CARIN Credential Policy

v0.1

March 2023

Background

Credential Service Providers (CSPs), and the infrastructure they support, form the basis for one of the primary mechanisms for providing strong assurance of identity in online transactions. The widely placed trust in CSPs is at the heart of security mechanisms used to protect business and financial transactions online. With the advent of a set of technologies such as UDAP™, RFC 8705 enhancements to SAML, OpenID Federation, and identity brokers, non-PKI CSPs can enjoy the benefits federated trust offers while allowing users the flexibility to choose from a number of different types of authenticators. Such a capability has immense potential to enable trust in online communication for the masses.

However, while the technical mechanism of trusting non-PKI CSPs using any federated trust mechanism is deployable immediately, the identity proofing processes, operational controls, and overall trustworthiness of the CSP must be understood by all parties relying on assertions from the CSP. Such a challenge is generally addressed through a Trust Framework where all parties involved in the online transaction subscribe to a set of obligations which enable shared liability that can be ensured throughout the community of participants.

Analyses have revealed that identity-based security breaches were often the result of insufficient security controls being in place on the computer systems & networks at these identity systems, and sometimes exacerbated by weak record keeping.

The purpose of this document is to provide a minimum set of security requirements that Trust Frameworks agree to employ in their respective communities. This document does not make any representations or specify criteria concerning the authorizing of Users in a system. This document only contemplates criteria relevant to resolving, authenticating and proving the identity of Users in a system. Authorization decisions are made at the sole discretion of the Relying Party system.

Reference Credential Policy

This baseline set of controls has been written in the form of a "Credential policy." As defined by RFC 3647: Internet X.509 Public Key Infrastructure Credential Policy and Certification Practices Framework. RFC 3647 was chosen as a common framework containing a set of criteria that generally applies to any CSP, regardless of whether or not the CSP issues Certificates or some other type of identity assertion, such as OAuth/SAMLUDAP assertion. Where sections defined in RFC 3647 do not generically apply to a non-certificate issuing CSP, the criteria will read "no stipulation" as a means of preserving the section numbering of RFC 3647 in this credential policy. In summary, a credential policy, defines the expectations and requirements of the relying party community that will trust the credentials issued and managed by the CSPs they rely on. The governance structure that represents the participants of the Trust Framework is known as the Policy Management Authority. The Policy Management Authority is responsible for identifying the appropriate set of requirements for a given community.

1 Introduction

1.1 Overview

A CSP is a collection of hardware, software, personnel, and operating procedures that issue and manage digital credentials. The credential binds an authenticator to a User. This allows relying parties to trust assertions made by the CSP issuing the assertion on behalf of the User who approved the release of claims contained in the assertion as part of the authentication process.

A fundamental element of modern secure communications is establishing trust in identity credentials. This begins with a Relying Party obtaining an assertion that is issued by a trusted entity (CSP) certifying that the claims in an assertion belongs to a particular user. Assertions are not trusted automatically, but may become trusted through successive validation of a chain of certificates from the CSP Assertion Signing Certificate to a trust anchor (typically a Root-CA public key). Trust anchors are explicitly trusted by Relying Parties. Relying parties are responsible for securely obtaining trust anchors and for securely managing their trust anchor store. Relying parties, should configure trust anchors with great caution and should give full consideration to the requirements the Trust Anchors and downstream certificates comply with and associated compliance annual audit requirements.

1.2 Name and Identification

Level	OID (draft/proposed)	URI (draft/proposed)
IAL2	1.3.6.1.4.1.41179.1.5	
IAL3	1.3.6.1.4.1.41179.1.6	
AAL1	1.3.6.1.4.1.41179.6.5	
AAL2	1.3.6.1.4.1.41179.6.6	
AAL3	1.3.6.1.4.1.41179.6.7	

1.3 Participants

This section identifies roles that are relevant to the administration and operation of CSPs under this policy.

1.3.1 Policy Management Authority (PMA):

A PMA is the entity that decides that a set of requirements are suitable for the trust community that the PMA represents for a given application or use. The Policy Management Authority (PMA):

- Establishes and maintains the Credential Policy (CP).
- Approves the establishment of trust relationships with trust frameworks that offer appropriately comparable assurance.
- Ensures that all aspects of the Trust Framework Polices, operations, and infrastructure as described in the approval process are performed in accordance with the requirements, representations, and warranties of the CP.

All organizations operating a Trust Framework under this policy must establish a PMA-function. The CSP must identify an individual to serve as the liaison for that organization to the Trust Framework.

1.3.2 Trust Framework

Authorities who accredit CSPs that satisfy the requirements defined in this Credential Policy. They act on behalf of the Trust Framework participants, basing their decisions concerning which CSPs to trust on the results of compliance audits and accreditations. A Trust Framework operator sets requirements for recognition of a CSP in their accreditation/certification program. These requirements are based on both security and business needs of the community that the Trust Framework serves. The Trust Framework operator has a duty to enforce compliance with these requirements, for example, requirements around the supply of compliance audit results, on initial accreditation/certification of a CSP, and on an ongoing basis. As specified in Section 5.7, the Trust Framework operator will require the CSP to provide notification of a compromise, and in response, the Trust Framework operator will take appropriate action.

1.3.3 Registration Authorities

The registration authorities (RAs) collect and verify each User's identity and information that is to be entered into the User's CSP system. The RA performs its function in accordance with a Credential Practices Statement (CPS) or Registration Practices Statement (RPS) approved by a participating Trust Framework. The RA is responsible for:

- The registration process
- The identification and authentication (identity proofing) of identity evidence.

Registration Authority Staff: RA Staff are the individuals holding trusted roles that operate and manage RA components.

A CSP carries the responsibilities of an RA by policy, however, a CSP MAY outsource ID proofing to an accredited RA. RAs take on the responsibilities of IAL as defined in NIST 800-63-3.

1.3.4 Credential Service Provider (CSP)

The CSP is the collection of hardware, software and operating personnel that create, sign, and issue credentials to Users. The credentials issued by the CSP are only issued to natural persons, not roles. The CSP is responsible for issuing and managing credentials including:

- Identity proofing
- Binding authenticators to a User's account and authenticating Users
- Approving the issuance of all credentials
- Maintenance of active web services in support of CSP discovery
- Revocation of credentials
- Signing assertions of identity containing verified claims about the CSP's Users
- Generation and destruction of assertion signing keys
- Establishing and maintaining the CSP system
- Establishing and maintaining the Credential Practices Statement (CPS)

A CSP carries the responsibilities of an RA by policy, however, a CSP MAY outsource ID proofing to an accredited RA. CSPs take on the responsibilities defined in NIST 800-63-3 for IAL, AAL and FAL.

When meeting these requirements, "IdP" may be another term used to describe this participant.

1.3.5 User Client App

A User Client App is an application making protected resource requests on behalf of the User and with the User's authorization. The term "client" does not imply any particular implementation characteristics (e.g., whether the application executes on a server, a desktop, or other devices). The User Client App may share information with a Data Holder to support the discovery of the User's CSP via UDAP tiered OAuth in order to obtain trustworthy claims about the User, or employ other mechanisms.

User Client Apps that take on the responsibilities of authenticating Users and attesting to authenticated Users' identities, effectively take on the role and responsibilities of a CSP as defined by this policy.

1.3.6 User

A User is the natural person who has been:

- Identity proofed by the CSP;
- Issued an authenticator bound to the User's account;
- Is represented in the assertions signed by the CSP, and;
- Consents to the CSP sharing the User's data with other parties.

User is analogous to the term Subscriber in NIST 800-63-3 as defined by this policy.

1.3.7 Relying Parties

A Relying Party is an entity that relies on the validity of the binding of the User's identity attributes to an assertion signed by a CSP. The Relying Party uses a CSP's signed assertion to verify or establish the identity and status of the User. A Relying Party is responsible for deciding whether or how to check the validity of the assertion and the mechanisms used to verify the origin and trust of the data contained in an assertion from a CSP. A Relying Party may use information in a certificate to determine the suitability of an assertion for a particular use. Relying parties may be User Client Apps, Data Holders or other participants that require the ability to discern trustworthiness of identity claims contained in an assertion of identity.

Relying Parties should also be policy aware to ensure the assurance level defined in the assertion does not exceed the maximum level of assurance granted by a Trust Framework to the CSP, thereby ensuring the level of assurance at which a user has been authenticated is commensurate with the risk assumed by the Relying Party. The responsibility to make authorization and access control decisions lies solely with the Relying Party.

1.3.7.1 Clients to CSPs

Entities that are servers relying on federated identity embody the role of client to the CSP. User Client Apps may also be capable of interfacing with CSPs as per UDAP Dynamic Client Registration (when Servers relying on federated identity embody the role of client to the CSP) and UDAP Tiered OAuth.

1.3.8 Trusted Roles

CSP components are operated and managed by individuals holding trusted, sensitive roles. Specific responsibilities for these roles, as well as requirements for separation of duties, are described in Section 5.2 for all CSP Trusted Roles.

1.3.9 Trusted Agents

Also known as a Trusted Referees, Trusted Agents performs identity proofing as a proxy for the RA. The trusted agent records information from and verifies biometrics (e.g., fingerprints, photographs) on presented credentials for an applicant's identity on behalf of the RA. The CPS shall identify the parties responsible for providing such services, and the mechanisms for determining their trustworthiness. This policy assumes the trusted agent has some preexisting relationship with the Users they onboard (work for the same employer, notary, etc.)

1.3.10 Data Holder

A Data Holder is a type of Relying Party that possesses or manages data about Users and makes risk-based decisions concerning the release of the User's data. User's data is released when requested by an authenticated and authorized requestor. Data Holders are responsible for properly matching the User's identity to records that the Data Holder possesses.

1.4 Credential Usage

1.4.1 Appropriate Credential Uses

The credentials issued by CSPs defined in this policy are used for the purposes of authenticating Users. Credentials issued by CSPs defined in this policy may be used to carry an intent to execute a signature or encrypt data with a key that is associated with the user under certain conditions defined by this policy. The table below depicts the various aspects that make up a credential and each aspect's respective purpose. An X.509 Certificate Features column is added for context and illustrative purposes only. This documents principal focus is on Non-PKI credentials.

Attributes of a Credential	X.509 Certificate Features	Non-PKI Credential
Authenticator *How does the User prove who they claim to be?*	Public/Private Key Pair	OTP, FIDO, Biometrics, Password, etc..
User Attributes *Who does the User claim to be?*	Subject: CN = John Doe - ID SERIALNUMBER = 87000002728 OU = Example Healthcare Org OU = Users O = Example CA inc. C = CA Subject Alt Name: RFC822 Name=John.Doe@directtrust.org Other attributes May include an identifier	OpenID Connect: "iss": “s6BhdRkqt3” "sub": {same as in ID Token} "given_name": "John" "family_name": "Doe" ...more claims… Other attributes May include a universal identifier

Assertion of Legitimacy *How can external parties Trust that the User is who they claim to be?*	Signature of certificate Issuer: CN = Carillon PKI Services CA 3 OU = Certification Authorities O = Carillon Information Security Inc. C = CA Other details Assurance level expiration Trust Chain	CSP UDAP metadata: https://idp.example.com/optionalpath/.well-known/udap Signed token by Trusted CSP: code=authz_code_from_idp Other details Assurance level expiration Federation Trust Chain

1.4.2 Prohibited Credential Uses

No stipulation.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The Policy Authority is responsible for all aspects of this CP.

1.5.2 Contact Person

Ryan Howells <ryan.howells@leavittpartners.com>.

1.5.3 Person Determining CPS Suitability for the Policy

The Policy Authority shall approve the CPS for each CSP that issues Credentials under the policy.

1.5.4 CPS Approval Procedures

CSPs issuing under the policy are required to be evaluated against all facets of the policy by Trust Frameworks that evaluate conformance against this policy. The Policy Authority shall work with a CSP to minimize the use of waivers.

The Policy Authority shall make the determination that a CPS complies with the policy. The CSP and RA must meet all requirements of an approved CPS before commencing operations. The Policy Authority will make this determination based on the nature of the system function, the type of communications, or the operating environment.

In each case, the determination of suitability shall be based on an independent compliance auditor's results and recommendations. See section 8 for further details.

1.6 Definitions and Acronyms

See Appendices A and B.

2 Publication and Repository Responsibilities

2.1 CSP Endpoints

All CSPs that issue credentials under this policy can be discovered through a public facing endpoint(s) in order to communicate authenticated user's claims for validation by relying parties. To promote consistent access to the endpoint service, the service shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

2.2 Publication of CSP Information

2.2.1 Availability of CSP Endpoints

The publicly accessible CSP endpoints shall be designed and implemented to comply with the availability requirements stipulated in section 6.7.3.

2.2.2 Publication of CSP Information

The CSP's Credential Policy (CP) shall be publicly available.

2.3 Time or Frequency of Publication

Updates to the CP shall be publicly available within 30 days of ratification.

An updated version of the CP will be made publicly available within fifteen days of the incorporation of changes. All information to be communicated by the CSP service shall be made accessible after such information becomes available to the CSP. The CSP shall specify in its CPS time limits within which it will publish various types of information.

2.4 Access Controls on Repositories

The CSP shall protect information not intended for public dissemination or modification. CSP Certificates at the Server Metadata endpoint shall be publicly available through an HTTPS interface following the UDAP protocol, if supported. The CPS shall detail what information at the endpoint shall be exempt from automatic availability and to whom, and under what conditions the restricted information may be made available.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Standard claims from OpenID Connect (OIDC) Core Section 5.1 shall be supported by CSPs, but may not be populated in all cases. Additional claims defined by the HL7 Security IG may also be supported by CSPs to carry additional identifying information defined in section 3.1.5.

3.1.2 Need for Names to Be Meaningful

Although the Subject identifier issued by an CSP is not intended to be human-readable, the claims associated with Subject shall be meaningful enough for a human to identify the named User. Interpreting

the name semantic may require a reference database (e.g., human resources directory or inventory catalog) external to the CSP.

While the issuer name in CSP assertions is not generally interpreted by relying parties, this CP still requires use of meaningful names by CSPs issuing credentials under this policy.

Since OIDC Core requires the issuer parameter to be a URL identifying the CSP, the subject alternative name in CSP certificates, if used, must contain a uniformResourceIdentifier entry that matches the issuer URL in CSP assertions issued by the CSP.

3.1.3 Anonymity or Pseudonymity of Users

The CSP shall not issue anonymous assertions. Pseudonymous assertions, if issued shall be identified as such. CSPs issuing pseudonymous assertions shall maintain a mapping of identity to pseudonym.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting claims are specified in OIDC Core.

3.1.5 Uniqueness of Names

From OIDC Section 8: A Subject Identifier is a locally unique and never reassigned identifier within the Issuer for the User, which is intended to be consumed by the Relying Party.

Each CSP must ensure that each of its users is identifiable by a unique name. When other name forms are used, they too must be allocated such that each name identifies only one user of that CSP. Name uniqueness is not violated when multiple assertions are issued to the same entity.

In order to increase identity resolution rates among relying parties, CSPs shall collect and validate identifiers about identity proofed Users that can be used to uniquely identify the User in an external system. Those identifiers may include a driver's license number, passport number, email address, phone number and other attributes that may help uniquely identify the User.

The CPS shall identify the method for the assignment of unique User identifiers.

3.1.6 Recognition, Authentication, and Role of Trademarks

CSPs operating under this policy shall not issue an assertion knowing that it infringes on the trademark of another. The Trust Framework shall resolve disputes involving names and trademarks.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Authenticator (Authenticator Assurance Levels)

For certificates issued to CSPs:

Refer to the respective Trust Framework Certificate Policy that governs the assertion signing certificate employed by the CSP.

For Users' authenticators:

Users must demonstrate the ability to authenticate themselves using the authenticator(s) at the Authenticator Assurance Level (AAL) intended for the User. CSPs shall bind authenticators to User's accounts that at least meet the requirements of AAL2 or higher when identity proofed at IAL2 or lower and meet the requirements of AAL3 if the User is identity proofed at IAL3.

In all cases, CSPs shall bind at least one physical (something you have) authenticator to the User's account and one authenticator that is replay resistant. One authenticator may satisfy both of these requirements. CSPs shall not sign an assertion or expose personal information associated with the User's account unless the account is activated at the AAL associated with the account.

Practice Note: If the User was ID proofed at IAL2, the User must be bound to the authenticator combinations found under the AAL2 row in the table below. For example, if the User only authenticates to the CSP at AAL1, PII associated with the User's account shall not be exposed by the CSP to the User until they have fully authenticated at AAL2.

All assurance levels with an (*) intends to be consistent with the authenticator assurance levels defined in NIST 800-63-3.

AAL	Acceptable Authenticators and/or Combinations
AAL1*	Memorized Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device
AAL2*	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: Look-Up Secret; Out-of-Band; SF OTP Device; SF Crypto Software; SF Crypto Device;
AAL3*	MF Crypto Device; SF Crypto Device plus Memorized Secret; MF OTP (software or hardware) plus SF Crypto Device; MF OTP Device hardware plus SF Crypto software. SF OTP hardware Device plus MF Crypto software; SF OTP hardware Device plus SF Crypto Software plus Memorized Secret

3.2.2 Authentication of Organization Identity

Requests for CSP Assertion Signing Certificates shall include the CSP organization name, street address, and documentation of the existence of the CSP. CSPs shall be issued certificates from Certificate Authorities (CA) that have been accredited by a Trust Framework to issue assertion signing certificates. Before issuing CSP assertion signing certificates, the CA shall verify the information included in the request, in addition to the identity of the requesting representative and the representative's authorization to act in the name of the CSP as stipulated by the Trust Framework Certificate Policy and section 3.2.5. The CA must also verify the CSP's certification status and that their approved assurance levels are currently in good standing with a Trust Framework conformant with this CP as a condition to issuing a

trusted assertion signing certificate which contains the assurance levels under which the subscribing CSP is approved to sign assertions as indicated in section 1.2.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Human Authorized Representatives and Users

The issuance of CSP assertion signing certificates requires identity proofing the individual authorized to represent the CSP at IAL2 and observe the requirements stipulated in section 3.2.5.

The Registration Authority (RA) shall ensure that the User's identity information is verified. Identity shall be verified no more than <30> days before initial credential issuance. Authentication by a trusted agent or notary does not relieve the RA of its responsibility to perform steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of records in step 4), below.

At a minimum, authentication procedures for individuals as required above must include the following steps:

1) Verify that a request for credential issuance to the applicant was submitted by the organization, if applicable.
2) Verify the individual's organizational membership, if applicable.
3) Establish the individual's identity by ID proofing before the registration authority, based on the following process:
   a) Individual presents an official form of identification (e.g., a passport, or driver's license) as proof of identity
   b) The RA examines the presented credential that can be linked to the individual (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and
   c) The credential presented above shall be verified by the RA for currency and legitimacy (e.g., the organization ID is verified as valid).
   d) ensure the ID proofing session occurs over an authenticated channel when in-person proofing is not employed
4) Verify information to be included in the credential profile (e.g., e-mail address, mobile phone number etc…).
5) Record and maintain records of the applicant by the RA or CSP. This information is archived to help establish an audit trail for dispute resolution.

The RA shall ensure the following criteria is met for the assurance level of credential being issued to the user:

All assurance levels with an (*) intend to be consistent with the identity assurance levels defined in NIST 800-63-3.

User Identity Proofing at IAL2*
Applicant supplies his or her full legal name, an address of record and date of birth for their claimed identity.

In-Person Vetting

Acceptable Evidence:

As evidence of their claimed identity, the Applicant provides:

- US Passport, OR
- REALID driver's license/REALID ID card, OR
- Enhanced driver's license/Enhanced ID card, OR
- Other acceptable evidence as described in the "Guidance for Authentication of Individual Identity."

Validation:

Evidence presented by the Applicant SHALL be confirmed as genuine by trained RA personnel and/or appropriate technologies including the integrity of any physical and cryptographic security features. All evidence and personal details from the evidence SHALL be confirmed as valid by comparison with information held or published by the issuing or authoritative sources and are consistent with the full legal name, address of record and date of birth of the claimed identity. The information printed on the physical evidence listed above is deemed information published by the issuing source.

Verification

The Applicant's ownership of the claimed identity is confirmed by physical comparison to the photograph or biometrics of the Applicant to the strongest piece of identity evidence provided to support the claimed identity. Additional requirements on the verification of biometrics is provided in the "Guidance for Authentication of Individual Identity".

The CSP issues credentials to the Applicant in a manner that confirms the address associated with the Applicant in the records.

CSP issues Credential or other credential and delivers it in a secure manner to the appropriate User.

Remote Vetting (unsupervised)

Acceptable Evidence:

As evidence of their claimed identity, the Applicant provides:

- US Passport, OR
- REALID driver's license / REALID ID card, OR
- Enhanced driver's license / Enhanced ID card, OR
- Other acceptable evidence as described in the "Guidance for Authentication of Individual Identity."

Validation:

Evidence presented by the Applicant SHALL be confirmed as genuine by trained RA personnel and/or appropriate technologies including the integrity of any physical and cryptographic security features. All evidence and personal details from the evidence SHALL be confirmed as valid by comparison with information held or published by the issuing or authoritative sources and are consistent with the full legal name, address of record and date of birth of the claimed identity. The information printed on the physical evidence listed above is deemed information published by the issuing source.

Verification:

The Applicant's ownership of the claimed identity is confirmed by physical comparison to the photograph or biometrics of the Applicant to the strongest piece of identity evidence provided to support the claimed identity. Additional requirements on the remote verification of biometrics or photograph is provided in the "Guidance for Authentication of Individual Identity."

The CSP sends an enrollment code, with at least six random alphanumeric characters, to a postal address (preferred), mobile telephone (SMS or voice), landline telephone or email that has been validated in records. Depending on the method sent, the enrollment code will remain valid for a maximum duration as follows:

- Postal address – 10 days
- Postal address outside of contiguous United States – 30 days
- Telephone – 10 minutes
- Email – 24 hours

Upon receipt of the valid enrollment code, the CSP issues the Credential and and binds authenticators to the User in a manner conformant to section 6.1.2. The CSP shall deliver a notification of proofing to a confirmed address of record, different from the destination address of record for the enrollment code unless that destination was a postal address.

User Identity Proofing at IAL3*
Applicant supplies his or her full legal name, an address of record and date of birth of their claimed identity.

In-Person Vetting Acceptable Evidence:

As evidence of their claimed identity, the Applicant provides evidence aligned with Identity Assurance Level 3 requirements as described in the "Guidance for Authentication of Individual Identity."

Validation:

Evidence presented by the Applicant SHALL be confirmed as genuine by trained RA personnel and/or appropriate technologies including the integrity of any physical and cryptographic security features. All evidence and personal details from the evidence SHALL be confirmed as valid by comparison with information held or published by the issuing or authoritative sources and are consistent with the full legal name, address of record and date of birth of the claimed identity. The information printed on the physical evidence listed above is deemed information published by the issuing source.

Verification:

The Applicant's ownership of the claimed identity is confirmed by physical comparison to the biometrics of the Applicant to the strongest piece of identity evidence provided to support the claimed identity. Additional requirements on the collection and verification of biometrics is provided in the "Guidance for Authentication of Individual Identity".

The CSP issues credentials to the Applicant in a manner that confirms the address associated with the Applicant in the records and a notification of proofing is sent to the confirmed address of record.

CSP issues credentials and binds authenticators to the User in a manner conformant to section 6.1.2.

Remote Vetting

Remote Vetting is not permitted unless employing a product that is certified to support the supervised remote identity proofing requirements defined in NIST SP 800-63A and further defined in FIPS 201-3.

3.2.3.2 Authentication of CSPs

An Authorized Organizational Representative (AOR), must provide identifying information for the CSP. The AOR is responsible for providing registration information which may include:

- Fully Qualified Domain Name (FQDN)
- legal name of the CSP
- URI that unique identifies the CSP under this policy
- Evidence of an accreditation by a recognized Trust Framework in good standing, which included the assurance levels that the CSP is accredited to issue.
- Equipment Credential signing request CSR

The registration information provided by the AOR/device shall be verified. If the information is provided by an AOR for a single CSP, the AOR shall be authenticated.

3.2.4 Non-verified User Information

Information that is not verified shall not be included in assertions.

3.2.5 Validation of Authority

Before issuing CSP assertion signing certificates that assert organizational authority, the CSP shall validate the AOR's authority to act in the name of the organization.

For User's seeking credentials that specify an affiliation with an organization, the CSP shall verify the existence of the organization by verifying the legal existence documentation and address of the organization, and that the address is the subscribing CSP's address of existence or operation. The CSP shall identify and identity proof at IAL2, an Authorized Organization Representative to verify the User's affiliation with the organization.

Individual Users intending to assert their own identity without affiliation with an organization do not require any authorization to obtain a credential from a CSP.

3.2.6 Criteria for Interoperation

CSPs shall conform to the stipulations of this policy to achieve interoperability with special attention paid to sections 2, 7 and 10, which substantially focus on interoperability between systems.

3.3 Identification and Authentication for Renewal

3.3.1 Identification and Authentication for Renewal

For renewal of any User Credential issued under this credential policy, identity may be established through use of current and unrevoked authenticators that meet the intended AAL of the User. If the User cannot authenticate at the AAL intended for the User's account, the User shall be required to be identity proofed per section 3.2.3.

3.3.2 Identification and Authentication for Renewal after Revocation

In the event of credential revocation, issuance of a new credential shall always require that the party go through the initial registration process per Section 3.2.3 above.

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated.

4 Credential Life-Cycle Operational Requirements

4.1 Credential Application

The credential application process must provide sufficient information to:

- Establish the applicant's authorization (by the employing or sponsoring organization if applicable) to obtain a credential. (per Section 3.2.5).
- Establish and record identity of the applicant. (per Section 3.2.3)
- The CSP shall bind the applicant to an authenticator commensurate with the level of assurance being requested by the applicant in a way that proves that User's possession of the authenticator (per section 3.2.1 and section 6.1.2).
- Verify any role or authorization information requested for inclusion in the assertion used to represent the User (per section 3.2.5).

These steps may be performed in any order that is convenient for the CSP and Users in a way that does not compromise security. All steps must be completed before the first assertion representing the user is signed by the CSP.

4.1.1 Who Can Submit a Credential Application

A credential application shall be submitted to the CSP by the User, AOR, or an RA on behalf of the User. Multiple credential requests from one RA or AOR may be submitted as a batch.

4.1.2 Enrollment Process and Responsibilities

All communications among Authorities supporting the credential application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band.

For CSP credentials, where electronic communications are used, cryptographic mechanisms commensurate with the strength of the authenticator shall be used. When information traverses the public internet, communications for provisioning CSP issued credentials between Authorities shall be protected at a level commensurate with the highest level of assurance credentials being managed. Out-of-band communications shall protect the confidentiality and integrity of the data.

Users are responsible for providing accurate information on their credential applications as further defined in section 9.6.3.

4.2 Credential Application Processing

Information in credential applications must be verified as accurate before credentials are issued. Procedures to verify information in credential applications shall be specified in the CPS.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the User shall meet the requirements specified for User authentication as specified in Sections 3.2 and 3.3. The participants (e.g., CSP or RA) that are responsible for authenticating the User's (or if required, AOR) identity in each case shall be identified in the CPS.

4.2.2 Approval or Rejection of Credential Applications

Any credential application that is received by a CSP under this policy, for which the identity and authorization of the applicant has been validated, will be duly processed. However, the CSP shall reject any application for which such validation cannot be completed, or when the CSP has cause to lack confidence in the application or certification process.

4.2.3 Time to Process Credential Applications

Credential applications must be processed and a credential issued within 30 days of identity verification.

4.3 Credential Binding

4.3.1 Actions during Credential Binding

Upon receiving the request, the CSPs/RAs shall:

- Verify the identity of the requester as specified in Section 3.2.
- Verify the authority of the requester and the integrity of the information in the credential request as specified in Section 4.1.
- Verify the User's possession of the authenticator as defined in section 3.2.1 and 6.1.2.
- Bind authenticators to the User's account if all credential requirements have been met as defined in section 6.1.2.
- Make the credential available to the User after confirming that the User has formally acknowledged their obligations (e.g. click through agreement including their typed name or digitally signed equivalent) in a secure manner as described in Section 9.6.3. An example of making the credential available to the User may involve prompting the user to authenticate to the CSP if such action isn't carried out in a previous step.

All authorization and other attribute information received from a prospective User shall be verified before inclusion in a credential or associating attributes bound to a credential. The responsibility for verifying prospective User data shall be described in the CPS.

CSPs shall observe credential binding requirements defined in section 6.1.2 when initially binding authenticators to User's accounts as part of enrollment.

4.3.2 Notification to User by the CSP of Issuance of a Credential

CSPs operating under this policy shall inform the User (or other subject) of the creation of a credential and make the credential available for use by the User. The CSP shall also notify the User of the retention policy of the CSP audit archive period defined in section 5.5.2. CSPs shall notify Users of the risks of using authenticators that are considered "restricted" by NIST SP 800-63B and provide a migration path for Users to take advantage of at their discretion until the authenticator is disallowed by the CSP or this policy as stipulated in section 4.8.1. CSPs shall inform users about the data being collected by the CSP, the reason for collection, and the consequences for withholding information during the identity proofing process to help Users make informed decisions about their privacy.

4.4 Credential Acceptance

Before a User can make effective use of their credential, the CSP shall explain to the User their responsibilities, and the CSP's responsibilities to protect the User's data and obtain the User's acknowledgement, as defined in Section 9.6.3.

4.4.1 Conduct Constituting Credential Acceptance

Failure to object to the credential or its contents shall constitute acceptance of the credential, however the CSP shall make a reasonable effort to obtain the Users acceptance of the credential.

4.4.2 Publication of the Credential by the CSP

As specified in Section 2.1, all CSP issued credentials shall be accessible by relying parties in repositories.

When applicable, CSPs shall publish metadata to facilitate CSP certificate discovery as per UDAP Tiered OAuth.

4.4.3 Notification of Credential Issuance by the CSP to Other Entities

No stipulation.

4.5 Key Pair and CSP Credential Usage

4.5.1 CSP Private Key and Certificate Usage

The intended scope of usage for a CSP private key shall be specified through the policy OIDs contained in the Certificate Policies extension, as well as the key usage and extended key usage extensions, in the CSP assertion signing certificate.

4.5.2 Relying Party Public Key and Credential Usage

CSP assertion signing certificates may specify restrictions on use through critical identifiers contained in the certificate signed by a CA operating under a recognized PKI Trust Framework Certificate Policy as defined in section 1.2. The identity assurance OIDs present in an assertion that is signed by a CSP and consumed by a relying party shall also be reflected in the CSP's assertion signing certificate. It is recommended that relying parties process and comply with this information whenever using credentials in a transaction.

4.6 Credential Renewal

Authenticators bound to Users shall be cycled in an effort to preserve cryptographic strength of the authenticator. This may include generating new key pairs, random values or shared secrets. Authenticator strength and life spans are defined in section 6.3.2.

4.6.1 Circumstance for Credential Renewal

Authenticators may need to be re-bound to Users for various reasons including:

- Loss of authenticator by User
- Authenticator's cryptographic material reached the end of its lifespan
- Authenticator type is no longer supported by the CSP

4.6.2 Who May Request Renewal

A User, RA, or AOR may request the renewal of a User credential.

4.6.3 Processing Credential Renewal Requests

User renewal requests shall be properly authenticated and validated before electronic renewal requests are processed per Section 3.3. Alternatively, User renewal requests may be processed using the same process used for initial credential issuance.

4.6.4 Notification of New Credential Issuance to User

The CSP shall inform the User of the renewal of the User credential.

4.6.5 Conduct Constituting Acceptance of a Renewal Credential

Failure to object to the renewal of the credential or its contents within 7 days of notification by the CSP or usage by the User constitutes acceptance of the credential.

4.6.6 Publication of the Renewal Credential by the CSP

As specified in Section 2.1, all CSP issued credentials shall be accessible at endpoints as stipulated in section 2.

Publication of renewed User credentials at an appropriate endpoint is subject to the requirements in Section 2 and Section 9.4.3 of this policy.

4.6.7 Notification of Credential Issuance by the CSP to Other Entities

This CP makes no stipulations for this section.

4.7 Credential Re-key

No Stipulation

4.8 Credential Modification

4.8.1 Circumstance for Credential Modification

CSP may perform credential modification for a User whose characteristics have changed (e.g., name change due to marriage). A credential may also be modified if the User or CSP wishes to update the Authenticator(s) bound to the User. If the User's name has changed, the User shall undergo the initial registration process.

There are many reasons a credential may be modified including the following:

- User wishes to bind additional authenticators of equal strength to their account
- User may have obtained a new or different mobile device
- User wishes to replace an existing authenticator with a new authenticator of equal strength to their account.
- User's identifying information has changed.
- Compromised authenticator (e.g. memorized secret)
- One or more of User's authenticators is classified as restricted, or risky, thereby justifying a migration from one authenticator to another. In such circumstances, CSPs shall document a migration plan for migrating users from risky authenticators in the CSP's CPS.

4.8.2 Who May Request Credential Modification

Requests for credential modification shall be considered as follows:

- Users with a currently valid credential may request credential modification.
- CSPs and RAs may request credential modification on behalf of a User.

4.8.3 Processing Credential Modification Requests

A credential modification shall be achieved using one of the following processes:

Initial registration process as described in Section 3.2

The validation of the changed subject information shall be in accordance with the initial identity-proofing process as described in Section 3.2. The RA shall complete all required re-verification prior to issuing the modified credential. User's shall be required to authenticate to their account at the highest AAL associated with the account in order to bind additional authenticators to the account. For example, if the User's target AAL is AAL2, the User shall be required to perform an AAL2 authentication event in order to bind additional authenticators to the User's account.

If a User loses all authenticators for a factor or cannot authenticate their account at the AAL originally established for their account, the User shall be required to perform the initial registration process as described in section 3.2. Following the initial registration process, the User shall be required to either authenticate or re-bind their previous (not lost) authenticator(s) to their account to confirm continuity of binding.

As an alternative to the above re-proofing process, the CSP may bind a new memorized secret authenticator in conformance with section 6.5.1.1.5, using two physical authenticators (the same factor), along with a confirmation code that has been sent to one of the subscriber's addresses of record. If this process is used, the confirmation code shall conform to the requirements defined in section 6.1.5 for strength and section 6.3.2 for operational period.

When binding additional authenticators to the account, the CSP shall observe the stipulations of this policy to ensure the authenticator meets the requirements of the AAL intended for the User.

4.8.4 Notification of Modified Credential Issuance to User

The CSP shall inform the User of any modification of the User's credential.

4.8.5 Conduct Constituting Acceptance of Modified Credential

Failure to object to the credential or its contents constitutes acceptance of the credential.

Failure to object to the modification of the credential or the metadata associated with the credential within 7 days of notification by the CSP or usage by the User constitutes acceptance of the credential.

4.8.6 Publication of the Modified Credential by the CSP or CSP

All CSP issued credentials must be accessible in repositories as specified in section 2.

Publication of modified User credentials is subject to the requirements in Section 2 and Section 9.4.3 of this policy.

4.8.7 Notification of Credential Issuance by the CSP to Other Entities

No stipulation

4.9 Credential Revocation and Suspension

CSPs operating under this policy shall fail to sign an identity assertion for Users with revoked or suspended credentials. A notice of revocation functionality shall be given to Users during credential request or issuance, and shall be readily available to any potential relying party.

Revocation requests must be authenticated. See Section 3.4 for more details.

4.9.1 Circumstances for Revocation

A credential must be revoked when the binding between the User and the User's authenticator or identifying information defined within a credential 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 credential becomes invalid.

- Subject can be shown to have violated the stipulations of its respective User, Issuer or Member Agreement, or the stipulations of its governing CP;
- The authenticator is compromised or is suspected of compromise.
- The User can be shown to have violated the stipulations of its User agreement.
- Certification of the User is no longer in the interest of the CSP
- The original credential request was not authorized.
- The User or other authorized party (as defined in the CPS) asks for his/her credential to be revoked.
- If the CSP receives a legal instrument from a competent court to revoke the User's account.

If a credential used to approve requests for one or more User's credentials has been compromised, all credentials authorized since the date of actual or suspected compromise must be revoked or verified as appropriately issued. A CSP may elect to perform a credential modification rather than revoke a User's account if done so within the timeframe stipulated in 4.9.5.

4.9.2 Who Can Request Revocation

A CSP may summarily revoke credentials they have issued at their discretion.

A User or legally authorized representative of a User may request revocation of a credential.

A written notice and brief explanation for the revocation should subsequently be provided to the User. The RA can request the revocation of a User's credential on behalf of any authorized party as specified in the CPS.

4.9.3 Procedure for Revocation Request

A request to revoke a credential must explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed, email from verified address). The CSP or RA must authenticate the request as well as the authorization of the requester per Section 4.9.2.

If an RA performs this function on behalf of the CSP, the RA must send a message to the CSP requesting revocation of the certificate. The RA must digitally or manually sign the message. The message must be in a format known to the CSP.

A User ceasing its relationship with a CSP is required to provide evidence of certified destruction or surrender all authenticators that were provided to the User by the CSP, prior to departure unless otherwise stipulated in writing by the CSP.

A User is considered revoked when all of the authenticators bound to the User's account are disabled, and the CSP is prevented (either procedurally or technically) from creating assertions of identity concerning the revoked User for use by a Relying Party.

A CSP may revoke (un-bind) an authenticator associated with a User's account if the CSP receives evidence that the authenticator has been compromised. The User may re-bind the authenticator with their account following the process defined in section 4.8.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this policy. Users and other participants shall request the revocation of a credential as soon as the need for revocation comes to their attention.

4.9.5 Time within which CSP must Process the Revocation Request

CSPs shall revoke credentials as quickly as practical upon receipt of an authenticated revocation request and after the requested revocation time. Revocation requests shall be processed within 22 hours of receiving an authenticated request.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

No stipulation.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-line Revocation/Status Checking Availability

No stipulation.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

In the event of CSP private assertion signing key compromise, the CSP shall publish a notice on their website in a highly visible fashion as well as information about the event and steps that are being taken to remediate. A reasonable effort should be carried out to inform relying parties of the compromise as a means of limiting impact.

4.9.12 Special Requirements Related To Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

Credential suspension is a temporary form of credential revocation. Credential suspension occurs by marking a credential as revoked within the CSP system. These credentials shall remain suspended until the credential is restored or the credential expires. A credential is restored when the CSP reinstates the User's account. CSPs are not required to support suspended credentials, but MAY opt to do so.

Authenticators associated with a User's account may be suspended by the CSP if the CSP receives evidence of compromise. An Authenticator may be reversible if the User authenticates to the account at the highest AAL associated with the account and requests re-activation of the authenticator. The CSP shall require the User to authenticate with the authenticator immediately after reversal to prove possession and proper function of the authenticator.

4.10 End Of Subscription

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

4.11 Key Escrow and Recovery

Credentials used for authentication shall not be escrowed.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

All CSP and RA equipment, including cryptographic modules, shall be protected from theft, loss, and unauthorized access at all times. Unauthorized use of the CSP and RA equipment is prohibited. CSP equipment shall be dedicated to performing CSP functions. RA equipment shall be operated to ensure that the equipment meets all physical controls at all times.

5.1.1 Site Location and Construction

The location and construction of the facility housing the CSP equipment, as well as sites housing remote workstations used to administer these components, must have protections that are consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, must provide robust protection against unauthorized access to the CSP equipment and records.

CSPs and CSPs must be certified by a third party assessor against an industry accepted cybersecurity framework (e.g. EHNAC, HITRUST, SOCII, PCI or FedRAMP/FISMA, etc…)

5.1.2 Physical Access

5.1.2.1 Physical Access for CSP and CSP Equipment

Physical access to CSP equipment shall be limited to CSP Operations Staff and Audit Administrators. The security mechanisms shall be commensurate with the level of threat in the equipment environment. Output devices shall be housed in a location that prevents unauthorized disclosure of sensitive information.

At a minimum, physical access controls for CSP equipment and all copies of the CSP cryptographic module shall meet the following requirements:

- Ensure that no unauthorized access to the hardware and physical communication lines is permitted
- Be manually or electronically monitored for unauthorized intrusion at all times, ensure an access log is maintained and available for inspection.
- Individuals other than Trusted Roles or designated facility maintenance staff in the event of an emergency shall be escorted. All individuals shall be recorded in the access log. [KN1]
- Upon the permanent departure of trusted personnel, ensure access to sensitive physical areas is denied.

When not in use, removable CSP cryptographic modules, removable media, and any activation information necessary to access or enable CSP cryptographic modules CSP equipment, or paper containing sensitive plain-text information shall be placed in locked containers sufficient for housing equipment and information commensurate with the sensitivity of the application being protected. Access to the contents of the locked containers shall be restricted to individuals holding CSP trusted roles as defined in Section 5.2.1.

Knowledge of the combination or access to the key used to secure the lock shall be restricted to authorized individuals only. When in active use, the cryptographic module shall be locked into the

system or container (rack, reader, server, etc.) using a physical lock under the control of the CSP Operations Staff to prevent unauthorized removal.

Any activation information used to access or enable the cryptographic modules or CSP equipment shall be stored separately from the associated modules and equipment. Such information shall either be memorized or recorded and stored in a manner commensurate with the security afforded by the associated cryptographic module or equipment.

A security check of the room/rack housing CSP equipment shall occur prior to leaving the room/rack unattended by the CSP Operations Staff. The check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed")
- Any security containers are properly secured
- Physical security systems (e.g., door locks, alarms, vent covers) are functioning properly
- The area is secured against unauthorized access

If unattended, the facility housing CSP equipment shall be protected by an intrusion detection system (IDS).

If a facility is not continuously attended and does not include an IDS, a check shall be made at least once every <24> hours to ensure that no attempts to defeat the physical security mechanisms have been made. A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons are responsible, a log identifying the person performing a check at each instance shall be maintained and secured. The last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated. The next person to arrive shall inspect this log and raise a security incident if a required check was not completed.

5.1.2.2 Physical Access for RA Equipment

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. RAs shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module or physical token is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

Any activation information used to access or enable the RA equipment shall be stored separately from the associated modules and equipment. Such information shall either be memorized or recorded and stored in a manner commensurate with the security afforded the associated cryptographic module or equipment.

5.1.3 Power and Air Conditioning

The CSP shall have backup power and emergency lighting capabilities sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The backup power capabilities shall support the availability requirements in Section 6.7.3.

Facilities shall employ environmental controls such that the computer system is protected from risks related from humidity, pressure, radiation and other environmental factors.

5.1.4 Water Exposures

CSP equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors). The facility shall employ the use of emergency shutoff or isolation valves and employ testing to ensure proper function.

Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

The CSP shall comply with local commercial building codes for fire prevention and protection.

5.1.6 Media Storage

Use of portable storage devices shall be limited to the maximum extent possible. When portable storage devices are used, portable storage devices share be logged per section 5.4.1 and sanitized before interfacing with the system if the device has not been used on the system previously.

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access. Media not required for daily operation or not required by policy to remain with the CSP or RA that contains security audit, archive, or backup information shall be stored securely in a location separate from the CSP or RA equipment.

Media containing secret key material shall be handled, packaged, and stored in a manner compliant with the requirements for the sensitivity level of the information it protects or provides access. Storage protection of CSP and RA secret key material shall be consistent with stipulations in Section 5.1.2. Media containing information other than secret key material shall be consistent with stipulation in section 5.4.4.

5.1.7 Waste Disposal

CSP and Operations Staff and RA Staff shall remove and destroy normal office waste in accordance with local policy. Media used to collect or transmit privacy information shall be destroyed, such that the information is unrecoverable, prior to disposal. Sensitive media and paper shall be destroyed in accordance with the applicable policy for destruction of such material.

Destruction of media and documentation containing sensitive information, such as secret key material, shall employ methods commensurate with those in [SP 800-88].

5.1.8 Off-Site Backup

A system backup shall be made when a CSP system is activated. If the CSP system is operational for more than a week, backups shall be made at least once per week. Backups shall be stored offsite. Only the latest backup needs to be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CSP system.

The data backup media shall be stored in a facility that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats and approved for storage of information of the same value of the information that will be protected by the credentials issued or managed using the equipment with a minimum requirement of transferring, handling, packaging, and storage of the information in a manner compliant with requirements for sensitive material identified in Section 6.2.4.1.

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 Trusted Roles shall be extraordinarily responsible, or the integrity of the CSP will be weakened. Trusted role operations include:

- The validation, authentication, and handling of information in credential Applications
- The acceptance, rejection, or other processing of credential Applications, revocation requests, renewal requests, or enrollment information
- The issuance, or revocation of credentials, including personnel having access to restricted portions of its repository
- Access to safe combinations and/or keys to security containers that contain materials supporting production services
- Access to hardware security modules (HSMs), their associated keying material, and the secret share splits of the PINs that protect access to the HSMs
- Installation, configuration, and maintenance of the CSP
- Access to restricted portions of the credential repository
- The ability to grant physical and/or logical access to the CSP equipment

The only trusted roles defined by this policy are the CSP Administrators, CSP Operations Staff, the RA Staff and Audit Administrators. Multiple people may hold the same trusted role, with collective privileges sufficient to fill the role. CSPs may use different titles to describe these roles, or break out the duties in different ways, as long as the requirements for separation duties are met (see Sections 5.2.2 and 5.2.4). Other trusted roles may be defined by the Organization administering the CSP, in which case they will be described as additional subsections below

The CSP shall maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in CSP Administrator, CSP Operations Staff, RAs, and Audit Administrator trusted roles, and shall make them available during compliance audits. The RA shall maintain lists, including names, organizations, and contact information of those who act in RA Staff, RA Administrators, and RA Audit Administrator roles for that RA.

5.2.1.1 CSP Administrator

The CSP Administrator is responsible for:

- Installation, configuration, and maintenance of the CSP;
- Establishing and maintaining CSP system accounts;
- Configuring credential/assertion profiles or templates and audit parameters, and;
- Generating and backing up CSP assertion signing keys.

CSP Administrators are not permitted to issue credentials.

5.2.1.2 CSP Operations Staff

The CSP Operations Staff role is responsible for issuing credentials, that is:

- Registering new Users and requesting the issuance of credentials
- Verifying the identity of Users and accuracy of information included in credentials
- Approving and executing the issuance of credentials
- Requesting, approving and executing the revocation of credentials
- Approving revocation of credentials issued to CSPs or to support the operations of the CSP
- Approving credentials issued to RAs
- Authorizing RAs
- Approving revocation of credentials issued to RAs
- Configuring credential/assertion profiles or templates

Note that the CSP Operations Staff may act as an RA to register and vet Users.

5.2.1.3 Audit Administrator

Audit Administrators are responsible for internal auditing of CSPs and RAs. This sensitive role shall not be combined with any other sensitive role, e.g. the Audit Administrator shall not also be part of the CSP Operations Staff or CSP Administrator. Audit Administrators shall review, maintain, and archive audit logs, and perform or oversee internal audits (independent of formal compliance audits) to ensure that CSPs and RAs are operating in accordance with the associated CPSs.

5.2.1.4 RA Staff

- RA Staff are the individuals holding trusted roles that operate and manage RA components.
- Installation, configuration, and maintenance of the RA
- Establishing and maintaining RA operating system and application accounts
- Routine operation of the RA equipment such as system backup and recovery or changing recording media
- Registering new User and requesting the issuance of credentials
- Verifying the identity of Users
- Verifying the accuracy of information included in credentials
- Approving and executing the issuance of credentials
- Requesting, approving, and executing the suspension, restoration, and revocation of credentials

5.2.2 Number of Persons Required per Task

At least two people shall be trained for each task but only one is required to execute each task.

5.2.3 Identification and Authentication for Each Role

Individuals holding trusted roles shall identify themselves and be authenticated by the CSP and RA before being permitted to perform any actions set forth above for that role or identity. CSP Operations Staff and RA Staff shall authenticate using a credential that is distinct from any credential they use to perform non-trusted role functions. This credential shall be generated per the requirements stipulated in section 3.2, and stored in a system that is protected to the same level as the CSP system.

CSP and RA equipment shall require, at a minimum, strong authenticated access control for remote access using multi-factor authentication. Examples of multi factor authentication include use of a password or PIN along with a time-based token, digital credential on a hardware token or other device that enforce a policy of what a user has and what a user knows.

Individuals holding trusted roles shall be appointed to the trusted role by an appropriate approving authority. These appointments shall be annually reviewed for continued need, and renewed if appropriate. The approval shall be recorded in a secure and auditable fashion. Individuals holding trusted roles shall accept the responsibilities of the trusted role, and this acceptance shall be recorded in a secure and auditable fashion.

Identity proofing of the RA shall be performed by a member of the CSP Operations Staff.

Users shall authenticate themselves to all aspects of the network (servers, operating systems, applications, databases, processes, etc.) before they can access that resource.

5.2.4 Roles Requiring Separation of Duties

Individuals serving as Audit Administrators shall not perform or hold any other trusted role.

Only an individual serving in a Audit Administrator role may perform internal auditing functions.

An individual that performs any trusted role shall only have one identity when accessing CSP equipment.

5.3 Personnel Controls

Personnel Security plays a critical role in the CSP facility's overall security system. Personnel Security shall be designed to prevent both unauthorized access to the CSP facility and CSP systems and compromise of sensitive CSP operations by CSP personnel.

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel seeking to become Trusted Persons shall present proof of the requisite background, qualifications and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any trusted role shall meet the following:

- Be employees of or contractor/vendor of the CSP and bound by terms of employment or contract.
- Be appointed in writing.
- Have successfully completed an appropriate training program.
- Have demonstrated the ability to perform their duties.
- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 5.2.1.
- Have not been previously relieved of trusted role duties for reasons of negligence or nonperformance of duties.
- Require the acknowledgement and periodic review of published rules of behavior.

5.3.2 Background Check Procedures

Persons fulfilling Trusted Roles shall pass a comprehensive background check. CSPs shall have a process in place to ensure employees undergo background checks at least every <5> years.

Prior to commencement of employment in a Trusted Role, the CSP shall conduct background checks (in accordance with local privacy laws) which include the following:

- Confirmation of previous employment
- Check of professional reference
- Confirmation of the highest or most relevant educational degree obtained
- Search of criminal records (local, state or provincial, and national)
- Check of credit/financial records
- Search of driver's license records
- Identification verification via National Identity Check (e.g., Social Security Administration records), as applicable

Factors revealed in a background check that should be considered grounds for rejecting candidates for Trusted Roles or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person
- Highly unfavorable or unreliable professional references
- Certain criminal convictions
- Indications of a lack of financial or personal responsibility

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CSP or RA shall receive comprehensive training and published rules of behavior documentation including, but not limited to social media and external site/application usage restrictions. Training shall be conducted in the following areas:

- CSP/RA security principles and mechanisms to include social engineering attacks that have relevance to the administration and operation of an CSP
- All software versions in use on the CSP/RA system
- All PKI duties they are expected to perform
- Disaster recovery, incident response procedures and business continuity procedures
- Stipulations of this policy

5.3.4 Retraining Frequency and Requirements

All individuals responsible for PKI Trusted Roles shall be made aware of changes in the CSP or RA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CSP software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

No stipulation. If regular job rotation is implemented by a CSP, it should be identified in the corresponding CPS, otherwise this is Not Applicable (N/A).

5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative and disciplinary actions as documented in organization policy shall be taken against personnel who perform unauthorized actions (i.e., not permitted by this CP or other policies) involving the CSP's systems, and the repository. Disciplinary actions may include measures up to and

including termination and shall be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

Contractor personnel filling trusted roles shall be subject to all requirements stipulated in this document. Independent contractors and consultants who have not completed or passed the background check procedures specified above shall be permitted access to the CSP's secure facilities only to the extent they are escorted and directly supervised by people holding trusted roles at all times.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CSP and RA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

5.4.1 Types of Events Recorded

Security auditing capabilities of CSP and RA operating system and applications shall be enabled during installation and initial configuration. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;
- Success or failure where appropriate, and
- The identity of the entity and/or operator that caused the event.

Time shall be synchronized with an authoritative time source to within <three minutes>.

A message from any source requesting an action by the CSP or RA is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents.

The CSP and RA shall record the events identified in the list below. Where these events cannot be electronically logged, the CSP and RA shall supplement electronic audit logs with physical logs as necessary.

- SECURITY AUDIT:
    - Any changes to the Audit parameters, e.g., audit frequency, type of event audited
    - Any attempt to delete or modify the Audit logs
    - Obtaining a third-party time-stamp
- IDENTIFICATION AND AUTHENTICATION:
    - Successful and unsuccessful attempts to assume a role
    - The value of maximum authentication attempts is changed
    - Maximum unsuccessful authentication attempts occur during user login

    - A CSP Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
    - A CSP Administrator changes the type of authenticator, e.g., from password to biometrics
    - Attempts to set passwords
    - Attempts to modify passwords
    - Logon attempts to CSP, CSS or RA applications
    - Escalation of privilege
- LOCAL DATA ENTRY:
    - All security-relevant data that is entered in the system
- REMOTE DATA ENTRY:
    - All security-relevant messages that are received by the system
- DATA EXPORT AND OUTPUT:
    - All successful and unsuccessful requests for confidential and security-relevant information
- KEY GENERATION OR AUTHENTICATOR BINDING:
    - Whenever the CSP generates a key. (Not mandatory for single session or one-time use symmetric keys)
    - Whenever the CSP binds an authenticator to an account
    - Whenever the CSP unbinds an authenticator to an account
- PRIVATE KEY LOAD AND STORAGE:
    - The loading of Component private keys
- TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:
    - All changes to the trusted public keys, including additions and deletions
    - All changes to authenticators including additions and deletions
- SECRET KEY STORAGE:
    - The manual entry of secret keys used for authentication
- PRIVATE AND SECRET KEY EXPORT:
    - The export of private and secret keys (keys used for a single session or message are excluded)
- CREDENTIAL REGISTRATION:
    - All credential requests
- CREDENTIAL REVOCATION:
    - All credential revocation requests
- TOKEN MANAGEMENT
    - Loading tokens with credentials
    - Shipment of tokens
    - Zeroizing tokens
- CREDENTIAL STATUS CHANGE APPROVAL:
    - The approval or rejection of a credential status change request
- CSP or RA CONFIGURATION:
    - Installation of the operating system
    - Installation of the CSP or RA
    - Removing hardware cryptographic modules
    - Re-key of the CSP or RA
    - Destruction of cryptographic modules
    - System startup
    - Any security-relevant changes to the configuration of the CSP or RA
- ACCOUNT ADMINISTRATION:

    - Roles and users are added or deleted
    - The access control privileges of a user account or a role are modified
    - Appointment of an individual to a trusted role
- CREDENTIAL PROFILE MANAGEMENT:
    - All changes to the credential profile
- MISCELLANEOUS:
    - Receipt of hardware / software
    - Backing up CSP or RA internal database
    - Restoring CSP or RA internal database
    - File manipulation (e.g., creation, renaming, moving)
    - Posting of any material to a repository
    - Access to CSP or RA internal database
    - All credential compromise notification requests
    - Configuration changes to the CSP or RA server involving:
        - Hardware
        - Software
        - Operating system
        - Patches
- PHYSICAL ACCESS / SITE SECURITY:
    - Personnel access to room housing CSP or RA
    - Access to the CSP or RA server
    - Known or suspected violations of physical security
    - Any removal or addition of equipment to the CSP/RA enclosure. (Equipment signout and return)
- ANOMALIES:
    - Software error conditions
    - Software check integrity failures
    - Receipt of improper messages
    - Misrouted messages
    - Network attacks (suspected or confirmed)
    - Equipment failure
    - Electrical power outages
    - Uninterruptible power supply (UPS) failure
    - Obvious and significant network service or access failures
    - Violations of credential policy
    - Violations of certification practice statement
    - Resetting operating system clock

5.4.2 Frequency of Processing Log

The audit log shall be reviewed at least once every <30> days and before being archived. All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

Such reviews involve verifying that the log has not been tampered with and performing a thorough examination of any alerts or irregularities in the logs. A statistically significant portion of the security audit data generated by the CSP and RA since the last review shall be examined. This amount will be described in the CPS.

Real-time automated analysis tools should be used. All alerts generated by such systems shall be analyzed.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained on-site for at least <60> days in addition to being archived as described in section 5.5. The individual who removes audit logs from the CSP system shall be an official different from the individuals who, in combination, command the CSP signature key. For the RA, a CSP Administrator other than the RA shall be responsible for managing the audit log.

5.4.4 Protection of Audit Log

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing.

Electronic logs shall be protected to prevent alteration and detect tampering. Examples include digitally signing audit records or the use of a data diode to transfer logs to a separate system to prevent modification after the log is written to media.

Physical logbooks shall implement controls to allow for the detection of the removal of pages or deletion of entries.

Security audit data shall be moved to a safe, secure storage location separate from the location where the data was generated.

CSP/RA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access).

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least every <30> days. A copy of the audit log shall be sent off-site every <30> days.

The audit log collection system may or may not be external to the CSP/RA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall 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; CSP/RA operations shall be suspended until the security audit capability can be restored.

5.4.6 Audit Log Backup Procedures

The audit log collection system may or may not be external to the CSP or RA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall 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; CSP/RA operations shall be suspended until the security audit capability can be restored.

5.4.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy. CSPs and RAs may make their own determination as to whether notifications are required and under what circumstances and specify it in the CSP. Otherwise indicate "None".

5.4.8 Vulnerability Assessments

See Section 6.7.7 for requirements on regular penetration testing.

5.5 Records Archival

5.5.1 Types of Events Archived

CSP or RA archive records shall be sufficiently detailed to determine the proper operation of the CSP or RA and the validity of any credential (including those revoked or expired) issued by the CSP. At a minimum, the following data shall be recorded for archive:

- CSP or RA accreditation (if applicable)
- Credential policy
- Certification practice statement
- Contractual obligations
- Other agreements concerning operations of the CSP or RA
- System and equipment configuration
- User identity authentication data as per section 3.2.3
- Documentation of receipt and acceptance of credentials (if applicable)
- User agreements
- Documentation of receipt of tokens
- All credentials issued
- All Audit logs
- Other data or applications to verify archive contents
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g. audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- All changes to the trusted public keys (i.e. assertion signing keys), including additions and deletions
- Remedial action taken as a result of violations of physical security
- Violations of credential Policy
- Violations of Certification Practice Statement

5.5.2 Retention Period for Archive

Archive records must be kept for a minimum of <7> years and <6> months without any loss of data.

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CSP, the authorized individuals are Audit Administrators. For the RA, authorized individuals are designated by the CSP administrator and must be someone other than the RA.

For the CSP or RA, archived records may be moved to another medium. The contents of the archive shall not be released except in accordance with sections 9.3 and 9.4. Records of individual transactions may be released upon request of any Users involved in the transaction or their legally recognized agents.

Archive media shall be stored in a safe, secure storage facility separate from the CSP or RA with physical and procedural security controls equivalent to or better than those of the CSP or RA. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

5.5.4 Archive Backup Procedures

The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for Time-Stamping of Records

CSP or RA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal or External)

Archive data shall be collected in an expedient manner.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures, detailing how to create, verify, package, transmit, and store the CSP archive information, shall be published in the CPS or a referenced document.

5.6 Key Changeover

To minimize risk from compromise of a CSP's private signing key, that key may be changed often. From that time on, only the new key will be used to sign assertions.

The CSP's signing key shall have a validity period as described in section 6.3.2.

Lifetime of secret key material employed by User's authenticators are defined in section 6.3.2.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

CSP organizations shall have an Incident Response Plan and a Disaster Recovery Plan. Contingency and incident response Plan training shall occur at least annually.

If compromise of a CSP is suspected, credential issuance by that CSP shall be stopped immediately. An independent, third-party investigation shall be performed in order to determine the nature and the degree of damage. The scope of potential damage shall be assessed in order to determine appropriate remediation procedures. If a CSP private signing key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed.

The CSP shall notify the issuing CA if any of the following occur:

- Suspected or detected compromise of any CSP system or subsystem
- Physical or electronic penetration of any CSP system or subsystem
- Successful denial of service attacks on any CSP system or subsystem

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

When computing resources, software, and/or data are corrupted, CSPs operating under this policy shall respond as follows:

- Notify the issuing CA as soon as possible.
- Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup.
- Reestablish CSP operations
- If the CSP signing keys are destroyed, reestablish CSP operations as quickly as possible
- If the integrity of the system cannot be restored, or if the risk is deemed substantial, reestablish system integrity before returning to operation.

5.7.3 Entity Private Key Compromise Procedures

5.7.3.1 Root CA Compromise Procedures

Not Applicable. Refer to recognized PKI Trust Framework Certificate Policy.

5.7.3.2 CSP Compromise Procedures

In the event of a CSP key compromise, the CSP shall notify the issuing CA immediately in the most expedient, authenticated, and trusted manner practicable. The Compromised CSP shall also investigate and report to the issuing CA and <Trust Framework> what caused the compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the compromise can be adequately addressed and it is determined that the CSP can be securely re-established, then, the CSP shall be re-established. Upon reestablishment of the CSP, new User credentials shall be requested and issued.

When a User credential is revoked because of compromise, suspected compromise, or loss of authenticator, a revocation notice as specified in Section 4.9.11, shall be published at the earliest feasible time by the CSP, but in no case more than <6> hours after the CSP is aware of the compromise.

5.3.7.3 CSS Compromise Procedures

Not Applicable. Refer to recognized PKI Trust Framework Certificate Policy.

5.3.7.4 RA Compromise Procedures

In case of an RA compromise, the CSP shall disable the RA. In the case that an RA's key or other authenticators are compromised, the CA or CSP that issued the RA credential shall revoke it, and the revocation information shall be published within <24> hours in the most expedient, authenticated, and trusted manner practicable. The compromise shall be investigated by the CSP in order to determine the actual or potential date and scope of the RA compromise. All credentials approved by that RA since the

date of actual or potential RA compromise shall be revoked. In the event that the scope is indeterminate, then the CSP compromise procedures in Section 5.7.3.2 shall be followed.

5.7.4 Business Continuity Capabilities after a Disaster

CSPs shall be required to maintain a Disaster Recovery and Incident Response Plans. The CSP Disaster Recovery and Incident Response Plans shall be coordinated with any overarching Disaster Recovery and Incident Response Plans that the broader organization may have. The Disaster Recovery and Incident Response Plans shall identify what procedures are in place to mitigate risks to environmental controls, procedures for annual update and testing of processes to restore service including lessons learned, individuals on call for this type of activity, and the order of restoral of equipment and services.

In the case of a disaster in which the CSP equipment is damaged and inoperative, the CSP operations shall be re-established as quickly as possible. If the CSP cannot re-establish capabilities with <6> hours, then the inoperative status of the CSP shall be reported to <Trust Framework> and the issuing CA. <Trust Framework> and the issuing CA shall decide whether to declare the CSP private signing key as compromised and re-establish the CSP keys and credentials, or allow additional time for reestablishment of the CSP's capability.

In the case of a disaster whereby a CSP installation is physically damaged and all copies of the CSP signature key are destroyed as a result, the CSP shall request that its credentials be revoked. The CSP installation shall then be completely rebuilt by re-establishing the CSP equipment, being recertified, and generating/obtaining new private and public keys. Finally, all User credentials will be re-issued.

5.8 CSP or RA Termination

When a CSP operating under this policy terminates operations before all credentials have expired, entities shall be given as much advance notice as circumstances permit.

In addition:

- The CSP and RA shall archive all audit logs and other records prior to termination
- CSP shall request revocation of its Assertion signing key
- The CSP and RA shall destroy all private keys upon termination
- The CSP and RA archive records shall be transferred to an appropriate authority specified in the CPS

6 Technical Security Controls

6.1 Authenticator Generation and Installation

6.1.1 Authenticator Generation

6.1.1.1 CSP Key Pair Generation

Cryptographic keying material used by CSPs to sign identity assertions shall be generated in cryptographic modules validated to [FIPS 140] Level 2, or some other equivalent standard.

Practice Note: NIST 140-3 testing involves inspection of the algorithms, roles, tamper evidence, authentication mechanisms, M of N support, software/firmware integrity, operating environment and mitigation of other attacks. In order for a CSP to claim an HSM is validated to a standard equivalent to FIPS 140, the CSP must provide evidence of third-party validation of the HSM in use that satisfies the same criteria and rigor that FIPS 140 validated HSM models undergo when tested by NIST approved labs. Please note the explicit use of the word "validated" in the policy rather than "compliant". Validation assumes the module has been certified by the Cryptographic Module Validation Program (CVMP) or some other equivalent program. If a comparable program is used, the program shall be stated in the CSPs CPS.

CSP key pair generation must create a verifiable audit trail demonstrating 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. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.1.2 RA Authenticator Binding and Delivery

Authenticators used by RAs to authorize requests and authenticate to the CSP shall be commensurate with the authenticator strength of the highest authenticator assurance level that the CSP is accredited to support under this policy and shall comply with section 6.1.2 of this policy. All communications between the RA and CSP shall occur over mutually authenticated and encrypted (e.g. client authenticated TLS) channels.

6.1.1.3 User Authenticator Secrets Generation

Users shall be bound to an authenticator that meets the requirements defined for an authenticator assurance level defined in section 3.2.1 and 6.2.1 of this policy. When binding additional authenticators to the account, the CSP shall observe the stipulations of this policy to ensure the authenticator meets the requirements of the AAL intended for the User.

Asymmetric key pair generation shall be performed by either the user, CSP, or RA. If the CSP or RA generates user key pairs, the requirements for key pair delivery specified in section 6.1.2 must also be met.

Software or hardware cryptographic modules compliant to [FIPS 140], or some other equivalent standard, should be used to generate all key pairs, as well as pseudo-random numbers and parameters used in key pair generation.

6.1.2 Authenticator Binding and Delivery

CSPs shall bind authenticators to the User's account in a secure manner, ensuring the authenticators issued by the CSP or supplied by the User, meet the criteria of an AAL defined in section 3.2.1 as part of account creation and credential modification as defined in section 4.8.

When single-factor OTP authenticators are bound to a User's account, the CSP shall conform to the stipulations of sections 4, 6.1.5 and 6.3.2 to:

1. Generate and exchange the OTP shared secret with the user using a mechanism that protects the OTP shared secret from compromise; or

2. Obtain the secret data from the user necessary to duplicate the authenticator output in a way that is impersonation resistant.

CSPs shall use cryptography defined in section 6.1.5 and 6.1.7 when collecting OTPs to prevent eavesdropping and MitM attacks.

If Users generate their own asymmetric key pairs, then there is no need to deliver private keys.

When CSPs or RAs generate secret key material on behalf of the User, then the secret key must be delivered securely to the User. Secret keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- The activation data and authenticators must be protected from activation, compromise, or modification during the delivery process.
- The User shall acknowledge receipt of an authenticator
- Delivery shall be accomplished in a way that ensures that the authenticators and activation data are provided to the correct Users.
    - For hardware modules, accountability for the location and state of the module must be maintained until the User accepts possession of it.
    - For electronic delivery of secret keys, the key material shall be encrypted using a FIPSapproved cryptographic algorithm and key size at least as strong as the secret key. Activation data shall be delivered using a separate secure channel.

The CSP must maintain a record of the User acknowledgment of receipt of the key.

CSPs shall ensure at least one authenticator that represents possession (something the User has) is bound to the user's account in addition to a memorized secret or a biometric that complies with section 6.1.7 of this policy. User-provided authenticators shall conform to the same requirements as CSP-issued authenticators.

If an authenticator cannot be bound to a User during the same (single) protected electronic session as the identity proofing event described in section 3.2.3, then the CSP shall issue a temporary, memorized secret either delivered during the protected session or delivered to the applicant via verified phone number, email address or postal address of record. The temporary memorized secret can then be provided by the User to bind additional authenticators to the User's account, at which point the temporary secret shall become invalidated.

A CSP may elect to bind a long-term memorized secret to the user's account, instead of a temporary memorized secret, provided the long-term memorized secret complies with section 6.5.1.1.5 of this policy. The CSP may use the long-term memorized secret to bind additional authenticators to the user's account as defined in section 4.8.

If the User has been identity proofed in-person, the User may be issued a short term authenticator as described above for protected electronic sessions or capture a biometric from the User for use at a later time to bind additional authenticators to the User's account. All long-term authenticators issued to a User (e.g. CSP-generated) during a physical session shall be loaded locally onto a physical device that is provided to the user in-person or to the User's address of record.

6.1.3 Public Key Delivery to CSP

Where key pairs are generated by the CSP or RA, the public key and the AOR's identity must be delivered securely (e.g., using TLS with approved algorithms and key lengths) to the CA for Certificate issuance. The delivery mechanism shall bind the CSP's verified identity and other attributes to the public key.

6.1.4 CSP Public Key Delivery to Relying Parties

The public key of one or more of a root CAs shall be provided to the relying parties in a secure manner so that it is not vulnerable to modification or substitution.

6.1.5 Key Sizes and Strength

If the PA determines that the security of a particular algorithm has been compromised, it will direct the accredited CSPs to revoke and re-bind unaffected authenticators of the same strength to the affected accounts per section 4.8.

All public keys placed in newly generated assertions and uses of symmetric, asymmetric or other cryptography by CSP components for signature, shared secrets, OTP, and/or key agreement/encryption operations must meet or exceed the following algorithm suites for the time periods indicated in the table below:

	Key length and/or Algorithm Attack Resistance	Sunset Date
Secret Key (used with cryptographic authenticators)	112 bits of security (per NIST SP 800-131A) CSPs shall define how the algorithms and authenticators supported by the CSP meet the attack resistance threshold in the CPS.	No stipulation
Nonce (used to generate OTP values)	Maintains uniqueness for each operation within the authenticator via time, incremental counter or some other method. CSPs shall define how uniqueness of nonces, if used, are maintained in the CPS.	No stipulation
Challenge Nonce (used to prove possession of private key)	64 bits and statistically unique over the verifier's/authenticator's lifetime or usings a random bit generator as defined in SP 800-90Ar1	No stipulation

Memorized Secret	See section 6.5.1.1.5 for entropy requirements. Key derivation function: NIST SP 800-132 One way functions: FIPS: 198-1, 202; NIST SP: 800-107, 800-38B, 800-185 latest revisions. Hash algorithms deprecated by NIST shall not be used.	No stipulation
salt (used in protect hashed passwords and lookup secrets)	32 bits generated randomly in conformance with NIST SP 800-90Ar1 and stored separately from the shared secret value per section 6.2.7.	No stipulation
PIN (used to activate authenticator)	6 digits	No stipulation
Confirmation Codes	at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1]	
Look-up Secrets	112 bits of security generated with a random bit generator conformant with [SP 800-90Ar1] and stored with salted SHA256 hash or higher for each lookup secret	No stipulation
Out-of-band Authenticator secrets	generated with at least 20 bits of entropy using an algorithm that complies with [NIST SP 800-90Ar1]. CSPs shall implements rate limiting functions for out-of-band authenticator secrets with less than 64 bits of entropy.	No stipulation
Authenticator Attestation Digital Signature	RSA: 2048 bit key size ECC: 224 bit ECDSA in prime field, or 233 bit ECDSA in binary field Hash: SHA 256	No stipulation
Assertion Signing Key	RSA: 2048 bit key size ECC: 224 bit ECDSA in prime field, or 233 bit ECDSA in binary field Hash: SHA 256	No stipulation

OTP output value (both single factor and multifactor)	May truncate value to 6 digits (20 bits of entropy) If the authenticator output has less than 64 bits of entropy, the CSP SHALL implement a rate-limiting mechanism to prevent brute force attacks of OTP output at the CSP and shall accept a time-based OTP once during the validity period	No stipulation

Assertions issued under this policy shall contain RSA or elliptic curve signatures.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall always be generated and validated in accordance with [FIPS 186-4].

Elliptic Curve public key parameters shall always be selected from the set specified in section 7.1.3.

CSPs shall include nonce values in signed assertions to prevent replay attacks. Nonce values shall only be accepted once, and shall conform to lifetime requirements and uniqueness requirements defined in sections 6.3.2 and 6.1.5 respectively.

6.1.7 Use of Authenticators and Biometrics

CSPs use authenticators to prove that a stated User is who they claim to be, either using biometrics, or by verifying that the User's possesses a secret (either physically or mentally) that is only known to the identity associated with the User's account. Therefore, CSPs shall employ carefully crafted technologies when using various authenticators bound to a User to prove a given User's identity and shall disallow use of authenticators that present unacceptable risks. Examples of such authenticators are either defined in this section or in section 3.2.1 with further elaboration in NIST 800-63-3B. CSPs shall adhere to industry standards that define best practices for employing the various authenticators supported by the CSP and ensure the algorithms & lifetimes, rate limiting functions and key sizes are observed as defined in sections 6.3.2 and 6.1.5. CSPs shall also inform Users about the risks associated with certain authenticators that the CSPs deems unacceptably risky and offer alternative authenticators that the User may employ to achieve the same AAL. CSPs shall define which standards adhered to for each authenticator as well as other relevant details within the CSP's CPS.

CSPs shall verify through a trusted statement from the authenticator source, or some other means that a multi-factor device is in fact multi-factor. If a multi-factor device cannot be verified as being muti-factor, the CSP shall treat the device as a single factor authenticator. If an attestation from an authenticator is signed, it shall employ a digital signature that complies with the requirements of section 6.1.5. Protocols that use nonces or challenges to prove the "freshness" of the transaction are resistant to replay attacks since the CSP will easily detect when old protocol messages are replayed and shall be employed for at least one authenticator when asserting an AAL2 or higher authentication event within a CSP signed assertion.

When lookup secrets are used, the CSP shall employ an authenticated and protected channel in order to preserve confidentiality of the lookup secrets and inhibit MitM attacks.

Data produced by an authenticator to prove possession of secret data to a verifier (e.g. OTP) or secret data that serves as an authenticator (e.g. password) shall be transmitted over an authenticated and encrypted channel in a way that is resistant to MitM attacks.

CSPs shall utilize a separate and protected (e.g. TLS) channel to obtain or receive out-of-band authenticator secrets and OTPs in such a fashion that the out-of-band authenticator proves the possession of the device by to subscriber to the CSP. Use of primary and secondary channels shall observe industry recognized techniques documented in the CSPs CPS in a way that conforms to the applicable requires defined in NIST SP 800-63B. Out-of-band authenticator secrets and OTPs shall only be used once and comply with sections 6.1.5 and 6.3.2.

When biometrics are used as a means of authenticating Users, they shall not be used alone. The CSP shall also require the User to authenticate with a physical authenticator bound to the User's account. If biometrics are used to activate secret data, such as the case with multifactor cryptographic devices, the biometric activation data shall be zeroized after the secret key has been exercised. The CSP sensor or endpoint used to collect a biometric sample from the User shall be authenticated and shall occur over an authenticated channel. Sensors shall operate with a False Match Rate (FMR) of 1 in 1000 or better. If the sensor cannot be authenticated and verified to operate at an FMR of 1 in 1000 or better, then biometrics shall not be used as an authentication factor by Users. Biometric sensors or endpoints shall implement Presentation Attack Detection (PAD) capabilities and shall impose a delay of at least 30 seconds or default to an on alternative authenticator in the event of 10 consecutive failed authentication attempts. Biometric capture devices and verifier endpoints shall be mutually authenticated to prevent MiM attacks.

Biometric templates generated, compared and stored by CSPs shall define how templates are protected and revocable in a manner conformant to ISO/IEC 24745 in the CSP's CPS.

6.2 Secret Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CSPs that assert AAL1 or AAL2 may use a hardware cryptographic module validated to [FIPS 140] Level 1 (or higher), or some other equivalent standard for signing operations. CSPs that assert AAL3 shall use a hardware cryptographic module validated to [FIPS 140] Level 3 (or higher), or some other equivalent standard for signing operations. RAs shall use AAL3 authenticators for authenticating to a CSP after verifying a User at all IALs.

When Users employ software cryptographic modules, the software module shall have been validated at FIPS 140-3 level 1. When Users employ hardware cryptographic modules, there is no requirement for the hardware module to be validated at FIPS 140-3 level 2 or some other equivalent standard.

Practice Note: If a FIPS 140-3 level 1 validated module requires a software update to secure a vulnerability, such an activity would not be considered a violation of this policy.

6.2.2 Private Key (N of M) Multi-Person Control

No stipulation.

6.2.3 Private Key Escrow

CSP private signing keys shall not be escrowed, but may be backed up per section 5.7.

6.2.4 Secret Key Backup

6.2.4.1 Backup of CSP Private Signature Key
The CSP private signature keys shall be backed up under the same control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CSP private signature key shall be accounted for and protected in the same manner as the original. Backup procedures shall be included in the CA's CPS.

6.2.4.2 Backup of Human User Secret Keys
Backed up human user and role secret keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the user's cryptographic module and shall be under the control of the user.

6.2.5 Secret Key Archival

CSP private signature keys and User secret key material shall not be archived.

6.2.6 Secret Key Transfer into or from a Cryptographic Module

CSP private keys may be exported from the cryptographic module only to perform CSP key backup procedures as described in Section 6.2.4.1. At no time shall the CSP private key exist in plaintext outside the cryptographic module or cached outside of HSM memory.

In the event that a CSP private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

CSPs shall prohibit the cloning or exporting of secret cryptographic data across multiple User devices in support of OTP generation or other authentication mechanisms.

6.2.7 Secret Cryptographic Data Storage on Cryptographic Module

User and CSP symmetric and asymmetric secret key material (including salts for for password security) shall be stored or protected by a module that has historically undergone FIPS 140-3 level 1 or equivalent cryptographic module testing or that conforms to the requirements defined in sections 6.1.5 and 6.3.2. CSP assertion signing private keys shall be protected at a level commensurate with the highest AAL supported by the CSP.

6.2.8 Method of Activating Assertion Signing Private Key

Activation of the CSP Assertion Signing Key shall only occur follow a specific set of events defined in the CSPs CPS that relate to User or Trusted Role authentication . The diversification master keys shall only be stored in hardware cryptographic modules. CSP Assertion Signing Key shall be protected from unauthorized activation, disclosure and distribution.

6.2.9 Method of Deactivating Authenticators

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CPS.

After successful activation of the Authenticator by the user, the activation data shall be zeroized immediately after the authenticator has finished its operation.

6.2.10 Method of Destroying Secret Key Material

Individuals in trusted roles shall destroy CSP and RA, private signature keys when they are no longer needed. Users may either surrender their cryptographic module to CSP/RA personnel for destruction or destroy their secret keys, when they are no longer needed or when the Credentials to which they correspond expire or are revoked. Physical destruction of hardware is not required.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Credential Operational Periods and Key Usage Periods

Cryptographic material employed by CSPs and authenticators used by CSP users shall have an expiration date defined in the CSP's CPS. If an authenticator or authenticator componet exceeds its maximum lifetime defined below, it shall not be used for authentication or to support an authentication event.

The following table provides the lifetimes for key material and authenticators issued to the owner of that credential.

Type of Cryptographic Material or Data	Maximum Lifetime
Authentication Token	5 minutes
Authorization Token	5 minutes
Session Secret (maximum period of inactivity)	AAL1: 30 days AAL2: 30 minutes AAL3: 15 minutes
Nonce	2 minutes

One-Time Passwords (OTP)	2 minutes. Allowances for expected clock drift, network delay and user entry are acceptable. Time-based nonces shall be generated based on a real-time clock.
Hardware-based FIDO Keys	
Software-based FIDO Keys	
OTP Shared Secret (seed)	
Memorized Secret	
Out-of-band authenticator secret validity period	10 minutes
Confirmation Codes	• Postal address of record: maximum of 7 days but may be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service. • Sent by means other than physical mail (i.e. email): maximum of 10 minutes.

All Credentials signed by a specific CSP key pair must expire before the end of that key pair's usage period.

6.3.3 Re-authentication Secrets Provided by CSP

After a User has been authenticated (verified) by a CSP at a given level using authenticators bound to the user's account, the CSP may issue a session secret that may be refreshed during the session, provided the session secret meets the requirements of this section for the AAL being asserted.

Reauthentication Requirements by AAL		
AAL	Maximum Period Between Re-authentication Events	Authentication Factors Required for Re-authentication
AAL1	30 days; refresh tokens can be up to 30 days	Any single factor
AAL2	12 hours; Refresh tokens limited to 30 minutes	Memorized Secret or biometric
AAL3	12 hours; Refresh tokens limited to 15 minutes	Factors defined in section 3.2.1

		for AAL3

All session secrets shall not be retained across a restart of the User's application or device and shall observe lifetime requirements defined in section 6.3.2. The CSP shall manage its session secrets and timeout periods based solely on the activity of the user and shall not correlate session secrets or management with a relying party system, except if the relying party system specifies a maximum authentication event time. If a maximum authentication event time is specified by a relying party, the CSP shall observe the time interval specified by the relying party and trigger a re-authentication event if necessary.

6.4 Activation Data

Activation data is information that is either entered by the user to activate a credential or through a feature necessary to use the credential, in a way that shows authentication intent.

The user must be authenticated to the cryptographic token or authenticator before the activation of the associated key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered). Some types of authenticators do not require authentication to activate, but rather require the User to tap the authenticator for activation. Support for such authenticators shall be documented in the CPS and shall only be used with an additional factor (e.g. memorized secret).

A device or application may be configured to activate its key without requiring activation data, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token.

6.4.1 Activation Data Generation and Installation

CSP activation data may be user-selected (by each of the multiple parties holding that activation data). If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

RA and user activation data may be user-selected. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

Single factor authenticators shall require some action to be taken by the user such as pressing a button or some other action that prevents the authenticator from being activated unintentionally or maliciously.

6.4.2 Activation Data Protection

Data used to unlock multi factor authenticators or other secret cryptographic data shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data used to activate the private or secret key of a multi factor authenticator shall be either:

- Memorized, at least 6 decimal digits in length and rate limited; or otherwise adhering to section 6.5.1.1.5 and chosen by the User; OR
- Biometric in nature.

For multi factor authentication, biometric activation data shall adhere to the requirements defined in section 6.1.7.

When a mobile device is used as an authenticator, the User shall be authenticated to the device (often with a PIN or biometric) in order to provide activation data to the authenticator. Unlocking the device shall not constitute an authentication factor and shall occur independent of the activation of an authenticator, even if the same activation data is used for unlocking the device and activating the authenticator.

6.4.3 Other Aspects of Activation Data Protection

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

6.5.1.1 Access Control

Access to information such as sensitive details about customer accounts, passwords, and ultimately, CSP related private keys should be carefully guarded, along with the machines housing such information.

6.5.1.1.1 Access Control Policy and Procedures

The CSP shall create and document roles and responsibilities for each trusted role employee job function in the CPS. The CSP shall create and maintain a mapping of these trusted roles and their associated responsibilities to specific employees and their accounts on CSP and/or RA systems.

6.5.1.1.2 Account Management

Information system account management features shall ensure that users access only that functionality permitted by their role or function. All account types with access to information systems shall be documented along with the conditions and procedures to follow in creating new accounts. Groups and roles shall have a documented relationship to the business or mission roles involved in operating the CA.

Section 5.2.1 of this document defines roles and job functions for personnel that the CSP will use when defining access control mechanisms. Section 4 of this document specified credential lifecycle requirements that shall be observed by the CSP when creating and managing the lifecycle of User accounts. The CSP shall employ the principle of least privilege when creating users and assigning them to groups and roles; membership to a group or role shall be justified based upon business need. The CSP shall take appropriate action, including notification of Security Officer or equivalent role defined in the CPS, when a user no longer requires an account, their business role changes, or the user is terminated or transferred. The CSP shall <annually> review all active accounts to match active authorized users with accounts, and disable or remove any accounts no longer associated with an active authorized user.

Automated systems shall be employed to deactivate emergency accounts as soon as practicable, and maintain access for only those users who are still authorized to use the information system. After <30 days> of inactivity, an account shall be automatically disabled and attempts to access any deactivated account shall be logged.

All account administration activities shall be logged and made available for inspection by appropriate security personnel. Account administration activities that shall be audited include account creation,

modification, enabling, disabling, group or role changes, and removal actions. See Section 5.4 for detailed requirements for these logs.

Guest/anonymous accounts for logon to information systems shall be prohibited. Accounts shall be assigned to a single user and shall not be shared.

6.5.1.1.3 Least Privilege

In granting rights to accounts and groups, the CSP shall employ the principle of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. The CSP shall explicitly authorize access to accounts and groups for controlling security functions and security relevant information. The CSP shall authorize access to privileged commands and features of information systems only for specific, organization-defined compelling operational needs and documents the rationale for such access. The CSP shall require that users of information systems with access to administrative privileges to utilize non-privileged accounts or roles when accessing non-privileged functions (such as reading email).

6.5.1.1.4 Access Control Best Practices

CSPs shall ensure session locks and pattern hiding displays are used after a period of inactivity defined in the CPS. CSPs shall ensure that the systems used to consume authenticators are employing and correctly implementing the industry standards that define the authenticators' appropriate use (e.g. IETF RFCs, ISO standards, FIDO Alliance, etc…). Trusted Roles shall authenticate the first time an account is activated (SSO is acceptable for subsequent authentications) and shall re-authenticate when activating or switching between Trusted Role accounts or when credentials change.

6.5.1.1.5 Authentication: Passwords and Accounts

When the authentication mechanism uses operator selectable passwords, strong passwords shall be employed, as defined in the CSP's CPS. Passwords for CSP authentication shall be different from non-CSP systems. Trusted Roles shall employ the use of authenticators to access CSP systems that are commensurate with the highest level of assurance credentials issued by the CSP.

CSPs shall define password complexity requirements in their CPS that include at least the following features:

- Password entropy should be at least 64 bits.
- at least 8 unicode characters long
- obscure password upon entry
- a mix of uppercase and lowercase characters, numbers, and symbols
- Symbols: `~!@#$%^&*()-=_+[{]}\|;':",.<>/?
- If a lesser pool of characters are used, the password length shall be increased in order to obtain at least 64 bits of entropy;
- no consecutive repeating characters (for example, RR or 55)
- not based on username, personal information, or dictionary words
- dissimilar to previous passwords
- regularly changed (for instance, every 90 days)
- Verify, when users create or update passwords, that the passwords are not found on

the list of commonly-used, expected, or compromised passwords.
- Transmit passwords only over cryptographically-protected channels;
- Store passwords using an approved salted key derivation function, preferably using a keyed hash;
- Disallow truncation of passwords;
- Require immediate selection of a new password upon account recovery;

CSPs shall employ the use of rate-limiting functions to prevent brute force attacks, limited to 100 attempts within a time span of no more than 1 hour. CSPs shall not use hints or similar mechanisms that are accessible to anonymous or otherwise unauthenticated Users. CSPs shall not recommend the contents of a password beyond specifying complexity requirements. CSPs shall force Users to change their password if the CSP receives evidence that a User's password is compromised, per section 4.8.

For all memorized secrets, the CSP shall employ industry defined and accepted one-way key derivation functions that included a salted hash, for each User account, that meets the complexity requirements defined in this section and section 6.1.5 and stored in conformance with section 6.2.7. The CSP shall document salted hash key derivation functions employed in the CPS in conformance with section 6.1.5 requirements.

For Trusted Roles, the CSP shall require the use of "strong" passwords if passwords are used and have the minimum number of user accounts that are necessary to its operation. Account access shall be locked after 5 unsuccessful login attempts. Restoration of access shall be performed by a different person who holds a trusted role, or restore access after a timeout period.

6.5.1.1.6 Permitted Actions without Identification or Authentication

The CSP shall document in the CPS a specific list of actions that can be performed on specifically enumerated information systems without identification or authentication, such as retrieving or verifying a published CRL from an Internet-accessible server or accessing a publicly available website. Furthermore, the organization shall document and provide supporting rationale in its security policy and procedures an enumerated list of user actions and systems not requiring identification or authentication (i.e., anonymous access).

6.5.1.2 System Integrity

6.5.1.2.1 System Isolation and Partitioning

CSP systems shall be configured, operated, and maintained so as to ensure the continuous logical separation of processes and their assigned resources. This separation shall be enforced by

- Physical and/or logical isolation mechanisms, such as dedicated systems or virtualization
- protecting an active process and any assigned resources from access by or interference from another process
- Protecting an inactive process and any assigned resources from access by or interference from an active process
- Ensuring that any exception condition raised by one process will have no lasting detrimental effect on the operation or assigned resources of another process

All trusted components should be logically separated from each other, and shall be logically separated from any untrusted components of the CSP system. The CPS shall document how this logical isolation of components is accomplished.

Security critical processes shall be isolated from processes that have external interfaces. For example the CSP signing processes shall be isolated from registration processes. The CPS shall outline how security critical processes are protected from interference by externally facing processes.

If there are system resources shared amongst trusted and/or untrusted processes, the underlying system(s) shall prevent any unauthorized and unintended information transfer between processes via those shared system resources.

The CSP shall develop and document controlled procedures for transferring software updates, configuration files, Credential requests, and other data files between trusted components.

6.5.1.2.2 Malicious Code Protection

The CSP system shall employ malicious code protection mechanisms to mitigate the risk of malicious code on CSP system components. Malicious code on trusted CSP components could allow an attacker to issue fraudulent Credentials, create a rogue intermediate or signing CSP server, or compromise the availability of the system.

CSP system components running standard operating systems that are not air-gapped from the Internet shall employ host-based anti-malware tools to detect and prevent the execution of known malicious code. These tools shall be configured to automatically scan removable media when it is inserted, as well as files received over the network. Introduction of removable media shall not cause automatic execution of any software residing on the media.

Anti-malware tools employed by a CSP shall be properly maintained and updated by the CA. Antimalware tools on networked systems shall be updated automatically as updates become available, or CSP Administrators shall push updates to system components on a <weekly> basis. Anti-malware tools may be employed on air-gapped systems. If anti-malware tools are employed on air-gapped systems, the CSP shall document in the CPS how these tools will be updated, including mitigations intended to reduce the risks of spreading malware and exfiltration of data off of compromised CSP systems. Anti-malware tools shall alert CSP Administrators of any malware detected by the tools.

On system components that do not implement host-based anti-malware tools, the CSP shall identify and employ other malicious code protection mechanisms to prevent the execution of malicious code, detect infected files or executables, and remediate infected systems. These mechanisms could include, but are not limited to, compensating physical protection on hosts, network-based malware detection tools at boundary points, application whitelisting, and manually scanning removable media by trusted CSP personnel. The CSP shall document all malware protection mechanisms in the CPS.

6.5.1.2.3 Software and Firmware Integrity

The CSP shall employ technical and procedural controls to prevent and detect unauthorized changes to firmware and software on CSP systems. Access control mechanisms and configuration management processes (see Section 6.5.1.1 and 6.6.2) shall ensure that only authorized CSP Administrators are capable of installing or modifying firmware and software on CSP systems.

Root and subordinate CSP servers shall implement automated technical controls to prevent and detect unauthorized changes to firmware and software. Example technical controls include signature verification prior to firmware/software installation or execution (such as firmware protections that comply with [SP800-147] or [SP800-147B]), or hash-based white-listing of executables. Unauthorized software or firmware detected by these mechanisms should be blocked from executing. Any instances of unauthorized firmware or software detected by the system shall be logged, and CSP Administrators shall be notified of these events.

6.5.1.2.4 Information Protection

The CSP shall protect the confidentiality and integrity of sensitive information stored or processed on CSP systems that could lead to abuse or fraud. For example, the CSP shall protect customer data that could allow an attacker to impersonate a customer. The CSP shall employ technical mechanisms to prevent unauthorized changes or accesses to this information, such as access control mechanisms that limit which users are authorized to view or modify files. Sensitive information stored on devices that are not physically protected from potential attackers shall be stored in an encrypted format.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls address various aspects related to the development and change of the CSP system through aspects of its life-cycle.

The CSP system shall be implemented and tested in a non-production environment prior to implementation in a production environment. No change shall be made to the production environment unless the change has gone through the change control process as defined for the system baseline.

In order to prevent incorrect or improper changes to the CSP system, the CSP system shall require Trusted Role controls for access to the CSP system when changes are made.

For any software developed by the CSP, evidence shall be produced relating to the use of a defined software development methodology setting out the various phases of development, as well as implementation techniques intended to avoid common errors to reduce the number of vulnerabilities. Automated software assurance (i.e. static code analysis) tools shall be used to catch common error conditions within developed code. For compiled code, all compiler warnings shall be enabled and addressed or acknowledged to be acceptable. Input validation shall be performed for all inputs into the system.

Hardware and software procured to operate the CSP shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device). The hardware and software shall be verified as being supplied and actively supported from the vendor, with no modifications, and be the version intended for use. Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner. The CSP shall designate one or more individuals responsible for Supply Chain Risk Management and mitigation.

All data input to CSP system components from users or other system components shall be validated prior to consumption by the receiving entity. Validating the syntax and semantics of system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match the expected definitions for format and content.

6.6.2 Security Management Controls

A list of acceptable products and their versions for each individual CSP system component shall be maintained and kept up-to-date within a configuration management system. Mechanisms and/or procedures shall be in operation designed to prevent the installation and execution of unauthorized software. A signed whitelist of the acceptable software for the system should be one of the ways to control the allowed software. A CSP system shall have automated mechanisms to inventory on at least a daily basis software installed on a system and alert operators if invalid software is found.

To reduce the available attack surface of a CSP system, only those ports, protocols, and services that are necessary to the CSP system architecture are permitted to be installed or operating. The CSP system shall maintain a list of ports, protocols, and services that are necessary for the correct function of each component within the CSP system and reviewed annually. There shall be automated mechanisms to monitor the running processes and open ports against the permitted list.

To validate the integrity of the CSP system, automated tools that validate all static files on a component shall be in operation to notify operators when a protected file has changed. If email is used on CSP systems, phishing and spam protection mechanisms must be employed.

The CSP system shall establish and document mandatory configuration settings for all information technology components which comprise the CSP system. All configuration settings capable of automated assessment shall be validated to be set according to the guidance contained within a documented security configuration checklist on at least daily basis for powered on systems or next power-on for systems which are not left powered-on.

6.6.3 Life Cycle Security Controls

CSPs shall implement security controls and a risk management process that is commensurate with the level of current and emerging risks to which the CSP is subject. For flaw remediation, the CSP shall scan all online CSP systems for vulnerabilities using at least one vulnerability scanner every <one week>. The use of multiple scanners on the most sensitive systems is strongly encouraged.

Each vulnerability found shall be entered into a vulnerability tracking database, along with the date and time of location, and shall be remediated within <72 hours>. Remediation shall be entered into the vulnerability database as well (including date and time).

The CSP shall monitor relevant notification channels on a <daily> basis for updates to packages installed on CSP systems (including networking hardware). CSPs shall have a plan for receiving notification of software and firmware updates, for obtaining and testing those updates, for deciding when to install them, and finally for installing them without undue disruption. For critical vulnerabilities, the CSP shall evaluate and install the update within <24 hours>. For less critical vulnerabilities, the CSP shall evaluate each package to determine whether an update is required, and if so, that update shall be applied to all affected CSP systems within <48 hours>. A log shall be kept of the notifications, the decision to apply/not apply including reason, and the application of relevant updates/patches.

From time to time, the CSP may discover errors in configuration files, either because of human error, source data error, or changes in the environment which have made an entry erroneous. The CSP shall correct such errors within <24 hours> of discovery, and shall document the reason for the error, and the associated correction.

Remediation activities should not cause unavailability of revocation information.

6.7 Network Security Controls

Many components of a CSP are connected to each other and their customers via various forms of

networks. While it is necessary for connections to customers and administrative systems, care needs to be taken to ensure those connections do not adversely impact the security of those components. Guidelines for effective CSP networking security are discussed in the following sections.

6.7.1 Isolation of Networked Systems

Communication channels between the network-connected CSP components and the trusted CSP processing components shall be protected against attack. Furthermore, information flowing into these CSP components from the network-connected CSP components shall not lead to any compromise or disruption of these components.

The components of a CSP requiring direct network connections shall be minimized. Those networked components shall be protected from attacks through the use of firewalls to filter unwanted protocols (utilizing access rules, whitelists, blacklists, protocol checkers, DNS security measures, etc., as necessary). Data loss prevention tools shall be employed to detect inappropriate leakage of sensitive information.

6.7.2 Boundary Protection

Instruction: Describe the boundary protections between CSP security zones here. The following sections will describe boundary protections in the context of four zone types. The zones are not assumed to be nested. They may be interconnected, but are independent. Zone boundaries are defined by limits of authority over the security of the data processed within the boundary. Interconnection of two zones, even at the same protection level, must be done in a way that respects the different authorities of the two zones. The zones are:

- *Special Access Zone (SAZ) - highly controlled network area for processing and storage of especially high value data. It should be assumed that a network in this zone is not interconnected to any other network.*
- *Restricted Zone (RZ) - controlled network area for sensitive data processing and storage.*
- *Operations Zone (OZ) - network area containing systems for routine business operations.*
- *Public Zone (PZ) - any network area that is not behind a protective boundary controlled by the organization. Includes the public Internet and the public telephone network. Since there is no presumed control over the Public Zone, there are no requirements for boundary protection.*

6.7.2.1 PKI Network Zones Overview

Instruction: The following three sections describe the boundary of each zone type in the context of an extended CSP, including connections to systems that support but are not part of the CA. In each section,

define the network protections to be provided to PKI components by assigning them to the permitted zone(s) for each component.

The following zone assignments represent typical and reasonable protection:

- *A Root CSP is expected to reside in a Special Access Zone with no network connection to any other network at all.*
- *Subordinate CSPs are expected to reside in one or more Restricted Zones, with connections allowed from the Public Zone for RA Agent access and from the Operations Zone for business function access.*
- *The RA Server is expected to reside in a Restricted Zone distinct from the Restricted Zone occupied by the CSP Signing Servers.*
- *The RA Agent may reside in a Restricted, Operations, or Public Zone. While the RA Agent may use special hardware and software to accomplish their tasks, the organization will have no control over the RA Agent's workstation's network connection if it operates in the Public Zone. The data must be selfprotecting or session protected as it leaves the RA Agent's workstation.*

6.7.2.2 Special Access Zone Boundary

Instruction: A SAZ has no physical nor logical interconnection to any other network.

- *Physical boundary protection measures shall include checks for network elements (cables, routers, wireless equipment) that indicate interconnection.*
- *Physical boundary protection devices shall fail securely in the event of an operational failure.*
- *Incoming communication is limited to Credential signing requests, revocation requests, and system maintenance data.*
- *Outgoing communication is limited to signed Credentials, CRLs, and any data related to monitoring and audit.*
- *Communication shall be accomplished by means of write-once media or media that is sanitized on first use and between uses. Media shall be scanned after writing. The sanitization and scanning shall take place on a device isolated and designated solely for this purpose.*
- *Auditing functions shall be enabled on systems in the SAZ, according to the requirements in Section 5.4.*
- *Systems shall be physically isolated to separate platform instances and uniquely identified on each subnet within SAZ boundary with managed interfaces.*

6.7.2.3 Restricted Zone Boundary

Instruction: An RZ has physical interconnections to other RZs, OZs, and potentially the PZ.

- *Physical interconnections must be documented as to where they exist, for what purpose, and what protections are provided.*
- *All physical systems shall identify and limit all systems to managed interfaces.*
- *All interconnections must be filtered based on origin, destination, and type.*
- *Physical boundary protection measures shall include checks for network elements (cables, routers, wireless equipment) that indicate unauthorized interconnection.*

- *Physical boundary protection devices shall fail securely in the event of an operational failure.*
- *Connections with other RZs may be firewalled interconnections that maintain the security posture of each RZ.*
- *Connections with OZs must be limited to specific protocols, and connections digitally authenticated. If there is a Wireless Access Point in the OZ, a VPN Gateway shall be used to connect to the Restricted Zone.*
- *Confidentiality shall be provided depending on the sensitivity of the information transferred and the route of the connection.*
- *Connection with the PZ must be made through a bastion host that is hardened for exposure to a hostile network environment. Such bastion hosts must be minimized in number and documented as to location, purpose, and system and service configuration.*
- *Firewalls shall allow only those protocols necessary to perform a function and only from recognized network origins by denying network traffic by default and allowing network traffic only by exception (i.e., deny all, permit by exception).*
- *All communications shall be source authenticated and should be encrypted.*

- *Incoming communications shall be limited to Credential signing requests, CRL requests, key recovery requests, key escrow messages, revocation requests, responses from support systems (e.g., from a directory), and system maintenance data.*
- *Outgoing communications shall be limited to signed Credentials, CRLs, key recovery data, revocation request responses, requests for user authentication and authorization data, and any data related to monitoring and audit.*
- *Monitoring and auditing functions shall be enabled on the systems in the RZ, including network components where appropriate, according to the requirements in Sections 5.4 and 6.7.5.*
- *Indications that boundary protections have failed must be dealt with urgently (see Section 5.7).*
- *Wireless access points (WAP) shall NOT be allowed in the Restricted Zone at any time.*

6.7.2.4 Operational Zone Boundary

Instruction: An OZ has physical interconnections to other OZs, RZs, and the PZ.

- *Physical interconnections must be documented as to where they exist, for what purpose, and what protections are provided.*
- *All interconnections must be filtered based on origin, destination, and type.*
- *Physical boundary protection measures shall include checks for network elements (cables, routers, wireless equipment) that indicate unauthorized interconnection.*
- *Physical boundary protection devices shall fail securely in the event of an operational failure.*
- *Connections with RZs shall be driven by the RZ boundary protection requirements.*
- *Connections with other OZs may be firewalled router interconnections that maintain the security posture of each OZ.*
- *Connections with the PZ must be limited to specific protocols, and connections digitally authenticated.*
- *Confidentiality of any interconnection shall be provided depending on the sensitivity of the information transferred and the route of the connection.*

- *Firewalls shall allow only those protocols necessary to perform a function and only from recognized network origins by denying network traffic by default and allowing network traffic by exception (i.e., deny all, permit by exception).*
- *All communications shall be source authenticated and should be encrypted.*
- *Incoming and outgoing communications shall be limited to data related to the business of the organization, system maintenance data, and any data related to monitoring and audit.*
- *Monitoring and auditing functions shall be enabled on the systems in the OZ, including network components where appropriate, according to the requirements in Sections 5.4 and 6.7.5.*
- *Indications that boundary protections have failed must be dealt with promptly (see Section 5.7).*
- *Wireless Access Points (WAP) should NOT be allowed in the OZ unless the radio frequency can be physically contained with high assurance to systems isolated in the OZ of the building structure.*

6.7.3 Availability

CSP systems shall be configured, operated, and maintained to maximize uptime and availability. Scheduled downtime shall be announced to Users.

Services supporting revocation requests shall be configured and deployed in such a manner and capacity that overall availability shall be maintained at a minimum of <99.9%>, with no single outage lasting longer than <10> minutes. Additionally, such services shall be homed in a minimum of two geographically independent locations with no single-points of failure (SPOFs – e.g., same backbone provider), which could affect availability.

6.7.3.1 Denial of Service Protection

CSPs shall state acceptable methods to request revocation in their CPS. At least one of those methods shall be out of band (i.e. network connectivity is not required).

CSPs shall take reasonable measures to protect Credential request and issuing services from known DoS attacks. The CSP request and issuing availability required by a User application shall be stated in its CPS. CSP shall ensure priority-of-service provisions are enabled for all telecommunication channels. CSP shall also ensure an alternate telecommunication channel is available in the event the primary channel is unavailable.

6.7.3.2 Public Access Protection

Instruction: "Public Access" in this section shall mean widespread, anonymous access.

Personal Identity Information used in the identity proofing process shall be protected at all times in accordance with local law and shall not be available to public access.

Revocation information and CSP Credential information shall be made available in accordance with Section 2 of this CP. However, individual user Credentials need not be made available for public access.

CSPs shall employ firewalls or air-gap procedures to protect privacy-sensitive information from public access.

6.7.4 Communications Security

This section covers three forms of CSP communication: Intra-CSP communications, CSP to RA communications, and RA to User communications. While communications security is necessary across all three forms of communication, the threats, vulnerabilities, and technological capabilities change depending on the environment.

6.7.4.1 Transmission Integrity

Source authentication and integrity mechanisms shall be employed to all Credential request, manufacture, and issuance communications, including all related services irrespective of whether those services are hosted on the same or different platform than the CSP workstation. Communications between CSPs and RAs shall be mutually authenticated to detect changes to information during transmission.

Source authentication for RA to User communications may employ either online (cryptographic) or offline methods. Offline RA to User communications shall be protected by traditional means that are legally sufficient (e.g., ink signatures on paper). Initial User data that has been collected in an unauthenticated or mutable manner shall be verified by the RA before the Credential request is created.

6.7.4.2 Transmission Confidentiality

Intra-CSP communications that cross the physical protection barrier of the Credential-signing portion of the CSP system shall be confidentiality-protected. Services used by the CSP system that are not administered by the CSP administrative staff shall provide protection commensurate with the CP.

Confidentiality of User data shall be maintained. CSP to RA communications shall employ encryption to prevent unauthorized disclosure of information during transmission. The level of protection for RA to User communications shall be determined by the User (or the User's organization); in any case, the RA and CSP shall be prepared to employ typical techniques for Internet confidentiality (e.g., single-side authenticated TLS).

6.7.4.3 Network Disconnect

Network connection lifetimes between co-located services are driven by the traffic between them. Connections should be terminated after a period of inactivity that is defined in the CA's CPS.

Network connections between CAs, RAs, and Users shall be terminated at the end of the session or after a period of inactivity. The length of the period of inactivity is defined in the CA's CPS. Keep-alive and quick-reconnect mechanisms should not be employed, so that message replay and session hijacking are avoided.

6.7.4.4 Cryptographic Key Establishment and Management

Cryptographic key management for network connections between CSPs, RAs and Users includes all aspects of cryptographic key life cycle: key generation, distribution, storage, access and destruction for both symmetric and asymmetric keys.

Key generation and management shall be performed in cryptographic modules that are validated to [FIPS140] Level 1 or higher. Keys that are backed up for business continuity shall have protection comparable to the operational key. All cryptographic key management processes shall be described in the CA's CPS.

RAs shall employ key protection mechanisms implemented in a hardware cryptographic module validated to [FIPS 140], or some other equivalent standard (e.g., smart token).

Keys that protect the integrity and confidentiality of an enrollment session shall be generated and managed using cryptographic mechanisms implemented in a cryptographic module validated to [FIPS 140], or some other equivalent standard.

6.7.4.5 Cryptographic Protection

Cryptographic mechanisms implemented in a cryptographic module validated to [FIPS 140], or some other equivalent standard, shall be employed to detect changes to information during transmission of Intra-CSP communications.

Communications between the CSP and RA systems shall use cryptographic mechanisms that are implemented in a cryptographic module validated to [FIPS 140], or some other equivalent standard.

Cryptographic processes for RA to User communications shall be implemented in a cryptographic module validated to [FIPS 140], or some other equivalent standard.

6.7.4.6 Application Session Authenticity

For stateless connections between CAs, RAs and Users, a unique, random session identifier for each session shall be generated. The session identifiers shall be validated for each request. Session identifiers shall be invalidated at logout to preserve session authenticity. A logout capability shall be provided with an explicit logout message that indicates the reliable termination of authenticated communications sessions. Session identifiers shall be invalidated after <30 minutes> of inactivity.

6.7.5 Network Monitoring

The CSP shall be monitored to detect attacks and indicators of potential attacks. This includes intrusion detection tools.

6.7.5.1 Events and Transactions to be Monitored

The CSP shall identify a list of essential information, transaction types and thresholds that indicate potential attacks. These events should include:

- Bandwidth thresholds
- Inbound and outbound communication events and thresholds
- Unauthorized network services
- CPU usage thresholds
- Credential request thresholds from a single RA
- Access Control thresholds

6.7.5.2 Monitoring devices

A CSP shall deploy intrusion detection tools and other monitoring devices with the CSP to collect intrusion information and at ad hoc locations within the system to track specific types of transactions of interest to the organization. These monitoring devices shall be configurable to react to specific indications of increased risk or to comply with law enforcement requests. The devices shall alert security

personnel when suspected unauthorized activity is occurring. These devices shall be network-based and should be also host-based. Only persons holding trusted roles shall manage the operating state of monitoring devices. The CSP should utilize automated tools to support near real-time analysis of events and these tools should be integrated into access control and flow control mechanisms for rapid response to attacks.

6.7.5.3 Monitoring of Security Alerts, Advisories, and Directives

A CSP shall monitor information system security alerts, advisories, and directives on an ongoing basis. The CSP shall generate and disseminate internal security alerts, advisories, and directives as deemed necessary. The CSP should employ automated mechanisms to make security alert and advisory information available throughout the organization as needed. The CSP shall implement security directives in accordance with established time frames, or notifies the compliance auditor of the degree of noncompliance.

6.7.6 Remote Access/External Information Systems

Instruction: For operational reasons, there may be a need to perform remote management of some CSP resources. The requirements in this section are meant to allow remote management while maintaining the desired security posture. Organizations that decide not to allow remote access to CSP equipment will make that statement here and not include the following subsections.

6.7.6.1 Remote Access

Instruction: The organization should state that remote access to CSP equipment is permitted and the circumstances for which it is permitted here.

6.7.6.2 Bastion Host

All access to CSP signing systems and RA servers shall be mediated by a bastion host (i.e. a machine that presents a limited interface for interaction with the other elements of the CA). No direct access is permitted. The bastion host shall be patched regularly, maintained, and shall only run applications required to perform its duties.

6.7.6.3 Documentation

The CSP shall document allowed methods of remote access to CSP systems, including usage restrictions and implementation guidance for each allowed remote access method.

6.7.6.4 Logging

Logging shall be performed on the bastion host for each remote access session with the CSP, consistent with Section 5.4. In particular, logs shall include date and time of the connection, the authenticated identity of the requestor, the IP address of the remote system and should also include the commands sent to the bastion host. Logs shall be maintained on a corporate audit server.

6.7.6.5 Automated Monitoring

Automated monitoring shall be performed on all remote sessions with the bastion host, and on all interactions between the bastion host and other CSP systems. Upon detection of unauthorized access, the CSP shall terminate the connection and log the event.

6.7.6.6 Security of Remote Management System

Machines used for remote access to the CSP system shall be either corporately managed (including patching) or shall be a machine dedicated to that purpose. In particular, it shall not be used as a personal machine for the remote user. The machine shall be maintained at the same level as the machines that it accesses (i.e. all policies on patching, virus scanning, etc. that are levied on the target systems shall apply to this machine as well). The CSP should make use of Network Access Control technology to check the security posture of the remote machine prior to connecting it to the network. Remote Management of the CSP system shall be the only use of Remote Access.

6.7.6.7 Authentication

Any machine used to access CSP systems remotely shall require two or more factors of authentication. In particular, a hardware token shall be required. Authentication shall occur between the remote machine and the bastion host.

6.7.6.8 Communications Security for Remote Access

All communications between the remote access host and the CSP system shall be protected by [FIPS 140], or some other equivalent standard, validated cryptography, as required for CSP to RA communications in Section 6.7.4.5. Session identifiers shall be invalidated at logout to preserve session authenticity, as described in section 6.7.4.6, Session Authentication.

6.7.7 Penetration Testing

Penetration testing exercises both physical and logical security controls. Regularly performing this testing will allow a CSP to mitigate and avoid vulnerabilities in their systems.

The CSP System shall <biannually>, or whenever major system changes occur, conduct external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems. Penetration testing shall occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.

A standard method for penetration testing consists of:

- pretest analysis based on full knowledge of the target system;
- pretest identification of potential vulnerabilities based on pretest analysis;
- testing designed to determine exploitability of identified vulnerabilities.

Detailed rules of engagement shall be agreed upon by all parties before the commencement of any penetration testing scenario. These rules of engagement are correlated with the tools, techniques, and procedures that are anticipated to be employed by threat-sources in carrying out attacks. An organizational assessment of risk guides the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing. Vulnerabilities uncovered during penetration testing shall be incorporated into the vulnerability remediation process.

6.8 Time-Stamping

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

7 Credential, CRL, and OCSP Profiles

7.1 Assertion Profiles

Assertions issued by a CSP under this policy shall conform to:

SAML: http://xml.coverpages.org/Federal-ICAMSC-SAML-20-Profile-Draftv010-36529.pdf

OpenID Connect: https://openid.net/specs/openid-connect-basic-1_0-28.html

7.1.1 Version Numbers

CSPs shall support OAuth2.0 and OpenID Connect version 1.0. CSPs may support multiple SAML versions

7.1.2 Credential Extensions

7.1.3 Algorithm Identifiers

7.1.4 Name Forms

Refer to Assertion Signing Certificate Profile.

7.1.5 Name Constraints

Refer to Assertion Signing Certificate Profile.

7.1.6 Credential Policy Object Identifier

Credentials issued under this CP shall assert the following OID(s):

Refer to section 1.2

7.1.7 Usage of Policy Constraints Extension

Refer to Assertion Signing Certificate Profile.

7.1.8 Policy Qualifiers Syntax and Semantics

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Relying parties should employ the following steps when verifying an assertion signed with an Assertion Signing Certificate:

1. Observe the OIDs (section 1.2) present in the assertion meet the security requirements for the system
2. Authenticate the assertion per RFC 6749, or appropriate SAML specifications
3. Validate the chain of trust of the assertion signing certificate per RFC 5280 back to a known and trusted Trust Anchor.

4. Validate that one or more OIDs in the assertion signing certificate match the OIDs present in the assertion
5. If steps 1-4 are successful, the assertion can be trusted.

7.2 CRL Profile
No stipulation.

7.3 OCSP Profile
No stipulation.

8 Compliance Audit and Other Assessments
CSPs shall have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced.

8.1 Frequency or Circumstances of Assessment

8.2 Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CSP's CPS and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a digital identity subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor either shall be a private firm that is independent from the entities (CSP and RAs) being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. To insure independence and objectivity, the compliance auditor must not have served the entity in developing or maintaining the entity's CSP Facility or Credential practices statement. The Policy Authority shall determine whether a compliance auditor meets this requirement.

8.4 Topics Covered by Assessment

The purpose of a compliance audit is to verify that a CSP and its recognized RAs comply with all the requirements of the current versions of the CSP's CPS. All aspects of the CSP/RA operation shall be subject to compliance audit inspections.

8.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the CSP system, the following actions shall be performed:

- The compliance auditor shall note the discrepancy
- The compliance auditor shall notify the parties identified in section 8.6 of the discrepancy
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the appropriate Authorities, as defined in Section 1.3.1.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Policy Authority may decide to temporarily halt operation of the CSP or RA, to revoke a Credential issued to the CSP or RA, or take other actions it deems appropriate. The Policy Authority shall provide to the CSP.

8.6 Communication of Results

An Audit Compliance Report shall be provided to the entity responsible for CSP operations. The Audit
Compliance Report and identification of corrective measures shall be provided to the appropriate Authorities within <30> days of completion. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Credential Issuance or Renewal Fees

9.1.2 Credential Access Fees

9.1.3 Revocation or Status Information Access Fees

9.1.4 Fees for other Services

9.1.5 Refund Policy

9.2 Financial Responsibility

This CP contains no limits on the use of Credentials issued by CSP under the policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for Credentials used to consummate a transaction.

9.2.1 Insurance Coverage

Instruction: Organizations whose CSP services are insured against loss/liability claims will describe that coverage here. Alternatively, this may be "Not Applicable".

9.2.2 Other Assets

Instruction: Any other assets associated with the CSP service that may be included in a financial settlement should be described here. Otherwise, this section is "Not Applicable."

9.2.3 Insurance or Warranty Coverage for End-Entities

Instruction: CSP service organization will describe any insurance or warranty coverage provided to user organizations and individuals. If none, this section may be noted as such.

9.3 Confidentiality of Business Information

The CSP shall protect the confidentiality of sensitive business information stored or processed on CSP systems that could lead to abuse or fraud. For example, the CSP shall protect customer data that could allow an attacker to impersonate a customer.

Public access to CSP organizational information shall be determined by the CA.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The CSP shall develop, implement and maintain a privacy plan. The privacy plan shall document what personally identifiable information is collected, how it is stored and processed, and under what conditions the information may be disclosed. The privacy plan shall also contemplate the use of PII and biometrics when used for fraud prevention, or other purposes explicitly authorized by the User and how privacy risk and overexposure of data is mitigated in such circumstances.

9.4.2 Information Treated as Private

CSPs shall protect all user personally identifiable information from unauthorized disclosure. Records of individual transactions may be released upon request of any users involved in the transaction or their legally recognized agents. The contents of the archives maintained by CSPs operating under this policy shall not be released except as allowed by the privacy plan.

9.4.3 Information not Deemed Private

9.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely, and may be released only in accordance with other stipulations in section 9.4.

9.4.5 Notice and Consent to Use Private Information

The CSP may only release private information about a User following explicit consent obtained from the authenticated User except when observing the stipulations of section 9.4.6 or other relevant sections of this CP.

CSP shall not deny a User's access to its services solely on the User's unwillingness to consent to sharing their data with other participants (i.e. sharing with advertising agencies).

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The CSP shall not disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

Instruction: If there are additional circumstances not already covered that might cause an organization operating a PKI to disclose sensitive or private information, it should be described here. Otherwise this section may be "Not Applicable" or "None."

9.5 Intellectual Property Rights

The CSP shall not knowingly violate intellectual property rights held by others.

9.6 Representations and Warranties

9.6.1 CSP Representations and Warranties

CSPs operating under this policy shall warrant that their procedures are implemented in accordance with this CP, and that any Credentials issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this policy.

A CSP that issues Credentials that assert a policy defined in this document shall conform to the stipulations of this document, including—

- Providing a CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance to the stipulations of the CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS.
- Including only valid and appropriate information in Credentials, and maintaining evidence that due diligence was exercised in validating the information contained in the Credentials.
- Revoking the Credentials of users found to have acted in a manner counter to their obligations in accordance with section 9.6.3.
- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.

9.6.2 RA Representations and Warranties

An RA that performs registration functions as described in this policy shall comply with the stipulations of this policy, and comply with a CPS approved by the Policy Authority for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy shall conform to the stipulations of this document, including—

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in Credential requests, and maintaining evidence that due diligence was exercised in validating the information contained in the Credential.
- Ensuring that obligations are imposed on users in accordance with section 9.6.3, and that users are informed of the consequences of not complying with those obligations.

9.6.3 User Representations and Warranties

A user (or AOR for device Credentials) shall be required to acknowledge acceptance of the requirements the user shall meet respecting protection of secret keys and use of the Credential before being issued the Credential.

Users shall—

- Accurately represent themselves in all communications with the authorities defined in section 1.3.
- Protect their authenticators at all times, in accordance with this policy, as stipulated in their Credential acceptance agreements and local procedures.
- Promptly notify the appropriate CSP upon suspicion of loss or compromise of their authenticator(s). Such notification shall be made directly or indirectly through mechanisms consistent with the CSP's CPS.

- Abide by all the terms, conditions, and restrictions levied on the use of their authenticator(s) and Credential(s).

9.6.4 Relying Parties Representations and Warranties

Instruction: This CP does not specify the steps a relying party should take to determine whether to rely upon a Credential. The relying party decides, pursuant to its own policies, what steps to take. The CSP merely provides the tools (i.e., Credentials and CRLs) needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination. Describe in this section any representations and warranties the CSP is required to make to relying parties. If none are required, state 'Not Applicable'.

9.6.5 Representations and Warranties of Other Participants

Instruction: If a PKI implementation has additional participants not covered by the other subsections of 9.6 who nevertheless need to be held to particular behavioral standards (representations and warranties), they should be described here. Otherwise this section may be marked "Not Applicable" or "None".

9.7 Disclaimers of Warranties

CSPs operating under this policy shall not disclaim any responsibilities described in this CP.

9.8 Limitations of Liability

Instruction: Organizations determining whether to "trust" a CSP and associated PKI if applicable, will generally look at this section to determine the degree of responsibility a CSP is willing to take for its actions. Appropriate text for this section may include:

- *A statement that liability and the limitation thereof will be set forth in applicable agreements between the CSP and its affiliates/customers/etc.*
- *A statement to the effect that the CSP shall not be liable for any indirect damages of any kind, including consequential, incidental, special, punitive, or other damages whatsoever arising out of or related to the CP, even if advised of the possibility of such damages.*

- *A statement limiting liability to direct damages actually incurred as a result of improper actions by the CSP or CSP personnel and limited to <monetary amount> per incident (misuse relating to a failure on the part of the CSP due to a particular occurrence of negligence, regardless of the number of relying parties (claimants) involved).*

9.9 Indemnities

Instruction: When organizations seek to establish trust relationships with external organizations, there may be need to establish indemnification clauses to protect the parties to the trust relationship. In some situations where there are contractual agreements, indemnity may be contained in the contractual language, otherwise it may be provided in this section.

9.10 Term and Termination

9.10.1 Term

Instruction: This section documents the term for which the CP is effective.

9.10.2 Termination

Instruction: This section documents under what conditions the CP may be terminated.

9.10.3 Effect of Termination and Survival

The requirements of this CP shall remain in effect through the end of the archive period for the last Credential issued.

9.11 Individual Notices and Communications with Participants

The Policy Authority shall establish appropriate procedures for communications with CSPs operating under this policy via contracts or memoranda of agreement as applicable.

9.12 Amendments

9.12.1 Procedure for Amendment

The Policy Authority shall review this CP at least once every year. Corrections, updates, or changes to this CP shall be publicly available. Suggested changes to this CP shall be communicated to the contact in section 1.5.2; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2 Notification Mechanism and Period

Whenever the CP is amended, it shall be published within <30> days of the date the amendment took place and all known concerned parties (OA staff, relying parties, users, etc.) shall be notified.

9.12.3 Circumstances under which OID must be Changed

Instruction: Describe in this section whether this is required, and any other circumstances requiring OID change. OIDs should be changed if there is a change in the CP that reduces the level of assurance provided.

9.13 Dispute Resolution Provisions

The Policy Authority shall facilitate the resolution between entities when conflicts arise as a result of the use of Credentials issued under this policy.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of <the governing jurisdiction> shall govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions.

9.15 Compliance with Applicable Law

All CSPs operating under this policy shall comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Instruction: Any business or legal provisions pertaining to the CSP that have not been covered previously in Section 9 should be identified here. Otherwise this may be "Not" Applicable or "None."

9.16.2 Assignment

Except where specified by contract, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the other party (such consent not to be unreasonably withheld), except that <PKI organization> may assign and delegate this CP to any party of its choosing.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

Instruction: Organizations will include language here pertaining to the waiver of rights. For example: "Any failure to exercise any right hereunder shall not be construed as a relinquishment of any future exercise of such right."

9.16.5 Force Majeure

Instruction: Organizations will include language here specifying extreme conditions under which the PKI will not be liable.

9.17 Other Provisions

CSP shall Establish agreements and procedures with entities involved in the supply chain for the system, system components, or system services in support of notification of supply chain compromises, results of assessments and audits, or other information deemed appropriate by the Supply Chain Risk Management Team defined in section 6.6.1.

Appendix A—Acronyms

Selected acronyms and abbreviations used in the guide are defined below.

AOR	Authorized Organizational Representative
CA	Certificate Authority
CSP	Credential Service Provider
COMSEC	Communications Security
CP	Credential Policy
CPS	Credential Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Registry
CSS	Certificate Status Server
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS PUB	(US) Federal Information Processing Standards Publication
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IS	Information System
LAN	Local Area Network
ISO	International Organization for Standardization
ITU-T	International Telecommunications Union – Telecommunications Sector
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OZ	Operations Zone
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure

PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA	Secure Hash Algorithm
SP	Special Publication
TAM	Trust Anchor Manager
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
UUID	Universal Unique Identifier
VPN	Virtual Private Network
WAP	Wireless Access Point

Appendix B—Glossary

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock authenticators).
Agent	A person authorized to act on behalf of another person.
Anonymous	Having an unknown name.
Archive	Long-term, physically separate storage.

Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Authorized Organizational Representative (AOR)	A person (potentially among several) within an organization who is authorized to vouch for non-person identities. Any particular AOR is not permanently linked to any particular non-person identity; the CSP must only ascertain that the AOR is legitimately associated with the organization, and that the AOR is identified as having authority for the identity in question.
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Bastion Host	A special purpose computer on a network specifically designed and configured to withstand attacks.
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Credential	The combination of an authenticator bound to a User and the generation of an assertion of identity following a successful authentication event by the User to the CSP. The term “credential” used in the context of this policy assumes the CSP manages and validates the identity data that appears in identity assertions signed by the CSP in conformance with the stipulations of this policy.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key Credentials and CRLs.
CSP Facility	The collection of equipment, personnel, procedures and structures that are used by a certification authority to perform Credential issuance and revocation.
CSP Operating Staff	CSP components are operated and managed by individuals holding trusted, sensitive roles.

Credential Policy (CP)	A Credential policy is a specialized form of administrative policy tuned to electronic transactions performed during Credential management. A Credential policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of public key Credentials. Indirectly, a Credential policy can also govern the transactions conducted using a communications system protected by a Credential-based security system. By controlling critical Credential extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CSP employs in issuing, suspending, revoking, and renewing Credentials and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
CPS Summary	A publically releasable version of the CPS.
Credential-Related Information	Information, such as a user's postal address, that is not included in a Credential. May be used by a CSP managing Credentials.
Credential Revocation List (CRL)	A list maintained by a certification authority of the Credentials that it has issued that are revoked prior to their stated expiration date.
Credential Status Server (CSS)	A trusted entity that provides on-line verification to a relying party of a subject Credential's revocation status, and may also provide additional attribute information for the subject Credential.
Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Credential	A Credential used to establish a trust relationship between two certification authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140]

Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital Credential; and (2) whether the message has been altered since the transformation was made.
End Entity Credential	A Credential in which the subject is not a CSP (also known as a user Credential).
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CSP	A CSP that is subordinate to another CSP, and has a CSP subordinate to itself.
Key Escrow	A deposit of the private key of a user and other pertinent information pursuant to an escrow agreement or similar contract binding upon the user, the terms of which require one or more agents to hold the user's private key for the benefit of the user, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Management Key	Key exchange, key agreement, key transport
Key Pair	Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (2) even knowing the public key, it is computationally infeasible to discover the private key.
Key Rollover Credential	The Credential that is created when a CSP signs a new public key for itself with its old private key, and vice versa
Modification (of a Credential)	The act or process by which data items bound in an existing public key Credential, especially authorizations granted to the subject, are changed by issuing a new Credential.

Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Federal PKI, OIDS are used to uniquely identify Credential policies and cryptographic algorithms.
Online Credential Status Protocol	Protocol which provides on-line status information for Credentials.
Operations Zone (OZ)	Network area containing systems for routine business operations.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring on-line).
Policy Authority (PA)	Body established to oversee the creation and update of Credential policies, review certification practice statements, review the results of CSP audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI Credential policies.
Privacy	Restricting access to user or relying party information in accordance with Federal law.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Pseudonym	A user name that has been chosen by the user that is not verified as meaningful by identity proofing. [NS4009]
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital Credential.

Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering Credentials and public/private key pairs, including the ability to issue, maintain, and revoke public key Credentials.
Public Zone (PZ)	Network area that is not behind a protective boundary controlled by the organization.
Registration Authority (RA)	An entity that is responsible for identification and authentication of Credential subjects, but that does not sign or issue Credentials (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a Credential)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new Credential that contains the new public key.
Relying Party	A person or entity who has received information that includes a Credential and a digital signature verifiable with reference to a public key listed in the Credential, and is in a position to rely on them.
Renew (a Credential)	The act or process of extending the validity of the data binding asserted by a public key Credential by issuing a new Credential.
Repository	A database containing information and data relating to Credentials as specified in this CP; may also be referred to as a directory.
Restricted Zone (RZ)	Controlled network area for sensitive data processing and storage
Revoke a Credential	To prematurely end the operational period of a Credential effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Root CSP	In a hierarchical PKI, the CSP whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Audit Administrator	An individual (e.g. employee, contractor, consultant, 3rd party) who is responsible for auditing the security of CSPs or Registration Authorities (RAs), including reviewing, maintaining, and archiving audit logs; and performing or overseeing internal audits of CSPs or RAs. A single individual may audit both CSPs and RAs. Audit Administrator is an internal role that is designated as trusted.
Server	A system entity that provides a service in response to requests from clients.

Signature Credential	A public key Credential that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Special Access Zone (SAZ)	Highly controlled network area for processing and storage of especially high value data.
Subordinate CSP	In a hierarchical PKI, a CSP whose Credential signature key is certified by another CSP, and whose activities are constrained by that other CA. (See superior CA).
User	A user is an entity that (1) is the subject named or identified in a Credential issued to that entity, (2) holds an authenticator that corresponds to their Credential, and (3) does not itself issue Credentials to another party. This includes, but is not limited to, an individual, an application or network device.
Superior CSP	In a hierarchical PKI, a CSP that has certified the Credential signature key of another CSP, and that constrains the activities of that CA. (See subordinate CA).
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of Trusted Credentials used by relying parties to authenticate other Credentials.
Trust Zone	The level of security controls in a network segment.
Trusted Agent	Entity authorized to act as a representative of a CSP in confirming user identification during the registration process. Trusted agents do not have automated interfaces with certification authorities.
Trust Anchor Manager	Authorities who manage a repository of trusted Root CSP Credentials. They act on behalf of relying parties, basing their decisions on which CSPs to trust on the results of compliance audits. A TAM sets requirements for inclusion of a CA's root public key in their store. These requirements are based on both security and business needs. The TAM has a duty to enforce compliance with these requirements, for example, requirements around the supply of audit results, on initial acceptance of a root, and on an ongoing basis. TAMs will follow their normal practice of requiring CSPs to submit an annual audit report.
Trusted Credential	A Credential that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted Credentials are used to start certification paths. Also known as a "trust anchor".

Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two 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. [NS4009]
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140]
Zone Boundary	The limit of authority over the security of the data processed within the boundary.

Appendix C—References

ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html
CABF Base	CSP Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Credentials, v.1.1, 14 Sep 2012. https://www.cabforum.org/Baseline_Requirements_V1_1.pdf
CABF EV	Guidelines for the Issuance and Management of Extended Validation Credentials, version 1.4, 29 May 2012. https://www.cabforum.org/Guidelines_v1_4.pdf
CCP-PROF	X.509 Credential and Credential Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program. http://www.idmanagement.gov/fpkipa/documents/CertCRLprofileForCP.pdf
CIMC	Credential Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001. http://csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf
E-Auth	E-Authentication Guidance for Federal Agencies, M-04-04, December 16, 2003. http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
FIPS 140	Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-4	Digital Signature Standard (DSS), FIPS 186-4, July 2013. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html
ISO9594-8	ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute Credential frameworks.
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html

NAG69C Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NSD42 National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)

NS4005 NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PACS *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 30, 2004. http://www.idmanagement.gov/smartcard/information/TIG_SCEPACS_v2.2.pdf

PKCS#1 Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003. http://www.ietf.org/rfc/rfc3447.txt

PKCS#12 PKCS 12 v1.0: Personal Information Exchange Syntax-June 24, 1999. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf

RFC 2119 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt

RFC 2560 X.509 Internet Public Key Infrastructure: Online Credential Status Protocol – OCSP, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, June 1999. http://www.ietf.org/rfc/rfc2560.txt

RFC 2822 Internet Message Format, Peter W. Resnick, April 2001. http://www.ietf.org/rfc/rfc2822.txt

RFC 3647 Credential Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003. http://www.ietf.org/rfc/rfc3647.txt

RFC 4122 A Universally Unique IDentifier (UUID) URN Namespace, Paul J. Leach, Michael Mealling, and Rich Salz, July 2005. http://www.ietf.org/rfc/rfc4122.txt

RFC 5280 Internet X.509 Public Key Infrastructure Credential and Credential Revocation List (CRL) Profile, D. Cooper etal, May 2008, http://www.ietf.org/rfc/rfc5280.txt

SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-37, May 2004. http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf

SP 800-63-3 Digital Identity Guidelines, NIST Special Publication 800-63-3, June 2017. https://pages.nist.gov/800-63-3

SP 800-88 NIST Special Publication 800-88: Guidelines for Media Sanitization http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

SP 800-53 NIST Special Publication 800-53: Recommendation for Security Controls for Federal Information Systems and Organizations http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3final_updated-errata_05-01-2010.pdf

SP 800-61 NIST Computer Security Incident Handling Guide, Rev 2. National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

SP 800-57 NIST Special Publication 800-57 Rev 3, Recommendation for Key Management stpubs/800-61/sp800-61-revised2_Aug-2012.pdfndards and Technology http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

SSP REP Shared Service Provider Repository Service Requirements. Federal PKI Policy Authority Shared Service Provider Working Group, December 13, 2011. http://www.idmanagement.gov/fpkipa/documents/SSPrepositoryRqmts.doc

SP 800-147 NIST Special Publication 800-147, BIOS Protection Guidelines. April 2011. http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf

SP 800-147B NIST Special Publication 800-147b, BIOS Protection Guidelines for Servers (Draft). July 2012. http://csrc.nist.gov/publications/drafts/800-147b/draft-sp800147b_july2012.pdf