North American Energy Standards Board
801 Travis, Suite 1675, Houston, Texas 77002
Phone: (713) 356-0060, Fax: (713) 356-0067, E-mail: naesb@naesb.org
Home Page: www.naesb.org

NAESB Accreditation Requirements for Certification Authorities

1. INTRODUCTION

1.1. About this Document

This document provides technical and management details which a certification authority is required to meet in order to be accredited as an Authorized Certification Authority (ACA) by NAESB. An ACA is expected to illustrate compliance with this standard within a Certification Practice Statement. The following ~~standard is is~~requirements are intended to apply to NAESB WEQ Business Practice Standards that employ PKI technology.

1.2. Definitions

1.2.1. Authorized Certification Authority (ACA): A Certificate Authority that has successfully completed the NAESB ACA certification process

1.2.2. Certificate Authority (CA): The CA manages the certificate life cycle, which includes generation and issuance, distribution, renewal, rekey, and revocation of certificates.

1.2.3. Registration Authority (RA): The RA is the entity responsible for the identification and authentication of subscribers, but does not sign or issue certificates.

1.2.4. Local Registration Authority (LRA): A delegation of the RA function by the CA to external registration authorities that may or may not be part of the same legal entity as the CA. For example, ~~A~~ a customer of a CA may arrange with that CA to perform the RA function itself or use its agent.

1.2.5. RA Operations/Functions: The identification and authentication of subscribers.

1.2.6. CA Operations/Functions: The management of the certificate life cycle, which includes generation and issuance, distribution, renewal, rekey, and revocation of certificates.

1.2.7. Critical CA Operations/Functions: The management of the certificate life cycle, which includes generation and issuance, distribution, renewal, rekey, and revocation of the CA's root and subordinate private keys.

1.3. Certificate Usage

1.3.1. Appropriate Certificate Uses

A certificate can be used for protecting information of varying sensitivity. As such, an ACA should have the ability to provide certificates at a number of assurance levels. The assurance level determines the ACA's overall confidence in the end entity's identity. An ACA will be responsible for providing one or more of the following assurance levels:

Assurance Level	Description
Rudimentary	This level provides the lowest degree of assurance concerning the identity of the end entity. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are

Comment [PS1]: OATI believes "requirements" is a better word choice here since this document identifies the requirements to be met by CAs.

Comment [PT2]: OATI believes "Applicant" and "Subscriber" should be defined. Subscribers would include people, roles, or devices.

Comment [PT3]: OATI believes the Assurance Levels are to vaguely worded to be enforced and should be replaced by tighter levels of identity proofing based on key usage (Signature, encryption, etc.), Enhanced Key Usage (Server Authentication, Client Authentication ,etc.), and type of certificate recipient (Person, role, device, etc.)

Comment [PS4]: OATI proposes alternate wording because as written it seemed to indicate a CAs requirement to offer them all.

Comment [PT5]: OATI believes the "Rudimentary" level should be removed or significantly clarified (i.e. to show its use should only be within an organization) to prevent misuse and confusion. Its stated primary function "is to provide data integrity to the information being signed" however throughout this document all safeguards were removed. (E.g. no stipulation for Intervals for CRL Issuance, only one person is required per task or to access CA private keys,

	unavailable.
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this assurance level that users are not likely to be malicious.
Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
High	This level is reserved for those environments where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

1.4. Requirements Administration

1.4.1. Organization Administering the Document

NAESB is responsible for the creation, modification, and all other aspects of ACA accreditation requirements.

1.4.2. Contacting NAESB

Questions regarding these standards may be directed to the NAESB office.

1.4.3. ACA Candidate Accreditation Procedures

The ACA candidate should submit the results of a WebTrust CA audit, or similar audit by an independent auditor with expertise in CA operations, as evidence of compliance with these accreditation requirements to NAESB per requirements stated in the approved NAESB Certification Program for Authorized Certification Authorities. NAESB will review the submitted materials and provide an accreditation decision in writing to the ACA candidate. The ACA candidate should meet all facets of this policy.

Comment [PS6]: OATI feels this section should state that the prospective ACA must submit all materials and evidence and meet all the requirements as stated in the approved NAESB Certification Program for Authorized Certification Authorities. This seems to take on that responsibility within this document rather than incorporating by reference the requirements of the board approved Certification Program.

2. IDENTIFICATION & AUTHENTICATION

2.1. Naming

2.1.1. Types of Names

The ACA shall only generate and sign certificates that contain a non-null subject Distinguished Name (DN). This applies to all assurance levels. The table below summarizes the naming requirements that apply to each level of assurance.

Assurance Level	Naming Requirements
Rudimentary	Non-Null Subject Name, or Null Subject Name if Subject Alternative Name is populated and marked critical
Basic	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical

Medium	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
High	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical

2.1.2. Need for Names to be Meaningful

Names used in the certificates issued by the ACA must identify the person or object to which they are assigned. When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading. When User Principal Names (UPNs) are used, they must be unique and accurately reflect organizational structures.

2.1.3. Anonymity or Pseudonymity of Subscribers

The ACA shall not issue anonymous certificates. Pseudonymous certificates may be issued by the ACA to support internal operations. CA certificates issued by the ACA shall not contain anonymous or pseudonymous identities.

2.1.4. Uniqueness of Names

The ACA is responsible for ensuring name uniqueness in certificates issued by the ACA. Name uniqueness is not violated when multiple certificates are issued to the same entity as long as each subject string is unique.

2.2. Initial Identity Validation

2.2.1. Authenticity of Organization Identity

Requests for Subscriber certificates in the name of an affiliated organization shall include the organization name, address, and documentation of the existence of the organization.

The ACA or RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

2.2.2. Authentication of Subscribers

An Authorized Certification Authority may elect to perform Registration Authority (RA) functions in-house or choose to delegate some, or all, RA functions to other parties that are separate legal entities from the ACA. In both cases the party or parties performing RA functions are subject to the obligations for identity proofing, auditing, logging, protection of subscriber information, record retention and other aspects germane to the RA function contained in this business process standard. All RA infrastructure and operations performing RA functions shall be held to this standard as incumbent upon the CA when performing in-house RA functions. The ACA and/or delegated entity are responsible for ensuring that all parties performing RA functions understand and agree to conform to this standard.

For Subscribers, the ACA, and/or associated RAs shall ensure that the applicant's identity information is verified in accordance with the process established by the applicable CP and CPS. Process information shall depend upon the certificate level of assurance and shall be addressed in these requirements. The documentation and authentication requirements shall vary depending upon the level of assurance.

The authentication requirements to be used are defined by NIST SP800-63 version 1.0.2 section *7.2.1 Registration of Identity Proofing Requirements*[1] using the following mappings:

Comment [PS7]: OATI feels this needs to be a defined term or incorporated by reference to an applicable standard or RFC.

Comment [P8]: Although OATI agrees with this from a pure security standpoint the use of pseudonymous or "Role" certificates is common within the industry.

Comment [PT9]: OATI feels perhaps a clarification should be added which states "The Subject fields within all certificates issued by the ACA must be unique (i.e. Two Joe Smith certificates could have the exact same Common Name but different OU fields would make them unique).

Comment [PS10]: As mentioned in comment #1, OATI feels this needs to be a defined term or incorporated by reference to an applicable standard or RFC.

Comment [PT11]: OATI proposes wording change to: "…other aspects of the RA function contained in this Accreditation Requirements document…."

[1] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

Table 1. Identity Proofing Requirements by Assurance Level

	In-Person	Remote
Level 2		
Basis for issuing credentials	Possession of a valid current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport)	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number.
RA actions	Inspects photo-ID, compare picture to applicant, record ID number, address and DoB. If ID appears valid and photo matches applicant then: a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record.	• Inspects both ID number and account number supplied by applicant. Verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. • Address confirmation and notification: a) Sends notice to an address of record confirmed in the records check or; b) Issues credentials in a manner that confirms the address of record supplied by the applicant; or c) Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at number or e-mail address associated with the applicant in records.
Level 3		
Basis for issuing credentials	Possession of verified current primary Government Picture ID that contains applicant's picture and either address of	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number

	In-Person	Remote
	record or nationality (e.g. driver's license or passport)	(e.g., checking account, savings account, loan or credit card) with confirmation via records of both numbers.
RA actions	Inspects Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address and other personal information in record are consistent with the application. Compare picture to applicant, record ID number, address and DoB. If ID is valid and photo matches applicant then: a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record	• Verifies information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. • Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.
Level 4		
Basis for issuing credentials	In-person appearance and verification of two independent ID documents or accounts, meeting the requirements of Level 3 (in-person and remote), one of which must be current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport), and a new recording of a biometric of the applicant at the time of application	Not Applicable
RA actions	• *Primary Photo ID:* Inspects Photo-ID and verify via the issuing government agency,	Not applicable

	In-Person	Remote
	compare picture to applicant, record ID number, address and DoB. • *Secondary Government ID or financial account* a) Inspects Photo-ID and if apparently valid, compare picture to applicant, record ID number, address and DoB, or; b) Verifies financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. • *Record Current Biometric* Record a current biometric (e.g. photograph or fingerprints to ensure that applicant cannot repudiate application. • *Confirm Address* Issue credentials in a manner that confirms address of record.	

At Level 2, employers and educational instructors who verify the identity of their employees or students by means comparable to those stated above for Level 2 may elect to become an RA or CSP and issue credentials to employees or students, either in-person by inspection of a corporate or school issued picture ID, or through on-line processes, where notification is via the distribution channels normally used for sensitive, personal communications.

At Level 2, financial institutions subject to the supervision of the Department of Treasury's Office of Comptroller of the Currency may issue credentials to their customers via the mechanisms normally used for on-line banking credentials and may use on-line banking credentials and tokens as Level 2 credentials provided they meet the provisions of Section 8.

In some contexts, agencies may choose to use additional knowledge-based authentication methods to increase their confidence in the registration process. For example, an applicant could be asked to supply non-public information on his or her past dealing with the agency that could help confirm the applicant's identity.

NIST Assurance Level	NAESB Assurance Level
Level 1	Rudimentary
Level 2	Basic
Level 3	Medium
Level 4	High

The ACA and/or RAs shall record the information set forth below for issuance of each certificate:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law. The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued;
- If in-person identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date of the verification;
- The Assurance Level at which the associated certificate will be issued; and
- For all Assurance Levels, except Rudimentary, a declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

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

For the High Assurance Level: Identity is established by an in-person appearance before the Registration Authority or Trusted Agent; the information provided shall be checked to ensure legitimacy. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Driver's License).

2.3. Identification and Authentication for Reissuance Requests

2.3.1. Identification and Authentication for Routine Reissuance

Subscribers of ACAs shall identify themselves for the purpose of reissuing as required in the table below.

Comment [PS12]: OATI feels this needs to be a defined term or incorporated by reference to an applicable standard or RFC.

Comment [PS13]: OATI believes this should be consistent with Section 3.6. OATI does not think these provisions were intended to only apply to reissuance which is new key pair with same validity period.

Also, sections 3.4, 3.5 and 3.6 need to carefully spell out the differences between Renew, Reissue, and Rekey.

Assurance Level	Identity Requirements
Rudimentary	Identity may be established through use of current signature key.
Basic	Identity may be established through use of current signature key, except that identity shall be reestablished through initial registration process at least once every five years from the time of initial registration.
Medium	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every three years from the time of initial registration.
High	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least annually.

2.3.2. Identification and Authentication for Reissuance after Revocation

After a certificate has been revoked other than during a renewal or update action, the subscriber is required to go through the initial registration process described elsewhere in this document to obtain a new certificate.

2.3.3 Re-verification and Revalidation of Identity When Certificate Information Changes

If at any point any subject name information embodied in a certificate issued by a CA is changed in any way, the identity proofing procedures outlined in this standard must be re-performed and a certificate issued with the validated information.

Comment [P14]: OATI believes most "High" certificates will be issued to "Roles" or "Devices" and as such are the least probable to have the identity change. Thus perhaps text to indicate role or device certificates are exceptions and can have a longer re-registration period may be in order.

Comment [P15]: OATI believes this phrase should be deleted.

Comment [PT16]: OATI believes this is extra stringent as most certificates are revoked for lost/compromised keys… not a change in identity. As long as subject name information remains the same there should not be a need for re-authentication.

3. CERTIFICATE LIFECYCLE

3.1. Issuance

The ACA will verify the RA digital signature of the certificate signing request prior to issuance. CA certificates created by the ACA shall be checked to ensure that all fields and extensions are properly populated.

3.2. Certificate Acceptance

Submission of a public key for signing by the ACA explicitly indicates acceptance of the subscriber agreement.

3.3. Key Pair and Certificate Usage

3.3.1. Subscriber Private Key and Certificate Usage

For High, Medium, and Basic Assurance, subscribers shall protect their private keys from access by other parties in accordance with the assurance level requirements specified elsewhere in this standard.

Restrictions in the intended scope of usage for a private key are specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

3.3.2. Relying Party Public Key and Certificate Usage

ACA-issued certificates specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. The ACA issues Certificate Revocation Lists (CRLs) specifying the current status of all unexpired ACA certificates.

3.4. ACA & Subscriber Certificate Rekey

Certificate rekey consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key. Rekeying of certificates is considered an insecure practice and increases the size of CRLs and thus is not allowed under this standard. After certificate renewal, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

3.4.1. Circumstance of Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must meet the requirements specified elsewhere in this document.

3.4.2. Processing Certificate Renewal Requests

The ACA may process certificate renewal requests only if the chain of trust has not been compromised. Generally, it is not advisable to perform certificate renewals as opposed to certificate re-key operations. Renewals may be performed if the subscriber certificate has been lost, but the associated private and public key pair has not been compromised.

3.5. ACA Certificate Renewal and Reissuance

Renewing an ACA certificate consists of creating new certificates with a different public and private key pair and serial number while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, CRL distribution point, and/or be signed with a different key. The renewal of a certificate does not require a change to the Subject Name and does not violate the requirement for name uniqueness. Reissuing is exactly the same as renewing a

Comment [PS17]: OATI believes use of the terms re-key, renewal, reissuance etc. in sections 3.4, 3.5 and 3.6 is very confusing. OATI believes the confusion can be addressed by using definitions used by the industry or within RFC 5280, but not both. (E.g. renewal means new keys based on industry practice but same keys in the RFC)

This section also appears to apply to the ACA certs in addition to the Subscriber certs. Is it appropriate for the ACA when you have section 3.5 that explicitly applies to ACA certs?

OATI believes the sections dealing with "Reissuance" need to be rewritten to be more clear and accurate.

Comment [PS18]: OATI believes this section should be moved to 3.6 to be consistent with section 3.5. Also, please address circumstance and process for renewal in 3.6 and delete 3.4.1 and 3.4.2.

Comment [PS19]: OATI believes this is inconsistent with 3.4.

Comment [PS20]: OATI believes the sections dealing with "Reissuance" need to be rewritten to be more clear and accurate.

Comment [PT21]: OATI believes this definition of renewing is industry practice and should replace the first two sentences in section 3.4.

certificate with the exception that the validity period end date remains the same as the old certificate which is being issued.

3.5.1. Circumstances of an ACA Certificate Renewal

An ACA certificate must be renewed before the validity period of the certificates it signs is shortened (i.e. a child certificate validity period cannot extend beyond the validity period of the parent signing certificate) and the Subject Name and other attributes should be unchanged. In addition, the validity period of the certificate must meet the requirements specified elsewhere in this document. ACA certificates should not be reissued as multiple ACA certificates with the same end validity date are confusing to both users and applications (i.e. browsers).

Comment [PT22]: OATI proposes substitution of "shall" instead of "should". Otherwise you have CA certificates with the same key pair (based on RFC 5280) but different subject information.

3.5.2. Processing ACA Certificate Renewal Requests

An ACA shall notify the NAESB office a minimum of 30 days in advance of a planned ACA certificate renewal, or as soon as practical in the event of an incident that forces an ACA certificate renewal.

3.6. Subscriber Certificate Renewal & Reissuance

Renewing a subscriber certificate consists of creating new certificate with a different public and private key pair and serial number while retaining the remaining contents of the old certificate that describe the subscriber. The new certificate may be assigned a different validity period, key identifiers, CRL distribution points, and/or be signed with a different key. The renewal of a certificate does not require a change to the Subject Name and does not violate the requirement for name uniqueness. Reissuing is exactly the same as renewing a certificate with the exception that the validity period end date remains the same as the old certificate which is being reissued.

Comment [PT23]: OATI proposes rewording: "…The renewal of a certificate shall not allow a change to the Subject Name…" Otherwise you have subscriber certificates with the same key pair (based on RFC 5280) but different subject information.

3.6.1. Processing Subscriber Certificate Renewal & Reissuance Report

Subscribers shall identify themselves for the purpose of renewal or reissuance of their certificate as required in Section 2.3.1. After certificate renewal or reissuance, the old certificate may or may not be revoked, but must not be further used for renewals or reissuance.

3.7. Certificate Revocation & Suspension

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised. For High, Medium, and Basic Assurance, all ACAs shall publish CRLs.

3.7.1. Circumstances for Revocation

For the ACA, a certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. There are three circumstances under which certificates issued by the ACA will be revoked:

- The first circumstance is when NAESB recommends that an ACA-issued certificate be revoked.
- The second circumstance is when the ACA reasonably suspects, is notified, or becomes aware that the private key of a certificate has been compromised.
- The third circumstance is when the ACA becomes aware of an emergency which, if the certificate is not revoked, may have material commercial impact to parties operating in accordance with this standard.

ACAs that implement certificate revocation shall, at a minimum, revoke certificates for the reason of key compromise upon receipt of an authenticated request from a party authorized by the ACA, with a certificate equal to or greater than the assurance level of the certificate being revoked, or the ACA itself.

For certificates that express an organizational affiliation, ACAs shall require that the organization must inform the ACA of any changes in the subscriber affiliation. If the affiliated organization no longer authorizes the affiliation of a Subscriber, the ACA shall revoke any certificates issued to that Subscriber containing the organizational affiliation. If an organization terminates its relationship with a Subordinate ACA such that it no longer provides affiliation information, the Subordinate ACA shall revoke all certificates affiliated with that organization.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

3.7.2. Procedure for Revocation Request

ACAs shall revoke certificates upon receipt of a secured and authenticated request from a verified, appropriate entity or when there is sufficient evidence of compromise or loss of the subscriber's corresponding private key. A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation and include credentials of the party deemed as the appropriate party to submit revocation requests for the Organization identified in the digital certificate being revoked.

3.7.3. Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber must make a revocation request after reasons for revocation have been identified.

In the case of key compromise, an ACA should direct subscribers to request revocation within 1 hour of becoming aware of a confirmed key compromise. An ACA should direct ACA subscribers to request revocation after becoming aware of a suspected key compromise.

3.7.4. Time Within Which ACA Must Process Revocation Request

The ACA shall revoke subscriber certificates as quickly as is practical upon receipt of a verified, proper revocation request.

3.7.5. CRL Issuance Frequency

For an ACA, the interval between CRLs shall not exceed 24 hours when there are no revocations during the interval. The following table specifies the maximum interval for CRL issuance when no revocation has occurred:

Assurance Level	Maximum Interval for CRL Issuance
Rudimentary	No stipulation
Basic	24 hours
Medium	24 hours
High	24 hours

3.7.6. Maximum Latency of CRLs

CRLs shall be published within 4 hours of generation. Each CRL shall be published no later than the time specified in the next Update field of the previously issued CRL for the same scope.

3.7.7. Online Revocation/Status Checking Availability

If on-line revocation/status checking is supported by an ACA, the latency of certificate status information distributed on-line by ACAs or their delegated status responders must meet or exceed the requirements for CRL issuance stated in 3.7.5.

3.7.8. Special Requirements Related to Key Compromise

For ACAs, when a CA certificate is revoked or subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued as specified below:

Assurance Level	Maximum Latency for Emergency CRL Issuance
Rudimentary	No stipulation
Basic	24 hours after notification
Medium	18 hours after notification
High	6 hours after notification

3.8. Key Escrow and Recovery

3.8.1. Key Escrow and Recovery Policy and Practices

The ACA shall not escrow private keys on behalf of subscribers or any other entity outside of the ACA. An ACA may offer secure backup facilities for key storage to subscribers.

Comment [PS24]: OATI believes the distinction between escrow, where the ACA has access to the private keys (which is not allowed) and key storage, where the ACA does not have access to the private keys (which is allowed) needs to be clearly described.

4. FACILITY MANAGEMENT AND OPERATIONS CONTROLS

4.1. Physical Controls

All equipment at the cryptographic hardware security module (HSM) level and any equipment and software associated or interfaced to the certificate authority functions shall be protected from unauthorized access at all times. All physical control requirements specified in sections 4.1.1 through section 4.1.7 apply to the ACA and any remote device used to administer or perform critical certificate authority operations except where specifically noted.

4.1.1. Site Location and Construction

The location and construction of the facility housing the ACA equipment, including sites housing any remote device used to administer or perform critical certificate authority functions shall meet the criteria established by section 3.4 Physical and Environmental Security of the Trust Service Principles and Criteria for Certification Authorities Version 2.0 or the latest effective version established by the AICPA/CICA.

4.1.2. Physical Access for CA Equipment

ACA equipment, to include any remote device used to administer or perform certificate authority functions, shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment. If the ACA intends to issue certificates at all levels of assurance, it shall be operated and controlled on the presumption that it will be issuing at least one High Assurance certificate.

Physical access controls for equipment shall meet the criteria established by section 4.7 CA Cryptographic Hardware Life Cycle Management of the Trust Service Principles and Criteria for Certification Authorities Version 2.0 or the latest effective version established by the AICPA/CICA

In addition to those requirements, the following requirements shall apply to ACAs that issue Medium or High assurance certificates:

- Ensure manual or electronic monitoring for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two person physical access control to both the cryptographic module and computer systems
- Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other ACA equipment used in critical CA functions shall be placed in secure containers when not in use. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module or removable hardware associated with any remote device used to administer or perform critical certificate authority functions.

A security check of the facility housing the ACA equipment or remote devices used to administer the CAs (operating at the Basic Assurance level or higher) shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

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

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

4.1.3. Power and Air Cooling

The ACA (operating at the Basic Assurance level or higher) shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. In addition, the ACA directories (containing ACA issued certificates and CRLs) shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power.

4.1.4. Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Water exposure from fire prevention and protection measures (e.g. sprinkler systems) are excluded from this requirement.

4.1.5. Media Storage

ACA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Sensitive ACA media shall be stored so as to protect it from unauthorized physical access.

4.1.6. Waste Disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

4.1.7. Off-Site Backup

For the ACA operating at the Basic Assurance level or higher, full system backups sufficient to recover from system failure shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an off-site location separate from the ACA equipment. Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational ACA.

4.2. Procedural Controls

Unless stated otherwise, the requirements in this section apply equally to the ACA

Comment [P25]: OATI believes this should say The procedural controls in this section are intended to apply to the ACA unless the ACA has specifically delegated a role or function to a third party (i.e. RA)

4.2.1.Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the ACA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions amongst more than one person, so that any malicious activity would require collusion.

The requirements of this policy are defined in terms of four roles:

1. Administrator
    a. Authorized to install, configure, and maintain the CA
    b. Establish and maintain user accounts
    c. Configure profiles and audit parameters
    d. ~~Generate~~ Management of CA private ~~component~~ keys
2. Registration Administrator
    a. Authorized to request or approve certificates or certificate revocations
    b. Verify the identity of subscribers and accuracy of information included in certificates
    c. Maintains records and other documentation acquired during identity proofing/validation of subscribers
3. Auditor
    a. Authorized to maintain audit logs
    b. Perform or oversee internal compliance audits to ensure that the ACA is operating in accordance with its CPS
4. Operator
    a. Authorized to perform system backup and recovery
    b. Other routine operation of CA equipment

Comment [P26]: OATI believes a clear indication of which role manages the ACA private keys is necessary.

Some roles may be combined. The roles required for each level of assurance are identified in Section 4.2.4.

4.2.2. Number of Persons Required per Task

Only one person is required per task for CAs operating at the Rudimentary Level of Assurance. Two or more persons are required for CAs operating at the Basic, Medium, or High Levels of Assurance for the following tasks:

- CA key generation;
- CA signing key activation;
- CA private key backup.

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 4.2.1. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

Physical access to the CAs does not constitute a task as defined in this section. See Section 4.1.2 for Physical Access Requirements

Comment [P27]: OATI believes this needs to be defined. Perhaps "all access not covered under Physical Access".

4.2.3. Identification and Authentication for Each Role

At all assurance levels other than Rudimentary, an individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

4.2.4. Separation of Roles

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means. Requirements for the separation of roles, and limitations on use of procedural mechanisms to implement role separation, are described below for each level of assurance:

Assurance Level	Role Separation Rules
Rudimentary	No stipulation
Basic	Individual personnel shall be specifically designated to the four roles defined in Section 4.2.1 above. Individuals may assume more than one role; however, no one individual shall assume both the Registration Administrator and Administrator roles. This may be enforced procedurally. No individual shall be assigned more than one identity, except in cases where the ACA issues a pseudonymous certificate to internal users to protect the identities of those users.
Medium	Individual personnel shall be specifically designated to the four roles defined in Section 4.2.1 above. Individuals may only assume one of the Registration Administrator, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and a Registration Administrator role, assume both the Administrator and Auditor roles, and assume both the Auditor and Registration Administrator roles. No individual shall have more than one identity, except in cases where the ACA issues a pseudonymous certificate to internal users to protect the identities of those users.
High	Individual personnel shall be specifically designated to the four roles defined in Section 4.2.1 above. Individuals may assume only one of the Registration Administrator, Administrator and Auditor roles. Individuals designated as Registration Administrator or Administrator may also assume the Operator role. An auditor may not assume any other role. The CA software and hardware shall identify and authenticate its users and shall enforce these roles. No individual shall have more than one identity, except in cases where the ACA issues a pseudonymous certificate to internal users to protect the identities of those users.

4.3. Personnel Controls

4.3.1. Background, Qualifications, and Experience Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. For PKIs operated at Basic Assurance and above, each person filling a trusted role must satisfy at least one of the following:

- The person shall be a citizen of the United States; or

- The person shall be a citizen of the country where the CA is located; or
- For PKIs operated on behalf of multinational governmental organizations, the person shall be a citizen of one of the member countries; or
- For PKIs located within the European Union, the person shall be a citizen of one of the member States of the European Union; or
- For RA personnel only, in addition to the above, the person may be a citizen of the country where the RA is located.

For PKIs operated at Rudimentary Assurance there is no citizenship requirement specified.

4.3.2. Background Check Procedures

ACA personnel shall, at a minimum, pass a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and
- References.

4.3.3. Training Requirements

All personnel performing duties with respect to the operation of the ACA shall receive comprehensive training in all operational duties they are expected to perform, including disaster recovery and business continuity procedures.

In addition, personnel performing duties with respect to the operation of the ACA shall receive comprehensive training, or demonstrate competence, in the following areas:

- CA/RA security principles and mechanisms;
- All PKI software versions in use on the CA system.

Documentation shall be maintained identifying all personnel who received training and the level of training completed. Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.

4.3.4. Retraining Frequency and Requirements

Individuals responsible for PKI roles shall be aware of changes in the ACA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan Annual refresher training is required at minimum. Documentation shall be maintained identifying all personnel who received training and the level of training completed.

4.3.5. Job Rotation Frequency and Sequence

For the ACA, any job rotation frequency and sequencing procedures shall provide for continuity and integrity of the ACA's services.

4.3.6. Independent Contractor Requirements

Contractor personnel employed to perform Trusted Roles shall meet the personnel requirements set forth in the ACA's CP and this NAESB standard as applicable.

4.3.7. Documentation Supplied to Personnel

For the ACA, documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role.

4.4. Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the ACA. 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.

4.4.1.Types of Events Recorded

A message from any source received by the ACA requesting an action related to the operational state of the CA is an auditable event. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,
- The date and time the event occurred,
- A success or failure indicator, where appropriate, and
- The identity of the entity and/or operator (of the ACA) that caused the event.

Detailed audit requirements are listed in the table below according to the level of assurance.

All security auditing capabilities of the ACA operating system and CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. Where events cannot be automatically recorded, the CA shall implement manual procedures to satisfy this requirement.

Auditable Event	Rudimentary	Basic	Medium	High
Security Audit				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X	X
Any attempt to delete or modify the Audit logs		X	X	X
Obtaining a third-party time-stamp		X	X	X
Identification and Authentication				
Successful and unsuccessful attempts to assume a role		X	X	X
The value of maximum authentication attempts is changed		X	X	X
The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login		X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		X	X	X
An Administrator changes the type of authenticator, e.g., from password to biometrics		X	X	X
Local Data Entry				

Auditable Event	Rudimentary	Basic	Medium	High
All security-relevant data that is entered in the system		X	X	X
Remote Data Entry				
All security-relevant messages that are received by the system		X	X	X
Data Export and Output				
All successful and unsuccessful requests for confidential and security-relevant information		X	X	X
Key Generation				
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
Private Key Load and Storage				
The loading of Component private keys	X	X	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X	X	X
Trusted Public Key Entry, Deletion, and Storage				
All changes to the trusted public keys, including additions and deletions	X	X	X	X
Secret Key Storage				
The manual entry of secret keys used for authentication			X	X
Private and Secret Key Export				
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X
Certificate Registration				
All certificate requests	X	X	X	X
Certificate Revocation				

Auditable Event	Rudimentary	Basic	Medium	High
All certificate revocation requests		X	X	X
Certificate Status Change Approval				
The approval or rejection of a certificate status change request		X	X	X
CA Configuration				
Any security-relevant changes to the configuration of the CA		X	X	X
Account Administration				
Roles and users are added or deleted	X	X	X	X
The access control privileges of a user account or a role are modified	X	X	X	X
Certificate Profile Management				
All changes to the certificate profile	X	X	X	X
Revocation Profile Management				
All changes to the revocation profile		X	X	X
Certificate Revocation List Profile Management				
All changes to the certificate revocation list profile		X	X	X
Miscellaneous				
Appointment of an individual to a Trusted Role	X	X	X	X
Designation of personnel for multiparty control			X	X
Installation of the Operation System		X	X	X
Installation of the CA		X	X	X
Installing hardware cryptographic modules			X	X
Removing hardware cryptographic modules			X	X
Destruction of cryptographic modules		X	X	X
System Startup		X	X	X
Logon Attempts to CA Applications		X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
Receipt of Hardware/Software			X	X
Attempts to set passwords		X	X	X
Attempts to modify passwords		X	X	X
Backing up CA internal database		X	X	X
Restoring CA internal database		X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
(Miscellaneous)				
File manipulation (e.g., creation, renaming, moving)			X	X
Posting of any material to a repository			X	X
Access to CA internal database			X	X
All certificate compromise notification requests		X	X	X
Loading tokens with certificates			X	X
Shipment of Tokens			X	X
Zeroizing tokens			X	X
Re-key of the CA	X	X	X	X
Configuration Changes to CA Involving:				
Hardware		X	X	X
Software		X	X	X
Operating System		X	X	X
Patches		X	X	X
Security Profiles			X	X
Physical Access / Site Security				
Personnel access to room housing CA			X	X
Access to the CA server			X	X
Known/suspected violations of physical security		X	X	X
Anomalies				
Software error conditions		X	X	X
Software check integrity failures		X	X	X
Receipt of improper messages			X	X
Misrouted messages			X	X
Network attacks (suspected or confirmed)		X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
Equipment failure	X	X	X	X
Electrical power outage			X	X
Uninterruptible power supply failure			X	X
Obvious and significant network service or access failures			X	X
Violations of Certificate Policy	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X
Resetting operating system clock		X	X	X

4.4.2.Frequency of Processing Logs

Audit logs shall be reviewed in accordance to the table below. Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries with a more thorough investigation of any alerts or irregularities in the log. Examples of irregularities include discontinuities in the logs and loss of audit data. Actions taken as a result of these reviews shall be documented.

Assurance Level	Review Audit Log
Rudimentary	Only required for cause.
Basic	Only required for cause.
Medium	At least once every two months. Statistically significant set of security audit data generated by ACAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity.
High	At least once per month. Statistically significant set of security audit data generated by ACAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity.

4.4.3.Retention Period for Audit Logs

For Medium and High Assurance, audit logs shall be retained on-site until reviewed, as well as being retained in the manner described below. For Rudimentary and Basic Assurance, audit logs shall be retained on-site for at least two months or until reviewed, as well as being retained in the manner

described below. The individual who removes audit logs from the ACA systems shall be an official different from the individuals who, in combination, command the ACA signature key.

4.4.4. Protection of Audit Logs

The ACA system configurations and procedures must be implemented together to ensure that:

- Only personnel assigned to trusted roles have read access to the logs;
- Only authorized people may archive audit logs; and,
- Audit logs are not modified.

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

The off-site storage location for audit logs shall be a safe, secure location separate from the location where the data was generated.

4.4.5. Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site on a monthly basis.

4.4.6. Audit Collection System

The audit log collection system may or may not be external to the ACA systems. Automated audit processes shall be invoked at system (or application) startup, and cease only at system (or application) shutdown.

4.4.7. Cyber Security Vulnerability Assessments

ACA personnel shall routinely assess PKI systems for the presence of known vulnerabilities and have a process by which those vulnerabilities are remediated.

4.4.8 Security Control Assessments

ACA personnel shall routinely assess security control processes to identify process failures for non-conformance with this standard. The ACA shall have a process by which identified instances of non-conformance are remediated.

4.4.9 Real Time Security Monitoring

ACA personnel shall have a process by which real time security events are monitored and analyzed.

4.4.10 Incident Investigation and Response

ACA personnel shall have a process by which identified security incidents are investigated and identified breaches are remediated and reported to NAESB, their subscribers, and the energy ISAC.

4.5. Records Archive

The ACA archive records shall be sufficiently detailed as to verify that the ACA was properly operated as well as verify the validity of any certificate (including those revoked or expired) issued by the ACA.

4.5.1. Types of Events Archived

At a minimum, the following data shall be recorded for archive in accordance with each assurance level:

Data to be Archived	Rudimentary	Basic	Medium	High

Data to be Archived	Rudimentary	Basic	Medium	High
CA accreditation	X	X	X	X
Certificate Policy	X	X	X	X
Certification Practice Statement	X	X	X	X
Contractual obligations	X	X	X	X
Other agreements concerning operations of the CA	X	X	X	X
System and equipment configuration	X	X	X	X
Modifications and updates to system or configuration	X	X	X	X
Certificate requests	X	X	X	X
Revocation requests		X	X	X
Subscriber identity authentication data		X	X	X
Documentation of receipt and acceptance of certificates		X	X	X
Subscriber agreements		X	X	X
Documentation of receipt of tokens (if applicable)		X	X	X
All certificates issued or published	X	X	X	X

Data to be Archived	Rudimentary	Basic	Medium	High
Record of CA re-key	X	X	X	X
All CRLs issued and/or published		X	X	X
Other data or applications to verify archive contents		X	X	X
Compliance Auditor reports		X	X	X
Any changes to audit parameters, e.g., audit frequency, type of events audited		X	X	X
Any attempt to delete or modify the audit log		X	X	X
Whenever the CA generates a key (not mandatory for single-session or one-time-use symmetric keys)	X	X	X	X
All access to the certificate subject private keys retained within the CA for key recovery purposes	X	X	X	X

All changes to the trusted public keys, including additions and deletions	X	X	X	X
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X
The approval or rejection of a certificate status change request		X	X	X
Appointment of an individual to a Trusted Role	X	X	X	X
Destruction of cryptographic modules		X	X	X
All certificate compromise notifications		X	X	X
Remedial action taken as a result of violations of physical security		X	X	X
Violations of Certificate Policy	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X

4.5.2. Retention Period for Archive

The minimum retention periods for archive data are identified below. All entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities. This minimum retention period for these records is intended only to facilitate the operation of the ACA.

Assurance Level	Minimum Retention Period
Rudimentary	7 years
Basic	7 years
Medium	7 years
High	20 years and 6 months

Comment [PT28]: OATI believes rounding to the nearest 10 year increment is needed for simplicity's sake.

4.5.3. Protection of Archive

No unauthorized user shall be permitted to write to or delete the archive. The contents of the archive shall not be released except as required by any statute, valid court order, or rules and regulations of any governmental authority having jurisdiction over the parties. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the ACA itself.

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.

4.5.4. Requirements for Time Stamping of Records

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

4.5.5. Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store archive information shall be published in the applicable CP or CPS. The contents of the archive shall not be released except as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

4.6. Key Changeover

To minimize risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, public key will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that cover certificates signed with that key, then the old key must be retained and protected.

For the ACA, key changeover procedures will establish key rollover certificates where a certificate containing the old public key will be signed by the new private key, and a certificate containing the new public key will be signed by the old private key.

Comment [P29]: OATI believes CA Re-Key is covered in section 3.4 and the reuse of existing keys is, or will be, prohibited. Thus this description of rollover certificates is unnecessary and can be deleted.

4.7. Compromise and Disaster Recovery

4.7.1. Incident and Compromise Handling Procedures

In addition to requirements of the NAESB board certification of ACAs, ACAs shall notify the certificate subscribers if any of the following cases occur:

- Reasonably suspected or detected compromise of the ACA private keys
- Successful or sustained attempt at physical or electronic penetration of ACA systems;
- Successful or sustained attempt at denial of service attacks on ACA components;
- Any incident preventing the ACA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

4.7.2. Computing Resources, Software, and/or Data are Corrupted

When computing resources, software, and/or data are corrupted, the ACA shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored
- If the CA signature keys are not destroyed, CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule
- If the CA signature keys are destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

4.7.3. Business Continuity Capabilities after a Disaster

The ACA system shall be deployed so as to provide 24 hour, 365 day per year availability.

The ACA shall operate a hot backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary site. The ACA operations shall be designed to restore full service within six (6) hours of primary system failure.

The ACA shall at the earliest feasible time directly advise the certificate subscribers in the event of a disaster where the ACA installation is physically damaged and all copies of the ACA's signature keys are destroyed.

4.8. CA and RA Termination

In the event of termination of the ACA operation, certificates signed by the ACA shall be revoked. Certificate subscribers will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought in the event the ACA is terminated. An ACA that voluntarily plans to withdraw from the NAESB certification program must provide subscribers and parties performing RA functions 90 days advance notice of such withdrawal. NAESB may terminate an ACA at any time with 30 ~~days notice~~days' notice.

5. TECHNICAL SECURITY CONTROLS

5.1. Key Pair Generation and Installation

5.1.1. CA Key Pair Generation

For all levels of assurance above rudimentary, cryptographic keying material used to sign certificates, CRLs or status information by the ACA must be:

- Generated in FIPS 140-2 validated cryptographic modules that must meet or exceed Security Level 3.

- CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed.
- Multiparty control is required for CA key pair generation.
- 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.

For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used.

5.1.2. Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 5.1.3 must also be met.

For certificates issued at the High assurance level, subscriber key generation shall be performed using a FIPS-2 Level 2 validated hardware cryptographic module. The ACA must maintain a record of the subscriber acknowledgement of receipt of the token.

Comment [PT30]: OATI believes the tokens are obtained outside the "Subscriber Key Pair Generation" process and thus OATI believes this should state "receipt of the certificate" or be deleted.

For Basic and Medium assurance, either FIPS-2 validated software or hardware cryptographic modules shall be used for key generation.

5.1.3. Private Key Delivery to Subscriber

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Only those parties explicitly authorized by the subscriber may retain any copy of the private key after delivery to the Subscriber.
- The private key must be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

The ACA must maintain a record of the subscriber acknowledgement of receipt of the token.

Comment [P31]: OATI believes the tokens are obtained outside the "Private Key Delivery to Subscriber" process and thus OATI believes this should be deleted.

5.1.4. Public Key Delivery to Certificate Issuer

For CAs operating at the Basic, Medium, or High level of assurance, the following requirements apply:

- Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance.
- The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

For Rudimentary Assurance, no stipulation is made.

5.1.5. CA Public Key Delivery to Relying Parties

When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in a new CA (e.g., cross-) certificate obtained from the issuer(s) of the current CA certificate(s).

Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks.

Key rollover certificates are signed with the CA's current private key, so secure distribution is not required.

CA Certificates are signed with the issuing CA's current private key, so secure distribution is not required.

Comment [P32]: OATI believes "key rollover certificate" needs to be defined or removed.

Comment [P33]: OATI believes cross certification should not be allowed in these requirements and thus be removed.

Comment [P34]: OATI believes this should state "The new public key must be distributed in a self-signed certificate" as OATI believes "rollover certificates" are not defined and cross certification should not be allowed.

5.1.6. Key Sizes

All FIPS-approved signature algorithms shall be considered acceptable; additional restrictions on key sizes are detailed below.

- For all CA certificates the signature keys should be at least 2048 bits for RSA or DSA, and at least 160 bits for ECDSA.
- All CAs certificates should use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. The signatures on all certificates and CRLs that are issued after 12/31/2013 shall be generated using, at a minimum, SHA-256.
- All CA certificates that expire after 12/31/2012, when they expire should be signed with keys of at least 4096 bits for RSA or DSA and at least 256 bits for ECDSA.
- Where implemented, CSSes shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.
- After December 31, 2013, all OCSP responders that generate signatures on OCSP responses shall use SHA-256.
- Beginning with the effective date of these standards, all valid subscriber certificates that include a keyUsage extension that asserts the nonRepudiation, keyEncipherment, dataEncipherment, or keyAgreement bit shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.
- Beginning with the effective date of these standards, all valid end-entity certificates that do not include a keyUsage extension shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.
- Subscriber certificates shall contain public keys that are at least 1024 bit for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms.
- Subscriber certificates that expire after December 31, 2030 shall contain public keys that are at least 3072 bits for RSA or DSA, or 256 bits for elliptic curve algorithms.
- Subscriber certificates that include a keyUsage extension that only asserts the digitalSignature bit that expire after December 31, 2013 shall contain public keys that are at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms.

5.1.7. Public Key Parameters Generation and Quality Checking

Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186. Parameter quality checking (including primarily~~primality~~ testing for prime numbers) shall be performed in accordance with FIPS 186.

5.1.8. Key Usage Purposes (as per X.509 v3 key usage field)

The use of a specific key is determined by the key usage extension in the X.509 certificate.

Subscriber certificates shall assert key usages based on the intended application of the key pair. In particular, certificates to be used for digital signatures (including authentication) shall set the digitalSignature and/or nonRepudiation bits. Certificates to be used for key or data encryption shall set the keyEncipherment and/or dataEncipherment bits. Certificates to be used for key agreement shall set the keyAgreement bit.

Comment [PT35]: OATI proposes rewording: "All valid Subscriber certificates, issued two or more years after the effective date of these requirements, that include…"

Comment [PT36]: OATI believes this bullet item should be deleted per Section 5.1.8 (Subscriber certificates **shall** assert key usages)

Comment [P37]: OATI proposes rewording: "All valid end-entity certificates, issued two or more years after the effective date of these requirements, that do not include…"

Comment [P38]: OATI believes these certificates seemed to be addressed in bullet point #6 and thus this can be deleted.

Comment [P39]: OATI proposes rewording: "All valid subscriber certificates, issued two or more years after the effective date of these requirements, that include…" Also, perhaps bullet items 6, 7, and10 might be combined to say "All valid subscriber certificates, issued two or more years after the effective date of these requirements, must include a keyUsage extension and shall contain public keys that are at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms".

All certificates may include a single key for use with encryption and signature in support of legacy applications. Such dual-use certificates shall be generated and managed in accordance with their respective signature certificate requirements.

Comment [PT40]: OATI believes this should state "signature requirements per section 5.1.6.Key Sizes"

5.2. Private Key Protection and Cryptographic Module Engineering Controls

5.2.1. Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS PUB 140, Security Requirements for Cryptographic Modules.

Cryptographic modules shall be validated to the FIPS 140 level identified in this section. Additionally, the NAESB PKI Subcommittee reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the ACA.

The table below summarizes the minimum requirements for private key storage in cryptographic modules; As mentioned elsewhere if any certificates are issued at a higher assurance level then all CA operations must operate at the highest assurance level (i.e. If a CA issues one high assurance certificate then all CA operations must operate at that assurance level).

Assurance Level	CA, CMS, & CSS	Subscriber
Rudimentary	Level 1 (hardware or software)	N/A
Basic	Level 3 (hardware or software)	Level 1
Medium	Level 3 (hardware)	Level 1
High	Level 3 (hardware)	Level 2 (hardware)

5.2.2. Private Key Multi-Person Control

Use of the ACA private signing key shall require action by multiple persons as set forth in Section 4.2.2 of this document.

5.2.3. Private Key Escrow

5.2.3.1. Escrow of ACA Private Signature Keys

Under no circumstances shall an ACA's signature key used to sign certificates or CRLs be escrowed.

5.2.3.2. Escrow of Subscriber Encryption Keys

Per section 3.8.1, the ACA shall not escrow private keys on behalf of subscribers or any other entity outside of the ACA. An ACA may offer secure backup facilities for key storage to subscribers.

5.2.4. Private Key Backup

5.2.4.1. Backup of ACA Private Signature Keys

ACA private signature keys shall be backed up under multi-person control, as specified in Section 4.2.2.

At least one copy of the ACA private signature key shall be stored off site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original.

5.2.4.2. Backup of Subscriber Private Signature Keys

Comment [PT41]: OATI believes any reference to this document should say "FIPS PUB 140-2" throughout the entire document.

At the High assurance levels, Subscriber private signature keys are stored in a hardware device as non-exportable and thus may not be backed up or copied.

At the Rudimentary, Basic, or Medium levels of assurance, Subscriber private signature keys may be backed up or copied, but must be either held in the Subscriber's control or generated and delivered in accordance to sections 5.1.2 and 5.1.3.

Backed up subscriber private signature keys shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module listed in section 5.2.1.

5.2.5. Private Key Archival

Private signature keys shall not be archived.

For private encryption keys (key management or key transport), no stipulation is made.

5.2.6. Private Key Transfer into or from a Cryptographic Module

ACA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 5.2.4.1. At no time shall the CA private key exist in plain text outside the cryptographic module.

All other keys shall be generated by and in a cryptographic module. In the event that a 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 from outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

5.2.7. Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS-140.

5.2.8. Method of activating Private Keys

For the ACAs that operate at the Medium or High level of assurance, CA signing key activation requires multiparty control as specified in Section 4.2.2.

The Subscriber, LRA, or assigned agent must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include, but are not limited to, pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

5.2.9. Methods of Deactivating Private Keys

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. CA Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

5.2.10. Method of Destroying Private Keys

Individuals in trusted roles shall destroy CA, RA and status server (e.g., OCSP server) private signature keys when they are no longer needed. Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Physical destruction of hardware is not required.

5.3. Aspects of Key Management

5.3.1. Public Key Archival

The public key is archived as part of the certificate archival.

5.3.2. Certificate Operational Periods/Key Usage Periods

The ACA shall limit the use of its private keys to a maximum of three years for certificate signing and six years for CRL signing. ACAs that distribute their self-signed certificates for use as trust anchors shall limit the use of the associated private key to a maximum of 20 years, unless qualifying to be grandfathered in by adhering to all of the following conditions:

- must have a minimum of 10 years with no security breaches to CA operations which resulted in compromise of CA keys,
- must have all CA keys sizes in certificate chain at least 2048.

; The self-signed certificates shall have a lifetime not to exceed 20 years. Code and content signers may use their private keys for three years; the lifetime of the associated public keys shall not exceed 2 years. Subscribers' signature private keys and certificates have a maximum lifetime of 2 years.

CAs must not issue subscriber certificates that extend beyond the expiration date of their own certificates and public keys.

The validity period of the subscriber certificate must not exceed the routine re-key Identity Requirements as specified in section 2.3.1.

5.4. Activation Data

5.4.1. Activation Data Generation and Installation

The activation data used to unlock ACA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. 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. Where the ACA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key.

5.4.2. Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be:

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

The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP or CPS.

5.5. Computer Security Controls

5.5.1. Specific Computer Security Technical Requirements

Comment [P42]: The first sentence appears to contradict other requirements in this section and OATI recommends it be deleted.

Comment [PT43]: OATI believes this is redundant and can be removed.

Comment [PT44]: OATI is not sure if this is referring to CA or Subscriber certificates.

Comment [PT45]: OATI believes this conflicts with the sentence below (The validity period of the subscriber certificate must not exceed the routine re-key Identity Requirements as specified in section 2.3.1.) and should be removed. OATI also believes setting "hard" maximum validity periods with no consideration to the use of the type of subscriber (i.e. devices) will severely limit the applications which adopt this requirement.

For the ACA, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The ACA and its ancillary parts shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to ACA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities Prohibit object re-use or require separation for ACA random access memory
- Require use of cryptography for session communication and database security
- Archive ACA history and audit data
- Require self-test security related ACA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanisms for keys and the ACA system
- Enforce domain integrity boundaries for security critical processes

For Certificate Status Servers, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

For remote workstations used to administer the CA's, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Generate and archive audit records for all transactions; (see section 4.4)
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

All communications between any PKI trusted role and the CA shall be authenticated and protected from modification.

5.6. Lifecycle Security Controls

5.6.1. System Development Controls

The System Development Controls for ACAs at the Basic Assurance level and above are as follows:

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology.

- For hardware and software developed specifically for a particular CA, the applicant shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment.
- Where open source software has been utilized, the applicant shall demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management.
- Hardware and software procured to operate the CA shall be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation.
- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Hardware and software shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

5.6.2. Security Management Controls

The configuration of the ACA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the ACA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the ACA systems. The ACA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

5.7. Network Security Controls

Network security controls shall be employed to protect the ACA. Networking equipment shall have all unused network ports and services turned off. Any network software installed on the ACA equipment shall be necessary to the functioning of the ACA. Any boundary control devices used to protect the ACA local area network shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network. ACAs, RAs, CMSs, directories, remote workstations used to administer the CAs, and certificate status servers shall employ appropriate network security controls. Any network software present shall be necessary to the functioning of the equipment. The CA shall establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.

5.8. 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 4.4.1.

6. CERTIFICATE, CRL, and OCSP PROFILES FORMAT

6.1. Certificate Profile

6.1.1. Version Numbers

The ACA shall issue X.509 v3 certificates (populate version field with integer "3").

6.1.2. Certificate Extensions

For all CAs, use of standard certificate extensions shall comply with [RFC 5280].

6.1.3. Algorithm Object Identifiers

Certificates issued by the ACA shall identify the signature algorithm using one of the following OIDs:

id-dsa-with-sha1	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3 }
sha-1WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
Sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }

ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }

Where certificates are signed using RSA with PSS padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. RSA signatures with PSS padding may be used with the hash algorithms and OIDs specified below:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Certificates issued by the ACA shall identify the cryptographic algorithm associated with the subject public key using one of the following OIDs:

id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }
RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
Dhpublicnumber	{ iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1 }
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }

6.1.4. Name Forms

Where required as set forth in Section 2.1.1, the subject and issuer fields of all certificates shall be populated with an X.500 Distinguished Name. Distinguished names shall be composed of standard attribute types, such as those identified in [RFC5280].

6.1.5. Certificate Policy Object Identifier

Unless certificates issued under a given assurance level are uniquely identified by the certification path (e.g., Root CA),aAll end entity certificates issued by the ACA shall include a Certificate Policies extension containing Certificate Policy's asserting the OID(s) appropriate to the level of assurance with which it was issued. This is in addition to any Certificate Policy identifiers internally used by the ACA. The following table lists the certificate attributes for valid assurance levels. Note that an OID for a higher level covers all lower level assurance levels. For example an end entity certificate which contains the OID for High Assurance means only the Certificate Policy OID associated with High assurance is required and not OID is needed for Rudimentary, Basic, or Medium.

Assurance Level	URI	Object Identifier
Rudimentary	http://www.naesb.org/PKI/AssuranceLevel/Rudimentary	TBD
Basic	http://www.naesb.org/PKI/AssuranceLevel/Basic	TBD
Medium	http://www.naesb.org/PKI/AssuranceLevel/Medium	TBD

Comment [P46]: OATI recommends this document (or WEQ-012) must provide Object Identifier information before the WEQ-012 standards are acted upon. Failure to have this defined before ratification would mean the whole PKI is un-implementable.

OATI recommends reinstatement of language similar to what was in the current WEQ-012 v2.1 (Section 012-1.26.3 Certificate policy Object Identifier) that stipulated if the cert trust chain was unique for a given assurance level you didn't need a specific OID; the trust chain itself could be registered as being associated with a given assurance level.

High	http://www.naesb.org/PKI/AssuranceLevel/High	TBD

6.1.6. Policy Qualifiers Syntax and Semantics

Certificates issued by the ACA may contain policy qualifiers.

6.2. CRL Profile

6.2.1. Version Numbers

The ACA shall issue X.509 version two (2) CRLs.

6.2.2. Algorithm Object Identifiers

The ACA shall sign all CRL's with an approved signature algorithm listed in section 6.1.3.

6.3. Authority Key Identifiers

To assist with digital signature validation and speed the processing of CRL's, the ACA shall include the Authority Key Identifier of the CA certificate used to sign the CRL.OCSP Profile.

If implemented, Certificate Status Servers (CSS) shall sign responses with an approved signature algorithm listed in section 6.1.3.

Comment [P47]: OATI believes one or more words are missing.

7. OTHER BUSINESS and LEGAL MATTERS

7.1. Financial Responsibility

These standards contain no limits on the use of any certificates issued by the ACA. Rather, entities acting as Relying Parties shall determine what financial limits, if any, they wish to impose for certificates used to complete a transaction.

7.2. Confidentiality of Business Information

ACA information not requiring protection can be made publicly available.

7.3. Privacy of Personnel Information

7.3.1. Privacy Plan

The ACA should have a Privacy Plan to protect its personnel's personally identifying information from unauthorized disclosure.

7.3.2. Information Treated as Private

The ACA shall protect a subscriber's personally identifying information from unauthorized disclosure.

7.3.3. Information Not Deemed Private

Information included in ACA and subscriber public key certificates are not subject to protections outlined in Section 7.3.2.

Comment [P48]: OATI proposes wording changes to "… outlined in Section 7.3.2, provided however, that existing agreements between the ACA and Subscribers may require public key certificates to be treated as private under 7.3.2"

7.3.4. Responsibility to Protect Private Information

Sensitive information must be stored securely by ACA's and may be released only in accordance with other stipulations in Sections 4.5.3 and 7.3.

7.4. Intellectual Property Rights

The ACA will not knowingly violate intellectual property rights held by others.

7.5. Representations and Warranties

7.5.1. Subscriber Representations and Warranties

For Medium and High Assurance levels, the ACA shall require Subscribers to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. For Basic Assurance level, the ACA shall require Subscribers to acknowledge his or her obligations respecting protection of the private key and use of the certificate before being issued the certificate.

Comment [P49]: OATI believes this should apply to only High Assurance level certificates.

ACA's should require all Subscribers at Basic, Medium, and High Assurance Levels to agree to the following terms and conditions:

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.

7.5.2. Representations and Warranties of Affiliated Organizations

The ACA should inform Affiliated Organizations of their obligations to authorize the affiliation of subscribers with the organization, and shall inform the ACA of any severance of affiliation with any current subscriber.

7.6. Compliance with Applicable Law

The ACA is required to comply with applicable law.