair and Certificate shall be immediately created (signed by the SubCA) and installed in the OCSP Responder as soon as possible.

For any period of compromise, all signed validations for that period (during which the CSA Key was suspected to have been compromised) shall be reviewed and either re-signed with a new Key or may be handled by agreement with the Participants CAs involved in each affected transaction.

5.7.3.5 CA Private Key Compromise Procedures-CMS Keys

If a CMS Content Signing or the master Keys have been or are suspected to have been compromised, the Head of IdenTrust Operations shall convene a meeting of management representatives (including representatives of the CA, RAs, and smart card vendor/bureau) to assess the situation and take appropriate action. IdenTrust personnel in Trusted Roles shall implement the procedural steps and tasks that have been outlined for Key Compromise in the Security Incident Response Plan, including:

1. Quantifying the scope, extent, and effects of the compromise,
2. Suspending all Certificates that are Issued to the CMS if there is suspicion of compromise,
3. Suspending end entity Certificates that are suspected of being Issued after the compromise,
4. Revoking Certificates that are Issued to the CMS and end entities if there is confirmation of compromise,
5. Suspension of the CMS operation,
6. Notifying all interested parties (either by Certificate-based communication, telephone or written letter sent by courier service). Recipients of this communication will include:
    - IdenTrust, if they have not already received notice,
    - Smart card vendor/bureau,
    - All of RAs and LRAs; and

- All Subscribers affected.

The IdenTrust PMA shall investigate the incident, and if necessary, will forensically record and analyze the cause of the compromise. A report shall be prepared and delivered to the IdenTrust PMA concerning the cause of the compromise and what measures have/will be taken to prevent a future recurrence.

If no compromise has been confirmed, all Certificates shall be unsuspended in accordance with Section *4.9.16 Limits on Suspension Period*.

If compromise of the Content Signing Private Key has been confirmed, the CMS operator shall generate a new Content Signing Key Pair and request a Certificate with a new DN, in accordance with original Key Generation procedures. If the compromise of master Keys is confirmed, in collaboration with the smart card vendor, new master Keys shall be generated and transferred to the CMS Operator. The CMS shall issue new smart cards and associated Certificates, upon completing identity verification processes outlined in Section *3.2 Initial Identity Validation*.

5.7.3.6 CA Private Key Compromise Procedures-RA System and LRA Private Keys

All RA Administrators and LRAs, including External RA Administrators and LRAs who are obligated by contract, shall be required by this CP and CPS to immediately notify IdenTrust if they believe an RA System Private Key or an LRA's Private Key has been or is suspected to have been compromised and request Revocation. IdenTrust must revoke the Certificate, and the Head of IdenTrust Operations, the Security Officer or an Authorizing Official for the RA shall meet with the LRA or RA Administrator to assess and address the situation (including deciding on Revocation) and take any other actions needed to identify and remedy the causes of the compromise, to ensure no recurrence happens. These actions shall include, but are not limited to, the Issuance of new RA System or LRA Certificates in accordance with this CP, Renewal, or reissuance of compromised Subscribers' Certificates. In cases where approved Subscribers Certificates cannot be ascertained as legitimate, the Certificates must be revoked and the Subscribers notified of the revocation action.

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 must request that its Certificates be Revoked. The CA must follow the steps in Section *5.7.3 Entity (CA) Private Key Compromise Procedures* and its sub-sections.

5.8 CA AND RA TERMINATION

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

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

Whenever possible, IdenTrust will notify all vested parties at least 2 weeks prior to the termination of any CA operated by an Entity cross certified under this policy. For emergency termination, CAs must follow the notification procedures in Section *5.7 Compromise and Disaster Recovery* and/or its sub-sections.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

Key generation must be performed using a FIPS approved method or equivalent international standard (e.g. FIPS mode), with the exception of subscriber rudimentary keys. When a FIPS 140-1/2 module is used, the module must be validated and must be used in FIPS approved mode.

6.1.1.1 CA Key Pair Generation

For CAs, Cryptographic keying material must be generated in FIPS 140 Level 3 (or higher) validated hardware KSMs using FIPS approved methods. CA Key Pairs must be generated under Two-Person Control. Key Pair generation must create a verifiable audit trail that security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show appropriate role separation was used. The Key Pair generation process must be validated by an independent third party by witnessing the Key Generation or by examining the signed and documented record of the Key Generation.

6.1.1.1.1 CSA Key Pair Generation

For CSAs, Cryptographic keying material must be generated in FIPS 140 Level 2 (or higher) validated hardware KSMs using FIPS approved methods. CSA, Key Pairs must be generated under Two-Person Control. Key Pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. The Key Pair generation process must be validated by an independent third party by witnessing the Key Generation or by examining the signed and documented record of the Key Generation.

6.1.1.1.2 RA LRAs and CMS Key Pair Generation

For RA, LRAs and CMS, Cryptographic keying material must be generated in FIPS 140 Level 2 (or higher) validated hardware KSMs. Cryptographic keying material for the PIV-I Content Signing Certificate must be generated in FIPS 140 Level 2 (or higher) validated hardware KSMs.

Activation of the CMS Master Key must require hardware assurance authentication by Individuals in Trusted Roles. Key diversification operations by the CMS must also occur on the CMS hardware KSM. The diversified Keys must only be stored in hardware KSMs that support PIV-I hardware assurance or commensurate. CMS Master Key and diversified Keys must be protected from unauthorized disclosure and distribution. Card management must be configured such that only the authorized CMS can manage Issued cards.

6.1.1.1.3 PIV-I Content Signing Key Pair Generation

The diversified Keys must only be stored in hardware KSMs that support PIV-I hardware assurance or commensurate. CMS Master Key and diversified Keys must be protected from unauthorized disclosure and distribution. Card management must be configured such that only the authorized CMS can manage Issued cards. Cryptographic keying material for the PIV-I Content Signing Certificate must be generated in FIPS 140 Level 2 (or higher) validated hardware KSMs.

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 Private Key Delivery to Subscriber* must also be met.

6.1.1.2.1 Subscriber Non-PIV-I Certificates Key Pair Generation

Key Generation must be performed using a FIPS approved method as specified in Section *6.2.1 Cryptographic Module Standards and Controls* of this CP.

6.1.1.2.2 Subscriber PIV-I Certificates Key Pair Generation

For PIV-I Hardware and PIV-I Card Authentication Assurance levels, other requirements explained in Section 11 of this CP apply.

6.1.1.3 CSS Key Pair Generation

Cryptographic keying material used by CSSs to sign status information must be generated in [FIPS 140] validated cryptographic modules as specified in Section *6.2.1 Cryptographic Module Standards and Controls*.

6.1.1.4 PIV-I Content Signing Pair Generation

Cryptographic keying material used by PIV-I issuing systems or devices for PIV-I Content Signing must be generated in [FIPS 140] validated cryptographic modules as specified in Section *6.2.1 Cryptographic Module Standards and Controls*.

6.1.2 Private Key Delivery to Subscriber

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 must 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 must be met:

- For Group Certificates, any entity receiving and holding Private Key(s) of a Signature Certificate on behalf of a Subscriber must meet the requirements for control of Private Keys as stated in Section *3.2.3.3 Authentication of Human Subscribers for Group Certificates*.
- Other than for Group Certificates, any entity that generates a Private Key for the Signature Certificate of a Subscriber must not retain any copy of the Private Key after delivery to the Subscriber,
- The Private Key must be protected from activation, compromise, or modification during the delivery process,
- The Subscriber must acknowledge receipt of the Private Key, typically by having the Subscriber use the related Certificate,
- Delivery must 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 must be maintained until the Subscriber accepts possession of it,
- For electronic delivery of Private Keys, the Key material must be encrypted using a cryptographic algorithm and Key size at least as strong as the Private Key,
- Activation Data must be delivered using a separate secure channel, and
- For shared Key applications, Organizational identities, and network Devices, see Section *3.2 Initial Identity Validation* and/or section 3.2 sub-sections.

The CA, RA, or CMS operator must maintain a record of the Subscriber acknowledgement of receipt of the KSM.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity must be delivered securely to the CA for Certificate issuance.

Public Keys must be delivered to the Certificate Issuer in a way that binds the Applicant's verified identification to the Public Key being certified. Any method of binding (cryptography, physical, procedural or other appropriate method) must be accomplished using means that are at least as secure as the security offered by the Keys being certified. Methods used for Public Key delivery are stipulated in the CPS or RPS.

6.1.4 CA Public Key Delivery to Relying Parties

CA must distribute the Public Key in a secure fashion. The 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 must 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 must be at least 2048 bits RSA or at least 256 bits for ECDSA. Public Keys in all self-signed Certificates generated after December 31, 2010, that expire after December 31, 2030, must be at least 3072 bits for RSA or at least 256 bits for ECDSA.

CAs that generate Certificates and CRLs under this policy must use Signature Keys of at least 2048 bits for RSA or at least 256 bits for ECDSA. All Certificates, except self-signed Certificates, that expire after December 31, 2030, must 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 must 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 December 31, 2030, must be generated using, at a minimum, SHA-256. CSSs must 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 must contain Public Keys that are at least 2048 bits RSA, or 256 bits for elliptic curve algorithms. The following special conditions also apply:

- End-entity Certificates that expire after December 31, 2030, must 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 must contain Public Keys and algorithms that conform to [NIST SP 800-78-4].

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP must 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 must 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 December 31, 2030.

6.1.6 Public Key Parameters Generation and Quality Checking

IdenTrust performs partial public key validation as specified in Nist SP 800-89 (section 5.3.3) and must be generated in accordance with FIPS 186. Parameter quality checking, including primarily testing for prime numbers, must also 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 must assert digitalSignature or keyEncipherment, but not both. With the exception of Device Certificates, "dual use" Certificates asserting both digitalSignature and keyEncipherment must not be Issued by CAs operating under this CP.

For End Entity Certificates, the Extended Key Usage extension must always be present and must not contain anyExtendedKeyUsage {2.5.29.37.0}.

Extended Key Usage OIDs must be consistent with key usage bits asserted.

If a Certificate is used for authentication of ephemeral keys, the Key Usage bit in the Certificate must assert the digitalSignature bit and may or may not assert keyEncryption and keyAgreement depending on the public key in the Certificate.

PIV-I Content Signing certificates must include a critical Extended Key Usage extension that asserts only id-fpki-pivi-content-signing {2.16.840.1.101.3.8.7} (see [PIV-I Profile]).

PIV-I Card Authentication certificates must include a critical Extended Key Usage extension that asserts id-piv-cardAuth {2.16.840.1.101.3.6.8}

6.1.7.1 Key Usage Purposes for Signing Certificates

Subscriber Certificates must assert key usages based on the intended application of the Key Pair. In particular, Certificates to be used for digital signatures (including authentication) must set the digitalSignature and/or nonRepudiation bits.

6.1.7.2 Key Usage Purposes for Encryption Certificates

Certificates to be used for Key or data encryption must set the keyEncipherment bits. Certificates to be used for key agreement must set the keyAgreement bit.

6.1.7.3 Key Usage Purposes for DirectTrust Signing and Encryption Certificates

All Subscriber Certificates issued with a DirectTrust policy OID must assert a Basic Constraint of CA=FALSE and may assert an extended key usage not in conflict with the Certificate primary key usages.

6.1.7.4 Key Usage Purposes for Group Certificates

Group Certificates must not assert nonRepudiation.

6.1.7.5 Key Usage Purposes for CA Certificates

CA Certificates must set 2 key usage bits: cRLSign and/or keyCertSign.

6.1.7.6 Key Usage Purposes for RA System Certificates

RA System Certificates are Device Certificates and may include both digitalSignature and keyEncipherment in the key usage extension.

6.1.7.7 Key Usage Purposes for Content Signing Certificates

PIV-I Content Signing Certificates must include an extended key usage of id-fpki-pivi-content-signing.

6.1.7.8 Key Usage Purposes for OCSP Responder Certificates

Where the subject signs OCSP responses, the Certificate may also set the digitalSignature and/or nonRepudiation bits.

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 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.

PIV-I Cards must only be issued using card stock that has been tested and approved by the FIPS 201 Evaluation Program and listed on the GSA Approved Products List (APL). Card stock that has been removed from the APL may continue to be issued for no more than 1 year after GSA approved replacement card stock is available. PIV-I cards issued using the deprecated card stock may continue to be used until the current Subscriber Certificates expire. On an annual basis, for each PCI configuration used (as defined by the FIPS 201 Evaluation Program), a populated, representative sample PIV-I Card from each RA that utilizes PIV-I cards must be submitted to the FIPS 201 Evaluation Program for testing.

For PIV-I Assurance Levels, additional requirements for PIV-I cards detailed in *Appendix A* & *Appendix B* also apply.

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of Subscriber Certificates in 1 location. The Custodial Subscriber Key Store must 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.

Cryptographic modules for Custodial Subscriber Key Stores at the Rudimentary Assurance Level must be no less than FIPS 140 Level 1 (Hardware or Software). For all other levels, the cryptographic module must be no less than FIPS 140 Level 2 Hardware.

In addition, authentication to the Cryptographic Device in order to activate the private key associated with a given Certificate must require authentication commensurate with the assurance level of the Certificate.

6.2.2 Private Key Multi-Person Control

A single person must 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 must 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 Number of Persons Required per Task* of this CP.

6.2.3 Private Key Escrow

Private signature and encryption Keys of a CA, must not be escrowed under any circumstances, as escrow and key recovery are not supported within the IdenTrust CA.

6.2.3.1 Escrow of Subscriber Private Signature Keys

Private Keys of Subscriber encryption Certificates may be escrowed. Subscriber Private Keys used to support services associated with digitalSignature and nonRepudiation bits must not be escrowed.

6.2.3.2 Escrow of Subscriber Private Encryption and Dual Use Keys

IdenTrust does not issue dual use Subscriber Certificates under this policy.

6.2.4 Private Key Backup

See subsections below.

6.2.4.1 Backup of CA Private Signature Key

Backup of Private Keys of CA Certificates is required to facilitate disaster recovery. Private Keys must 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 Number of Persons Required per Task*.

At least 1 copy of the Private Key of the CA Certificate must be stored off site. All copies of the Private Key must be accounted for and protected in the same manner as the original. Procedures for Private Key backup of CA Certificates must be identified in the CA'S CPS.

Refer to section *6.2.4.4 Backup of Subscriber Key Management Private Key* for additional details.

6.2.4.2 Backup of RA Private Signature Key

Backup Private Keys of RA system Certificates by the RA is permitted only to facilitate disaster recovery. Such Private Keys must be backed up under the same multi-person control as used to generate the original Private Key, as described in Section *5.2.2 Number of Persons Required per Task*, and must undergo audit(s) in accordance with Section 8 of this CP. Procedures for backup of Private Keys of RA system Certificates must be identified in the CA'S CPS, or RA'S RPS.

6.2.4.3 Backup of Subscriber Private Signature Key

Private Keys of LRA Signing Certificates must not be backed up.

Private Keys of Signing Certificates Issued to Subscribers on hardware KSMs must 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 must not be stored in plain text form outside the KSM. Storage must ensure security controls are consistent with the protection provided by the Subscriber's KSM.

6.2.4.4 Backup of Subscriber Key Management Private Key

Backed up Private Keys of Subscriber Encryption Certificates must not be stored in plain text form outside the KSM. Storage must ensure security controls are consistent with the protection provided by the Subscriber's KSM.

6.2.4.5 Backup of CSA Private Key

CSA is also referenced as CSS in this CP and the terms can be considered as interchangeable. Private Keys of CSA Certificates may be backed up on a KSM approved for CSAs. The backup must be performed under the same control as the CSA Key activation. A single copy of the Private Key must be stored at the CSA location. A second copy must be kept at the CSA backup location. All copies of the CSA Private Key must be accounted for and protected in the same manner as the original. Procedures for backup of CSA Private Keys must be identified in the CA'S CPS.

6.2.4.6 Backup of PIV-I Content Signing Private Key

Private Keys of PIV-I Content Signing Certificates must be backed up under the same multi-person control as for initial Issuance. A single backup copy of the Private Key must be stored at or near the content signing system location. A second backup copy must be kept at a backup location. Procedures for backup of the Private Keys of PIV-I Content Signing Certificates must be included in the appropriate CPS and must meet the multiparty control requirements of Section *5.2.2 Number of Persons Required per Task*.

6.2.4.7 Backup of Device Private Keys

Private Keys of Devices may be backed up or copied but must be held under the control of the Device's Primary Machine Operator or other authorized administrator. Backed up Private Keys must not be stored in plain text form outside the KSM. Storage must ensure security controls consistent with the protection provided by the Device's KSM.

6.2.5 Private Key Archival

CA Private Signature keys and Subscriber Private signature keys must 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 must be generated in and remain in a KSM meeting the storage requirements for such Keys as described in Section *6.2.1 Cryptographic Module Standards and Controls*. At no time must 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 Backup of CA Private Signature Key*.

Subscribers of Certificates Issued to hardware KSMs must 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 must be protected from disclosure.

6.2.7 Private Key Storage on Cryptographic Module

Procedures for Private Key storage on a Cryptographic Module may vary based on the type of Certificate to which the Private Keys are associated. See Section 6.2.7 of the IGC CPS for details.

No stipulation beyond that specified in [FIPS-140]

6.2.8 Method of Activating Private Keys

Cryptographic modules must be protected from unauthorized access.

CA, CSA, and PIV-I Content Signing Key activation requires multiparty control as specified in Section *5.2.2 Number of Persons Required per Task*.

Subscribers must 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. When pass-phrases or PINs are used, they must be a minimum of 6 characters. Entry of Activation Data such as passwords and PINs must be protected from disclosure (i.e., the data must 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 must be commensurate with the level of threat in the Device's environment, and must protect the Device's hardware, software, and the KSM and its Activation Data from compromise.

6.2.9 Method of Deactivating Private Keys

KSMs that have been activated must not be left unattended. After use, the KSM must be deactivated (e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS). Hardware KSMs must be removed and stored in a secure container or environment when not in use.

6.2.10 Method of Destroying Private Keys

Individuals in Trusted Roles must destroy CA, CSA, CMS, RA, and LRA Private Keys when they are no longer needed.

Subscriber Private Keys must 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 Cryptographic Module Standards and Controls*.

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 Usage Periods

CAs that distribute their self-signed Certificates for use as trust anchors must limit the use of the associated private key to a maximum of 30 years.

For all other CAs, the CA must limit the use of its private keys to a maximum of 10 years for Subscriber Certificates and 10 years for CRL signing and OCSP responder Certificates.

Content signers may use their private keys for 3 years; the lifetime of the associated public keys must not exceed 9 years.

Subscribers' signature private keys and Certificates have a maximum lifetime of 3 years. Subscriber key management Certificates have a maximum lifetime of 3 years; use of Subscriber key management private keys is unrestricted.

PIV-I Subscriber Certificate expiration must not be later than the expiration date of the PIV-I hardware token on which the Certificates reside.

Subscriber public keys in Certificates that assert the id-fpki-pivi-content-signing OID in the extended key usage extension have a maximum usage period of 9 years. The private keys corresponding to the public keys in these Certificates have a maximum usage period of 3 years. Expiration of the id-fpki-certpcy-pivi-contentSigning Certificate must be later than the expiration of the id-fpki-certpcy-pivi-hardware and id-fpki-certpcy- pivi-cardAuth Certificates.

For PIV-I, CSS Certificates that provide revocation status have a maximum Certificate validity period of 35 days.

The following table provides the maximum Private Key Certificate Validity Periods for CA, CSA, CMS, RA, LRA, Subscriber Certificates, and Cross-Certificates implemented by IdenTrust.

Table 7 - Private Key Certificate Validity Periods

Key Type	Private Key Usage Period	Certificate Lifetime
Root CA	30 years	30 years
SubCA	10 years	10 years
CSA/CSS	3 years	31 days
RA	3 years	3 years
IGC PIV-I Content Signer	3 years	9* 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 years	3 years
Cross-Certificate Key Pair usage is dictated by whether the Key belongs to the SubCA 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 must not Issue Subscriber Certificates that extend beyond the expiration date of their own Certificates and Public Keys.		

(*)PIV-I Subscriber Certificate expiration cannot be later than the expiration date of the PIV-I hardware token on which the Certificate resides and the expiration date of the PIV-I Content Signer Certificate used to sign the Subscriber Certificate on the PIV-I card will not expire before the expiration date of such Subscriber Certificate.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The Activation Data used to unlock Private Keys, in conjunction with any other access control, must have an appropriate level of strength for the Keys or data to be protected. Activation Data may be user selected. Activation

Data must meet the requirements of FIPS 140 Level 2. If the Activation Data must be transmitted, it must 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 must be changed upon corresponding Re-Rey.

6.4.2 Activation Data Protection

Activation Data used to unlock Private Keys must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data must be either:

- Memorized,
- Biometric in nature, or
- Recorded and secured at the level of assurance associated with the activation of the cryptographic module, and must not be stored with the cryptographic module.

The protection mechanism must 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

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 must 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 must 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

For those portions of the CA operating in a VME, the following security functions also pertain to the hypervisor:

- Require authenticated logins,
- Provide discretionary access control,
- Provide a security audit capability,
- Enforce separation of duties for PKI roles,
- Prohibit object reuse or require separation for CA random access memory,

- Require use of cryptography for session communication and database security,
- Archive CA history and audit data,
- Require self-test security-related CA services,
- Enforce domain integrity boundaries for security-critical processes.

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

The computer system must be configured only the minimum required accounts and network services.

6.5.2 Computer Security Rating

The Issuing CA's equipment will meet and be operated to at least a C2 [TCSEC] or E2/F-C2 [ITSEC] rating or equivalent. The Issuing CA's equipment operating at a C2 equivalence

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

CAs and RAs must 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 must be met as part of the system development process:

- CAs and RAs must 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 must 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 must be developed in a controlled environment, and the development process must be defined and documented. The CA or RA must 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 must demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management,
- All hardware and software must 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) must be dedicated to performing PKI functions. There must 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 must be taken to prevent malicious software from being loaded. Applications required to perform the PKI operation must be obtained from sources authorized by local policy; and
- Hardware and software updates must be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

CA, CSA, CMS, and RA hardware and software must 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 must be documented and controlled. There must be a mechanism for detecting unauthorized modification to the CA, CSA, CMS and RA software or configuration.

A formal configuration management methodology must be used for installation and ongoing maintenance of CA, CSA, CMS, and RA systems. The CA, CSA, CMS, and RA software, when first loaded, must 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 must be verified continually.

6.6.3 Life Cycle Security Controls

The CAS's TAs and LRAs are required to take reasonable care to prevent malicious software from being loaded on RA equipment through user education coupled with the use of antivirus programs and adhering to the software manufacturers recommended patches applicable to the installed software. Only applications required to perform the organization's mission must be loaded on the RA computer, and all such software must be obtained from sources authorized by local policy. Data on RA equipment must be scanned for malicious code on first use and periodically afterward.

6.7 NETWORK SECURITY CONTROLS

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

CAs, CSAs, CMSs, RAs, and LRAs must 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 must be turned off. Any network software present must be necessary to the functioning of PKI services.

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

Any remote workstation used to administer the CA must use a Virtual Private Network (VPN) to access the CA. The VPN must be configured for mutual authentication, encryption, and integrity. If mutual authentication is shared secret based, the shared secret must be changed at least annually, must be randomly generated, and must have entropy commensurate with the cryptographic strength of certificates issued by the PKI being administered.

The CA must permit remote administration only after successful multi-factor authentication of the Trusted Role at a level of assurance commensurate with that of the CA.

6.8 TIME STAMPING

All CA, CSA, CMS, and RA components must 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 must 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 must be accurate to within 3 minutes. Electronic or manual procedures may be used to maintain system time on a contingency basis if automated processes encounter a failure, requiring time resynchronization. Clock adjustments are auditable events as listed in Section *5.4.1 Types of Events Recorded*.

The time precision must be such that the sequence of events can be determined.

7 CERTIFICATE, CARL/CRL, AND OCSP IGC PROFILES FORMAT

7.1 CERTIFICATE PROFILE

All certificates must be compatible with X.509. Detailed Profiles are found in the Certificate Profiles. For ease of reference, high-level profile information is described in this Section .

7.1.1 Version Numbers

IdenTrust must issue X.509 v3 Certificates with version field populated with integer "2".

7.1.1.1 Serial Numbers

All Certificates must include a unique serial number greater than zero (0) exhibiting at least 64 bits of output from cryptographically secure pseudo-random number generator of entropy using a FIPS-validated cryptographic module.

7.1.2 Certificate Extensions

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

Certificates Issued by CAs under this CP must comply with the IGC Certificate Profiles .

The IGC Certificate Profiles are subject to change and new versions will be published from time to time. CAs will be notified of the IGC Certificate Profiles changes and must 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 must include those extensions required by this CP. Any optional or additional extensions must be non-critical and must not conflict with the Certificate and CRL profiles defined in this CP and the IGC Profiles. Conforming Certificates must include all required extensions.

7.1.3 Algorithm Object Identifiers

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

7.1.3.1 Signature Algorithm OIDs

Table 8 - Algorithms and OIDs for Signatures

Algorithm	OID
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11} “1.2.840.113549.1.1.11”
Sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12} “1.2.840.113549.1.1.12”
Sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13} “1.2.840.113549.1.1.13”
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha256(2)} “1.2.840.10045.4.3.2”
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 } “1.2.840.10045.4.3.3”
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 } “1.2.840.10045.4.3.4”

7.1.3.2 Subject Public Key Information

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}. "1.2.840.113549.1.1.1"
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) public-key-type(2) 1} "1.2.840.10045.2.1"

7.1.3.3 Elliptic Curve Public Key

Where non-CA Certificates contain an elliptic curve Public Key, the parameters must be specified as one of the following named curves:

Table 10 - Algorithms and OIDs for Identifying Elliptic Curve Key Information

Table 9 - Elliptic Curve Public Key Named Curve	OID
Curve P-256 (ansip256r1)	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 } 1.2.840.10045.3.1.7
Curve P-384 (ansip384r1)	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 } 1.3.132.0.34

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 must have only 1 value.

Table 11 - 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 12 - 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")

When multiple values exist for an attribute in a DN, the DN must 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 the IGC Certificate Profiles subject to the requirements above.

CAs may obscure a Subscriber Subject Name to meet local privacy regulations if 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

CA and Subscriber Certificates Issued under this CP must assert 1 or more of the OIDs listed in Section *1.2.2 Object Identifier (OID).* 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.
Certificates issued for PIV-I Card Authentication or PIV-I Content Signing do not express any other policy OIDs.
Delegated OCSP Responder Certificates assert all policy OIDs for which they are authoritative.

7.1.7 Usage of Policy Constraints Extension

CA and Subscriber Certificates that are Issued under this CP assert 1 or more of the IGC Certificate policy OIDs listed in Section *1.2.2 Object Identifier (OID).* Additional OIDs asserting compliance with other Certificate policies may also be included, as defined in the CPS and/or CP document.
CAs must adhere to the Certificate formats described in this CP.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates Issued by CA's may contain policy qualifiers identified in RFC 5280.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Processing semantics for the critical CP extension must conform to X.509 certification path processing rules.

7.1.10 Inhibit Any Policy Extension

The CA may assert inhibitAnyPolicy in CA Certificates. When present, this extension may be marked critical, to support legacy applications that cannot process inhibitAnyPolicy. Skip Certs must be set to 0, to support the requirement for Certificate policies in the Federal PKI.

7.2 CRL PROFILE

The CRL Profile is specified in the Certificate Profiles.

7.2.1 Version Number(s)

CAs must Issue X.509 version 2 CRLs (populate version field with integer "1").

7.2.2 CRL and CRL Entry Extensions

CRLs must comply with the CRL extension profiles specified in IGC Profiles.

7.3 OCSP PROFILE

OCSP Requests and responses are in accordance with RFC 6960. IGC Profiles contains the OCSP Request and response formats.

7.3.1 Version Number(s)

The version number for request and responses is version 1.

7.3.2 OCSP Extensions

Critical OCSP extensions must not be used.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

CAs, CMSs and RAs must 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 must specify the relevant MOAs in their CPS.

The following table details appropriate compliance audits performed annually by external auditors pertaining to this CP and the CPS.

Table 13 - Required Best-Practices Annual Audits

Audit
Federal Public Key Infrastructure (FPKI) FPKI Annual Review Requirements
WebTrust for Certification Authorities

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

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

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The auditor must demonstrate competence in the field of compliance audits for security and PKIs, and must be thoroughly familiar with requirements that the IdenTrust PMA imposes on the Issuance and management of Certificates Issued under this CP. The compliance auditor must 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 must state the reason for any aperiodic compliance audit.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

For CAs, the compliance auditor must be a private firm that is independent from the entity being audited, or it must 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 must 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 must be considered in the sample. The samples must 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 non-compliant 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 must be performed:

- The compliance auditor must note the discrepancy,
- The compliance auditor must notify the responsible party,
- The responsible party, if not IdenTrust, must immediately notify the IdenTrust PMA of the discrepancy; and
- The party responsible for correcting the discrepancy must 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 must submit an audit compliance package to the Federal PKI Policy Authority. This package must 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 must identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results must be communicated as set forth in Section 8.5 above.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance/ Renewal Fees

CAs and RAs may charge reasonable fees for Certificate Issuance and Certificate renewal in accordance with a fee schedule. The fee schedule is established either by publication or by written agreement between the provider of the service (CA, or the RA) and the consumer of the service.

9.1.2 Certificate Access Fees

Certificate access fees must not be charged for IGC Certificates.

9.1.3 Revocation or Status Information Access Fees

CAs must 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 must maintain reasonable levels of insurance coverage or demonstrate sufficient balance sheet to address all foreseeable liability obligations to entities described in Section *1.3 PKI Participants* of this CP.

9.2.2 Other Assets

CAs and RAs must maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to entities described in Section *1.3 PKI Participants* of this CP.

9.2.3 Insurance or Warranty Coverage for End-Entities

See Section 9.2.1 (above).

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 must keep confidential all such labeled information they receive as part of fulfilling their responsibilities under this CP.

9.3.1 Scope of Confidential Information

The following are considered within the scope of confidential business information:

- All Private Keys,
- Any Activation Data used to access stored Private Keys or to gain access to any CA system component,
- Any business continuity and disaster recovery plans,
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information used by PKI Participants,
- Any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CP),
- Any information held by CAs, an LRA, and TA that is held as private information in accordance with Section 9.4; and
- Any transactional, audit log and archive record identified in Section *5.4 Audit Logging Procedures* or *5.5 Records Archival*.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate Revocation Lists, OCSP Responses, and other publicly available information in the Repository are not considered confidential business information.

9.3.3 Responsibility to Protect Confidential Information

All PKI Participants are responsible for protecting the Confidential Business Information in their possession, custody, or control in accordance with the terms of the agreements entered into between IdenTrust and the FPKI.

9.4 PRIVACY OF PERSONAL INFORMATION

All Subscribers' identifying information as defined by local privacy regulations must be protected from

unauthorized disclosure. Any sensitive information must 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 must be handled as sensitive. Access to this information must be restricted to those with an official need-to-know to perform their responsibilities as defined in this CP, and such information must 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 must be defined in the respective CPS and/or privacy policy.

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

9.4.1 Privacy Plan

IdenTrust must define the plan for protecting private information in the CPS.

9.4.2 Information Treated as Private

IdenTrust must define in the CPS the information that is considered private.

Collection of PII must be limited to the minimum necessary to validate the identity of the Subscriber. This may include attributes that correlate identity evidence to authoritative sources. The RA must provide explicit notice to the Subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing purposes must not be used for any other purpose, unless otherwise permitted by the Subscriber.

9.4.3 Information Not Deemed Private

IdenTrust must define in the CPS the information that is not considered private.

9.4.4 Responsibility to Protect Private Information

IdenTrust must define in the CPS the responsibilities of those individuals and/or other entities responsible for protecting private information.

All information collected as part of the identity proofing process must be protected to ensure confidentiality and integrity. In the event the Entity terminates PKI activities, it must be responsible for disposing of or destroying sensitive information, including PII, in a secure manner, and maintaining its protection from unauthorized access until destruction.

9.4.5 Notice and Consent to Use Private Information

IdenTrust must define in the CPS the parameters for notification and consent to use private information.

9.4.6 Disclosure Pursuant to Judicial / Administrative Process

IdenTrust must define in the CPS the parameters for disclosure of private information pursuant to judicial or administrative requests.

9.4.7 Other Information Disclosure Circumstances

IdenTrust must define in the CPS all other information disclosure circumstances.

9.5 INTELLECTUAL PROPERTY RIGHTS

Neither IdenTrust, nor any Participant CA, nor any RA must 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 must define restrictions of use of the intellectual property within the CPS. A RA'S RPS must define restrictions of use of the intellectual property within the RPS.

A Private Key must 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 Representations and Warranties

CAs must represent and warrant that they must conform to the stipulations of this CP, 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 Representations and Warranties of Affiliated Organizations* and informing the Repository service provider of those obligations if applicable.

CAs must represent and warrant that they must conform to the provisions and stipulations of any applicable MOA and Cross-certification agreements.

For PIV-I Assurance Levels, CAs must 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 Actions Taken as a Result of Deficiency.*

9.6.2 RA Representations and Warranties

An RA must 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 must conform to and comply with the stipulations of this CP, the CA CPS and the RA'S RPS, and must 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, if it has not been Revoked, the Subscriber must 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 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 by 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).

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 Need for Names to Be Meaningful* 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 representations and warranties, Subscribers must 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 may stipulate 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 must 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 must designate an Individual who will perform the role of a Primary Machine Operator and must be responsible for carrying out Applicant and Subscriber duties in relation to the Device Certificate associated with the Device. Such Primary Machine Operator must 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 must sign a Subscribing Organization Authorization Agreement agreeing to the requirements in this Section.

For all end entity Certificate Assurance Levels except for Basic, the Applicant must sign a Subscribing Organization Authorization Agreement agreeing to all applicable requirements in this Section 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 must 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 to rely on such information or not,
- 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 must be avoided.

9.6.5 Representations and Warranties of Affiliated/Organizations

Subscribing Organizations must 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.

9.6.6 Representations and Warranties of Other Participants

9.6.6.1 Repository Representations and Warranties

See Section *2 Publication and Repository Responsibilities*.

9.6.6.2 CSA Obligations

A CSA that provides Revocation status and/or complete validation of Certificates represents and warrants that it must 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 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 Actions Taken as a Result of Deficiency* of this CP.

9.7 DISCLAIMERS OF WARRANTIES

EXCEPT AS EXPRESSLY WARRANTED IN (A) SECTIONS *9.6.1 CA Representations and Warranties* AND *9.6.2 RA Representations and Warranties* 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 NON-INFRINGEMENT WITH REGARD TO ANY CERTIFICATE, REPOSITORY OR CERTIFICATE STATUS SERVICE.

Except as expressly warranted in (a) Sections 9.6.1 and 9.6.2 (noted 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 must be set forth in the applicable agreement(s) between IdenTrust and the Participant CA.

OTHER THAN THE DESCRIBED LIMITATIONS OF LIABILITY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW (ABOVE), 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) must 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 must become effective upon publication in the Repository. This CP as amended from time to time must 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 must survive termination or expiration of this CP:

2.1 Repositories,

2.2 Publication of Certification Information

5.4 Audit Logging Procedures

5.5 Records Archival

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.4 Activation Data

6.5 Computer Security Controls

6.8 Time Stamping

9.11 Individual Notices and Communications with Participants

The provisions below in this Section 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 CPor (b) in an agreement between IdenTrust and the Participant.

9.11.1 Notices by Individual Participants to IdenTrust

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:

- 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
- 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.

9.11.2 Notices by IdenTrust to Individual Participants

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:

- 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 must be deemed effective when sent by IdenTrust; or
- 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.

The method(s) of providing notice between each CA (other than IdenTrust) and Participants (other than IdenTrust) must 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 shall be communicated to policy@IdenTrust.com; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.1 Procedure for Amendment

Updated CP versions are posted on IdenTrust's web site at:

https://www.identrust.com/support/documents/igc-standard.

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 must be set forth in the applicable agreements between the parties.

Provisions for resolving disputes between Participant CAs and other relevant entities must 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., must 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 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 Enforcement (Attorney Fees and 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

9.17.1 Legal Validity of Certificates

9.17.1.1 Waivers

Waivers will not be granted under any level of assurance. Variation in the Issuing CA's practice will either be deemed acceptable under this Policy, or a change will be requested to this Policy, or a new Policy will be established for the non-compliant practice.

9.17.1.2 Issuance

To be legally valid, an IGC Certificate must be issued in accordance with this Policy and any applicable law.

9.17.1.3 Acceptance

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

9.17.1.4 Operational Period

A revoked or expired IGC Certificate may not be used for any purpose. For revoked or expired Certificates, no

action taken by an Authorized Relying Party will be considered valid for purposes of this PKI unless the Authorized Relying Party's Digital Signature verification request is able to confirm that the Digital Signature in question was created during the Operational Period of a valid IGC Certificate. Exceptions to the Private Key Usage period may be permissible if approved by the PMA and so long as such exceptions do not conflict with documented best practices, including RFC 5280.

9.17.1.5 Rules of Repose Allowing Ultimate Termination of Certificate

Unless otherwise specified by the Parties, reliance on an IGC Certificate is no longer enforceable by an Authorized Relying Party against IdenTrust or RA 4 months after termination of the applicable Authorized Relying Party Agreement or 2 years after the Authorized Relying Party’s validation of the TrustID Certificate with IdenTrust's Repository, whichever occurs first.

10 DIRECTORY INTEROPERABILITY PROFILE

10.1 PROTOCOL

Each CA must 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 must be supported.

10.2 AUTHENTICATION

Each CA directory system must permit “none” authentication to read Certificate and CRL information. Each CA must 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., must require password over SSL or stronger authentication mechanism.

10.3 NAMING

When a LDAP Repository is used:

- Certificates must be stored under the directory entry for the Subject Name that appears in the Certificate,
- The issuedByThisCA element of crossCertificatePair must contain the Certificate(s) Issued by a CA whose name the entry represents; and
- All CRLs must 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 must be defined by the organizationalUnit structural object class,
- All CA entries must belong to the pkiCA cpCPS auxiliary object classes,
- Entries that describe Individuals (human entities) must be defined by the inetOrgPerson class, which inherits from other classes: person, and organizationalPerson; and
- These entries must also be a member of pkiUser auxiliary object class.

10.5 ATTRIBUTES

When a LDAP Repository is used:

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

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 must apply to PIV-I Cards:

1. To ensure interoperability with Federal systems, PIV-I Cards must 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 must conform to [NIST SP 800-73-4]. Special attention should be paid to UUID requirements for PIV-I.
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 must contain an asymmetric X.509 Certificate for Card Authentication that:
    a. conforms to [PIV-I Profile],
    b. conforms to [NIST SP 800-73-4]; and
    c. is issued under the PIV-I Card Authentication policy.
6. PIV-I Cards must 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 800-73-4] 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 must not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201].
9. The PIV-I Card physical topography must 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. PIV-I Cards must have an expiration date not to exceed 6 years of issuance.
11. Expiration of the PIV-I Card should not be later than expiration of PIV-I Content Signing Certificate on the card.
12. The digital signature Certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) must contain a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID. The PIV-I Content Signing Certificate must conform to [PIV-I Profile].
13. The PIV-I Content Signing Certificate and corresponding private key must be managed within a trusted CMS as defined by Appendix B.
14. At issuance, the RA must 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 Authentication of Human Subscribers.
15. PIV-I Cards may support card activation by the CMS to support card personalization and post-issuance card update. To activate the card for personalization or update, the CMS must perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73-4]. When cards are personalized, card management keys must be set to be specific to each PIV-I Card. That is, each PIV-I Card must contain a unique card management key. Card management keys must meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal

Identity Verification [SP800-78-4].

APPENDIX B – CARD MANAGEMENT SYSTEM REQUIREMENTS

PIV-I Cards are issued and managed through information systems called CMS. The complexity and use of these trusted systems may vary. Nevertheless, IdenTrust has 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 must be maintained in a FIPS 140-2 Level 2 Cryptographic Module and conform to [NIST SP 800-78-4] requirements. Diversification operations must 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 must require strong authentication of Trusted Roles. Card management must be configured such that only the authorized CMS can manage issued cards.

The PIV-I identity proofing, registration, and issuance process must 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 must be specifically designated to the 4 Trusted Roles defined in Section 5.2.1 Trusted Roles. Trusted Role eligibility and Rules for separation of duties follow the requirements for Medium assurance in 8rsonnel who perform duties with respect to the operation of the CMS must receive comprehensive training. Any significant change to CMS operations must have a training (awareness) plan, and the execution of such plan must be documented.

Audit log files must be generated for all events relating to the security of the CMS must be treated the same as those generated by the CA (see Sections 5.4 Audit Logging Procedures and 5.5 Records Archival).

A formal configuration management methodology must be used for installation and ongoing maintenance of the CMS. Any modifications and upgrades to the CMS must be documented and controlled. There must be a mechanism for detecting unauthorized modification to the CMS.

The CMS must 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 must be revoked, if applicable. The damage caused by the CMS compromise must be assessed and all Subscriber Certificates that may have been compromised must be revoked, and Subscribers must be notified of such revocation. The CMS must be re-established.

All Trusted Roles who operate a CMS must be allowed access only when authenticated using a method commensurate with PIV-I Hardware.

The computer security functions listed below are required for the CMS:

- authenticate the identity of users before permitting access to the system or applications,
- manage privileges of users to limit users to their assigned roles,
- generate and archive audit records for all transactions; (see Section 5.4 Audit Logging Procedures)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

APPENDIX C – IN-PERSON ANTECEDENT

Collection of Identity Data from an Antecedent In-Person Appearance

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

7. Utilize a specialized ID Form designed for TAs to record identity information inclusive of information from an Antecedent In-Person Appearance (if applicable);
8. Record the nature of the ongoing relationship between the Subscribing Organization and the Applicant, i.e., “employee” or “contractor;”
9. Record the date of the Antecedent In-Person Appearance,
10. Record the relationship between the Subscribing Organization and the Applicant,
11. View the Applicant-provided I-9 form and copies of credentials provided,
12. Record the date the I-9 Form was signed by the Applicant as a declaration of identity,
13. Record the required identity credentials as defined in Section 3.2.3.1 Authentication of Human Subscrivers,
14. Record the data to be used by Applicant in response to authentication questions to establish a Subscriber account and complete the application process:
    - Date of Antecedent In-Person Appearance (usually date of hire),
    - Applicant’s date of birth,
    - Applicant’s last 4 digits of Social Security Number,
    - Applicant’s work email address (must be of the same domain as Subscribing Organization),
    - Last name of Applicant’s direct manager,
    - Applicant’s previous employer,
    - Applicant’s home street address; and
    - Applicant’s home phone number (or mobile telephone number if no home telephone number).
15. Sign or Digitally Sign the ID Form and securely transmit the form to the CA or RA for verification.

Verification of Applicant Data from an Antecedent In-Person Identity Proofing

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

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

The Antecedent In-Person Identity Proofing Process requires that the Certificate Validity Period not exceed 12 years from the Antecedent In-Person Appearance date. To ensure that the Validity Period of a Certificate Issued on the basis of an Antecedent In-Person Appearance does not extend beyond the in-person identification limits stated above, the LRA enters the date of the Antecedent In-Person Appearance as the date of registration into the RA System. The RA System then ensures the Validity Period does not exceed 12 years beyond the registration date entered as described in Section 3.3.1. In the event a requested Certificate’s expiration would exceed 12 years from the Antecedent In-Person Appearance, the Applicant is required to undergo new identity proofing.

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

APPENDIX D – REFERENCES

Incorporated by reference from FBCA, and DirectTrust CP documents.

APPENDIX E – ACRONYMS & ABBREVIATIONS

Section 1.6 Definitions and Acronyms.

See Section 1.6.2 Acronyms

APPENDIX F – GLOSSARY

Section 1.6 Definitions and Acronyms

See Section 1.6.1 Definitions