Signature-Based Handling of Asserted Information using ToKENs (SHAKEN) Certificate Policy - Canada

Approved November 12, 2020

Abstract

This document defines the security controls and practices to support the issuance of STI certificates for the SHAKEN ecosystem in Canada. This document was developed for CAs that desire to be a trusted STI-CA for the issuance of STI certificates for SHAKEN. This document is based on the outline in ATIS-1000084 and is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework.

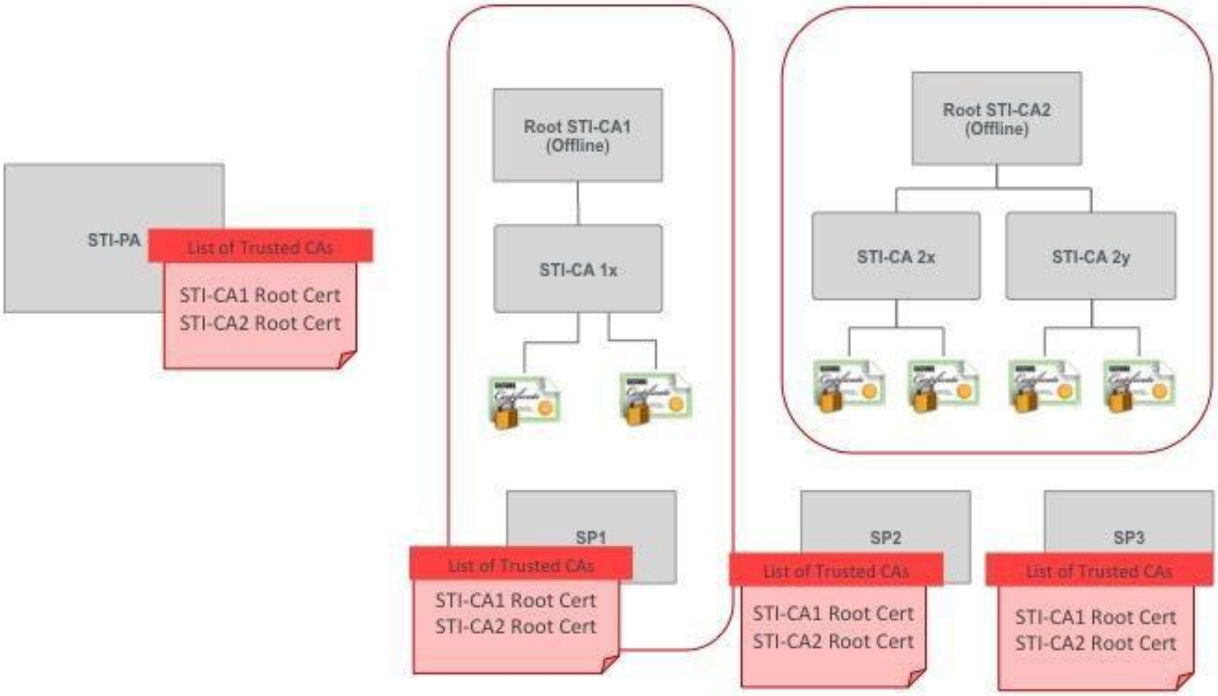
Table of Contents

[THIS PAGE INTENTIONALLY LEFT BLANK]

1 SHAKEN Certificate Policy

1.1 Introduction

This Certificate Policy (CP) for Canada introduces procedural and operational considerations for Secure Telephone Identity Certification Authorities (STI-CAs) within the context of the *Signature-Based Handling of Asserted Information Using toKENs (SHAKEN)* framework (ATIS-1000074) and the *SHAKEN: Governance Model and Certificate Management* framework (ATIS-1000080). The SHAKEN Public Key Infrastructure (PKI) model is an inter-domain model with the STI Policy Administrator (STI-PA) serving as the Trust Authority for the PKI. The STI-PA maintains a list of the root certificates of the STI-CAs that have been approved to issue certificates in the SHAKEN ecosystem, per the below diagram. Along with maintaining the list of Trusted STI-CAs, the STI-PA also maintains the Certificate Revocation List (CRL).



The centralized trust authority model for SHAKEN allows the Canadian Secure Token – Governance Authority Inc. (CST-GA) and STI-PA to have control of the policies to protect the integrity of the PKI. In order to ensure that each Service Provider (SP) to whom a CA issues STI-certificates is an approved SP in the SHAKEN ecosystem, the STI-PA provides a secure Service Provider Code (SPC) token that signifies approval. The SPs must provide this SPC token to a trusted CA when they request a certificate to prove that they have been authorized by the STI-PA. STI-CAs validate that token using the public key certificate corresponding to the private key that the STI-PA used to sign the token. If the token is not valid, the STI-CA must not issue a certificate to that SP.

The following points summarize the key functions that support the SHAKEN Trust Model and issuance of STI-certificates:

1. The STI-PA maintains and makes available the list of Trusted STI-CAs.
2. Local policy determines which issuing STI-CA an SP uses.
3. The STI-PA authorizes SPs to participate in the SHAKEN PKI and issues SPC tokens
4. An SP proves it is authorized to acquire a certificate from a CA by providing the SPC token to the CA:
    a. The STI-CA validates the token using the STI-PA's public key certificate.
5. The STI-PA maintains the CRL:
    a. The URL to the CRL is provided to the SPs when they request an SPC token.

b. The SP includes the CRL URL as part of the Certificate request, and the CA includes the URL to the CRL in the 'cRLDistributionPointName' in the certificate.
c. SPs and STI-CAs add revoked certificates to the CRL through an interface to the STI-PA.

6. During verification of the PASSporT [RFC 8588], a certificate is deemed valid if the root CA in the validation path is on the list of Trusted STI-CAs and the certificate is not on the CRL.

Note that the term CA may be used interchangeably with STI-CA and PA with STI-PA throughout the remainder of this document.

1.2 Overview

This document focuses on Certification Authority (CA) practices and policies that must be followed in order to be approved by the PA to serve as trusted STI-CAs in the SHAKEN ecosystem in Canada. This CP is based on the outline defined in the *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators* (ATIS-1000084), and identifies specific functions required to support the SHAKEN Trust Model as described in ATIS-1000080], including SPC token validation and CRL management.

This CP conforms to *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [Internet Engineering Task Force (IETF) RFC 3647]. To retain the corresponding Section numbers, Sections that are not applicable are annotated as such and Sections left blank identify specific Sections that must be included in the CA's Certification Practice Statement (CPS).

These CA practices and policies are controlled and defined by the SHAKEN Policy Management Authority (PMA) as authorized by the CST-GA.

1.3 Document Name and Identification

This document is the "Signature-Based Handling of Asserted Information using ToKENs (SHAKEN) Certificate Policy" for Canada.

- Version 1.0 was approved for publication on November 12, 2020.

This policy has been assigned the following Object Identifier [OID]: 1.3.6.1.4.1.56223 for SHAKEN CP Version 1.0.

Subsequent revisions to this CP will contain new OID extensions corresponding to the SHAKEN CP version.

1.4 PKI Participants

The participants in the SHAKEN PKI model include CAs, Subscribers, and Relying Parties. The Root CA is recommended to be an offline CA that only issues certificates to intermediate or issuing CAs. In the context of SHAKEN, SPs are the Subscribers and Relying parties.

1.4.1 Certification Authorities

The CAs include the root CAs and any trusted and vetted CA that issue STI certificates.

1.4.2 Registration Authorities

Not Applicable. Registration Authorities are not part of the SHAKEN PKI model.

1.4.3 Subscribers

The Subscribers are the SPs that request STI certificates in order to sign a PASSporT (including SHAKEN [RFC 8588]) in the SIP [RFC 3261] Identity header field [RFC 8224].

1.4.4 Relying Parties

The relying parties are the SPs that use a Subscriber's certificate to verify the authenticity of the calling party identity per the procedures defined in [RFC 8224] and [ATIS-1000074].

1.4.5 Other Participants

There are no other active participants in the SHAKEN PKI model.

1.5 Certificate Usage

1.5.1 Appropriate Certificate Usage

The certificates issued within the SHAKEN PKI trust model are only to be used by a Subscriber for signing SHAKEN PASSporTs, as described in ATIS-1000074, and any other PASSporT extensions defined for use in the SHAKEN ecosystem in Canada. The SHAKEN PASSporTs are used by a Relying party to determine the authenticity of the calling party in the SP's VoIP network.

1.5.2 Prohibited Certificate Uses

Any use other than described in Section 1.5.1, or outside of the SHAKEN eco-system, or not allowed by CST-GA policies are prohibited by this CP.

1.6 Policy Administration

1.6.1 Organization Administering the Document

The CP is administered by the SHAKEN Policy Management Authority (PMA). The PMA is a logical role whose functions are the responsibility of and handled by the CST-GA and/or PA.

The CST-GA can be contacted at:

Marian Hearn – Executive Director, CST-GA

Email: Marian.Hearn@cstga.ca

Phone: 613-287-0225

Website: www.cstga.ca

1.6.2 Contact Person

CA accounts are hosted by the PA. Administrative support personnel can be contacted at:

Neustar Customer Support

Email: communications@support.neustar

Phone: 844-638-7778, Option 3

Website: www.home.neustar

1.6.3 Entity determining CPS suitability for the policy

The PMA determines the suitability and applicability of this CP and the conformance of a CPS, provided by specific STI-CAs, to this CP based on procedures established by the PMA. The suitability and applicability criteria include the results and recommendations received from an independent auditor (see Section 8). The PMA is also responsible for evaluating and acting upon the results of the compliance audit.

1.6.4 CPS approval procedures

The PMA approves the CPS based on review procedures established by the PMA to determine compliance to this CP.

1.7 References

At the time of publication, the editions indicated below were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ATIS-1000074, *Signature-based Handling of Asserted Information using Tokens (SHAKEN).* [1]

ATIS-1000080, *Signature-based Handling of Asserted Information using Tokens (SHAKEN): Governance Model and Certificate Management.*[1]

ATIS-1000084, *Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrator.* [1]

ATIS-0300251, *Codes for Identification of Service Providers for Information Exchange.* [1]

draft-ietf-acme-authority-token-tnauthlist, *TNAuthList profile of ACME Authority Token.*[2]

RFC 3261, *SIP: Session Initiation Protocol.*[2]

RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*[2]

RFC 4949, *Internet Security Glossary, Version 2.*2.[2]

RFC 5217, *Memorandum for Multi-Domain Public Key Infrastructure Interoperability.*[2]

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*[2]

RFC 5905, *Network Time Protocol Version 4 (NTPv4).*[2]

RFC 7159, *The JavaScript Object Notation (JSON).*[2]

RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content.*[2]

RFC 7515, *JSON Web Signatures (JWS).*2 RFC 7516, *JSON Web Algorithms (JWA).*2 RFC 7517, *JSON Web Key (JWK).*[2]

RFC 7518, *JSON Web Algorithm (JWA).*[2]

RFC 7519, *JSON Web Token (JWT).*[2]

RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol*.[2]

RFC 8226, *Secure Telephone Identity Credentials: Certificates.*[2]

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at https://www.atis.org/docstore/.

[2] This document is available from the Internet Engineering Task Force (IETF) at: < http://www.ietf.org >.

RFC 8555, *Automatic Certificate Management Environment (ACME).*[2]

RFC 8588, *Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN).*[2]

X.501, *ITU-T Recommendation X.501 (2005) | ISO/IEC 9594-2:2005, Information technology - Open Systems Interconnection The Directory: Models.*[2]

1.8 Definitions and Acronyms

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

1.8.1 Definitions

The following provides some key definitions used in this document. Refer to IETF RFC 4949 for a complete Internet Security Glossary, as well as tutorial material for many of these terms.

(Digital) Certificate: Binds a public key to a Subject (e.g., the end-entity). A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object. [RFC 4949]. See also STI Certificate.

Certification Authority (CA): An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. [RFC 4949].

Certificate Chain: See Certification Path.

Certification Path: A linked sequence of one or more public-key certificates, or one or more public-key certificates and one attribute certificate, that enables a certificate user to verify the signature on the last certificate in the path, and thus enables the user to obtain (from that last certificate) a certified public key, or certified attributes, of the system entity that is the subject of that last certificate. Synonym for Certificate Chain. [RFC 4949].

Certificate Policy (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. [RFC 3647].

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates. [RFC 3647].

Certificate Revocation List (CRL): A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire. [RFC 4949].

CPS Summary (or CPS Abstract) - A subset of the provisions of a complete CPS that is made public by a CA. [RFC 3647].

Certificate Signing Request (CSR): A CSR is sent to a CA to get enrolled. A CSR contains a Public Key of the end-entity that is requesting the certificate.

Certificate Validation: An act or process by which a certificate user established that the assertions made by a certificate can be trusted. [RFC 4949].

Chain of Trust: Deprecated term referring to the chain of certificates to a Trust Anchor. Synonym for Certification Path or Certificate Chain. [RFC 4949].

Company Code: A unique four-character alphanumeric code (NXXX) assigned to all SPs [ATIS-0300251].

End-Entity: An entity that participates in the Public Key Infrastructure (PKI). Usually a Server, Service, Router, or a Person. In the context of SHAKEN, it is the SP on behalf of the originating endpoint.

Fingerprint: A hash result ("key fingerprint") used to authenticate a public key or other data [RFC 4949].

Identity: Unless otherwise qualified, an identifier that unambiguously distinguishes an entity for authentication and other security and policy application purposes. In this report, a SPC is an example of the identity of one kind of participant in the certificate management process.

Issuing CA: A Certification Authority that issues certificates to an End-Entity. In the context of SHAKEN, the Issuing CA must be subordinate to a trusted STI-CA or to an intermediate CA that is subordinate to a trusted STI-CA.

National/Regional Regulatory Authority (NRRA): A governmental entity responsible for the oversight/regulation of the telecommunication networks within a specific country or region.

National/Regional Regulatory Oversight (NRRO): A governmental entity responsible for the oversight/regulation of the telecommunication networks within a specific country or region. Synonym for NRRA.

Online Certificate Status Protocol (OCSP): An Internet protocol used by a client to obtain the revocation status of a certificate from a server.

Policy Management Authority (PMA): A person, role, or organization within a PKI that is responsible for (a) creating or approving the content of the certificate policies and CPSs that are used in the PKI; (b) ensuring the administration of those policies; and (c) approving any cross-certification or interoperability agreements with CAs external to the PKI and any related policy mappings. The PMA may also be the accreditor for the PKI as a whole or for some of its components or applications.

Private Key: In asymmetric cryptography, the private key is kept secret by the end-entity. The private key can be used for both encryption and decryption. [RFC 4949].

Public Key: The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography. [RFC 4949].

Public Key Infrastructure (PKI): The set of hardware, software, personnel, policy, and procedures used by a CA to issue and manage certificates. [RFC 4949].

Relying party: A system entity that depends on the validity of information (such as another entity's public key value) provided by a certificate. [RFC 5217].

Root CA: A CA that is directly trusted by an end-entity. See also Trust Anchor CA and Trusted CA. [RFC 4949].

Service Provider Code: In the context of this document, this term refers to any unique identifier that is allocated by a Regulatory and/or administrative entity to a SP. In the US and Canada this would be a Company Code as defined in [ATIS-0300251].

Service Provider Code (SPC) Token: An authority token that can be used by a SHAKEN SP during the ACME certificate ordering process to demonstrate authority over the identity information contained in the TN Authorization List extension of the requested STI certificate. The SPC Token complies with the structure of the TNAuthList Authority Token defined by [draft-ietf-acme-authority-token-tnauthlist] and contains a single SPC in the "atc" claim.

Signature: Created by signing the message using the private key. It ensures the identity of the sender and the integrity of the data. [RFC 4949].

Subscriber: A SP that requests STI certificates in order to sign a PASSporT (including SHAKEN [RFC 8588]) in the SIP [RFC 3261] Identity header field [RFC 8224].

Telephone Identity: An identifier associated with an originator of a telephone call. In the context of the SHAKEN framework, this is a SIP identity (e.g., a SIP URI or a TEL URI) from which a telephone number can be derived.

Trust Anchor: An established point of trust (usually based on the authority of some person, office, or organization) from which a certificate user begins the validation of a certification path. The combination of a trusted public key and the name of the entity to which the corresponding private key belongs. [RFC 4949].

Trust Anchor CA: A CA that is the subject of a trust anchor certificate or otherwise establishes a trust anchor key. See also Root CA and Trusted CA. [RFC 4949].

Trust Authority: An entity that manages a Trust List for use by one or more relying parties. [RFC 5217].

Trusted CA: A CA upon which a certificate user relies for issuing valid certificates; especially a CA that is used as a trust anchor CA. [RFC 4949].

Trust List: A set of one or more trust anchors used by a relying party to explicitly trust one or more PKIs. [RFC 5217].

Trust Model: Describes how trust is distributed from Trust Anchors.

1.8.2 Acronyms

ATIS	Alliance for Telecommunications Industry Solutions
ACME	Automated Certificate Management Environment (Protocol)
ATIS	Alliance for Telecommunications Industry Solutions
CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
CR	Certificate Repository
CRTC	Canadian Radio-television and Telecommunications Commission
CSR	Certificate Signing Request
CST-GA	Canadian Secure Token – Governance Authority Inc.
DN	Distinguished Name
HTTPS	Hypertext Transfer Protocol, Secure
IETF	Internet Engineering Task Force
JSON	JavaScript Object Notation
JWT	JSON Web Token
NNI	Network-to-Network Interface
OCN	Operating Company Number
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509 Certificates
PMA	Policy Management Authority
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SKS	Secure Key Store
SP	Service Provider
SPC	Service Provider Code
SP-KMS	SP Key Management Server
STI	Secure Telephone Identity
STI-AS	Secure Telephone Identity Authentication Service

STI-CA	Secure Telephone Identity Certification Authority
STI-CR	Secure Telephone Identity Certificate Repository
STI-PA	Secure Telephone Identity Policy Administrator
STI-VS	Secure Telephone Identity Verification Service
STIR	Secure Telephone Identity Revisited
TN	Telephone Number
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol

2 Publication and Repository Responsibilities

In the case of SHAKEN, it is expected that the SPs will maintain a repository of the certificates they acquire from trusted STI-CAs. Thus, it is not a requirement that a CA also maintain a CR.

2.1 Public Repositories

If an Issuing CA is publishing the certificates in a repository on behalf of the Subscriber, then that repository shall be accessible to all relying parties in the SHAKEN ecosystem in Canada.

2.2 Publication of Certification Information

Each CA shall publish the certificates that it issues via a repository system that is publicly accessible within the VoIP network, unless the Subscriber has established prior agreement with the CA that the CA will publish certificates on the Subscriber’s behalf (reference Section 2.1. In the former case where the Subscriber is publishing the certificates, the CA shall have an agreement with the Subscriber such that the Subscriber shall ensure the certificates are published in a repository accessible to all relying parties in the SHAKEN ecosystem in Canada.

Each CA shall notify the STI-PA of any revoked certificates via the STI-PA UI. It is required that certificate being revoked be uploaded as part of the revocation process.

2.3 Time or Frequency of Publication

If the Issuing CA chooses to host the certificate repository on behalf of an SP, then the issuing CA shall publish any issued certificate, within 24 hours after issuance. The CAs shall inform the Service Providers of any delays so that Service Providers do not sign calls until the certificate has been officially published.

Root CAs shall provide their root certificate once they have been approved by the PMA. Each Root CA shall provide the PA a revised root certificate at least one (1) week prior to expiration of the current root certificate being stored by the PA for distribution to the SPs.

2.4 Access Controls on Repositories

Information published in a repository is public information. The CA shall provide unrestricted access to its repositories and shall implement logical and physical controls to prevent unauthorized *write* access to those repositories.

3 Identification and Authentication

The CPS shall describe the procedures used to authenticate the identity and other attributes of an SP prior to issuing certificates to the SP. This shall include whether the CA supports the Automated Certificate Management Environment (ACME) [RFC 8555] protocol, as well as the ACME extension for token authorization using the SPC as described in ATIS-1000080 and [draft-ietf-acme-authority-token-tnauthlist]. The fingerprint in the SPC token is based on the public key associated with the SP's account ACME credentials.

If the Issuing CA does not support the ACME protocol, the Issuing CA is still required to validate that the SP requesting issuance of a certificate has been assigned a valid SPC token by the STI-PA, following the procedures as described in [ATIS-1000080]. The value to be used for the fingerprint in the SPC token should be based on a similar mechanism as that used ACME (i.e., the fingerprint of a public key used by the SP to interface with the CA) The CA shall describe the mechanism in the CPS.

3.1 Naming

3.1.1 Types of Names

The CA shall assign an X.501 Distinguished Name (DN) [X.501] to each Subscriber. The distinguished name for every CA and end-entity consists of a single Common Name (CN) attribute with a value generated by the issuer of the certificate. The 'serialNumber' attribute shall be included along with the CN (to form a terminal relative distinguished name set), to distinguish among successive instances of certificates associated with the same entity.

3.1.2 Need for Names to be Meaningful

Names used in the STI certificates shall represent an unambiguous identifier for the SP Subject. However, the names should be meaningful enough to represent the SP to whom the certificate is being issued, in a manner similar to that used to identify SP's equipment in the network.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymity is not a function of this PKI; thus, no explicit support for this feature is provided.

3.1.4 Rules for Interpreting Various Name Form

No specific rules are required.

3.1.5 Uniqueness of Name

Subject names need not be globally unique in this PKI. However, each CA shall certify that subject names are unique among the certificates it issues and must describe the process for creating unique names in the CPS.

3.1.6 Recognition, Authentication, and Role of Trademarks

No additional stipulations.

3.2 Initial Identity Validation

The SHAKEN model for identification requires that an SP shall first register with the STI-PA and have a valid SPC token issued by the STI-PA in order to obtain certificates.

3.2.1 Method to Prove Possession of Private Key

Each CA operating within the context of this PKI shall require each Subscriber to demonstrate proof of possession (PoP) of the private key corresponding to the public key in the certificate, prior to issuing the certificate. The means by which PoP is achieved is determined by each CA and shall be described in the CPS of that CA.

In the case of a CA that supports the ACME protocol, the SP is authenticated by means of an "account key pair." The SP uses the private key of this key pair to sign all messages sent to the server. The server uses the SP’s public key to verify the authenticity and integrity of messages from the SP.

3.2.2 Authentication of Organization Identity

The certificate shall contain the ‘countryName’ field and other Subject Identity Information. The CA shall verify the identity of the SP and the authenticity of the SP Applicant Representative’s certificate request using a verification process that must be described in the CA’s CPS. At a minimum, the CA shall validate the SP and ensure that the SP has a valid SPC token.

3.2.3 Authentication of Individual Identity

Each CA operating within the context of the SHAKEN PKI shall employ procedures to identify at least one individual as a representative of each SP. The specific means by which each CA authenticates individuals as representatives for the SP shall be described by the CPS for each CA.

3.2.4 Non-verified Subscriber Information

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

3.2.5 Validation of Authority

Each CA operating within the context of the SHAKEN PKI shall employ procedures to verify that an individual claiming to represent an SP to which a certificate is issued is authorized to represent that SP in this context. The procedures shall be described by the CPS for the CA.

3.2.6 Criteria for Interoperation

This PKI is neither intended nor designed to interoperate with any other PKI.

3.3 Identification and Authentication for Re-key Requests

The CPS shall describe the procedures required for identification and authentication for re-key requests. In the context of SHAKEN, a re-key request shall require issuance of a new Certificate.

3.3.1 Identification and Authentication for Routine Re-key

For re-key of any Subscriber certificate issued under this Certificate Policy, credentials may be established through use of a current signature key unless the certificate has been revoked (see Section 3.3.2). The credentials shall be established following the same procedures as the initial registration at least once every three (3) years from the time of the initial registration.

3.3.2 Identification and Authentication for Re-key after Revocation

In the context of SHAKEN, certificate re-key requests after revocation shall follow the same process as initial identity verification and Certificate issuance.

3.4 Identification and Authentication for Revocation Requests

Revocation requests shall be authenticated by authorized CA staff. The specific certificate to be revoked needs to be identified and the reason for revocation documented. In the case that the CA does not support ACME, the requests to revoke a certificate may be authenticated using the certificate's public key. CAs shall notify the STI-PA in the case that a certificate is revoked as soon as possible, via the STI-PA UI, which requires the actual certificate being revoked to be uploaded as part of the revocation process

4 Certificate Life-Cycle Operational Requirements

This component of the CP specifies requirements imposed upon Issuing CAs and Subscribers with respect to the life cycle of a certificate.

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The only entities that can apply for a certificate are SPs that have provided their CA with an SPC Token. The SPC Token will serve as the means for verification. The SPs must have previously set up an account with the STI-PA and must provide a valid SPC token, as defined in [ATIS-1000080], to prove that it is authorized to obtain STI Certificates.

4.1.2 Enrollment Process and Responsibilities

In the case of an Issuing CA that supports the ACME protocol, the procedures outlined in ATIS-1000080 shall be followed in order to create an account with the Issuing CA.

For CAs that do not support the ACME protocol, the mechanism shall be described in the CPS.

Prior to the issuance of a Certificate, the CA shall obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement or Terms of Use, which may be electronic.

The CA shall obtain any additional documentation the CA determines necessary to meet these requirements.

The CA shall provide and describe the means by which the SPC token associated with the certificate request can be transmitted to the CA.

4.2 Certificate Application Processing

This Section describes the procedure for processing certificate applications.

4.2.1 Performing Identification and Authentication Functions

In the case of CAs that support the ACME protocol the procedures for authentication and association of a Certificate Application shall follow the procedures for authenticating each ACME protocol request. If the CA does not implement the ACME protocol, the CPS must describe the procedure for authenticating and identifying the SP customer.

4.2.2 Approval or Rejection of Certificate Applications

The Issuer CA shall reject any certificate application that cannot be verified. Issuer CAs shall provide a reason for rejecting a certificate application.

4.2.3 Time to Process Certificate Applications

As part of its CPS, each CA shall declare its expected time frame to process a certificate application (i.e., the time between receiving the order for a new certificate from the SP and delivering the new certificate to the SP). Certificate applications shall be processed within a maximum of 24 hours).

4.3 Certificate Issuance

In the case of CAs that support the ACME protocol, the procedures for certificate issuance described in [ATIS-1000080] and [RFC 8555] shall be followed.

4.3.1 CA Actions During Certificate Issuance

If a CA determines that the request is acceptable, it shall issue the requested certificate. If the CA maintains a public repository it shall publish the certificate in the repository as described in Section 2.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

If the CA publishes the certificate on behalf of the SP, the CA shall notify the Subscriber when the certificate is published. If the ACME protocol is not supported, the means by which a Subscriber is notified shall be defined by each CA in its CPS.

4.4 Certificate Acceptance

If the CA publishes the certificate on behalf of the SP, the CP shall document the process for an SP applicant acceptance of a certificate, publication of the certificate by the CA, and notification of certificate issuance to other entities.

4.4.1 Conduct Constituting Certificate Acceptance

If the CA publishes the certificate on behalf of the SP, within the timeframe specified in its CPS, the CA shall place the certificate in the repository and notify the Subscriber. Each CA shall state in its CPS the procedures it follows for publishing of the certificate and notification to the Subscriber.

4.4.2 Publication of the Certificate by the CA

In the case that the CA is publishing the Certificates on behalf of the Subscriber, the CA shall publish the certificate in the repository as described on Section 2.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No other entities shall be notified of issuance of the STI certificates.

4.5 Key Pair and Certificate Usage

A summary of the SHAKEN model for the PKI is provided below.

4.5.1 Subscriber Private Key and Certificate Usage

All Subscribers shall protect their Private keys from unauthorized use or disclosure by third parties and shall use their Private keys only as specified in the key usage extension of the corresponding Certificate. Each SP that has a valid account with the STI-PA is eligible to request an X.509 STI Certificate containing the STIR/SHAKEN extensions.

4.5.2 Relying Party Public Key and Certificate Usage

Any SP that receives a SIP Identity header field with a SHAKEN PASSporT must verify the information. Before using the STI public key certificate, the SP shall perform digital signature verification per ATIS-1000074, as well as ensure that the certificate was issued by a CA that is on the list of trusted CAs, as provided by the STI-PA, and the certificate is not included in the CRL. The verifier shall ensure that the list of trusted CAs has not expired, i.e., is up to date. If it has expired, they shall retrieve the current list from the STI-PA.

4.6 Certificate Renewal

In the case of the ACME protocol, the Subscriber initiates a request for a new certificate. CAs shall not initiate the process to renew or issue a new certificate on behalf of the Subscriber. The process for renewal follows that of certificate issuance per Sections 4.2 through 4.4. Those CAs not using ACME shall provide equivalent procedures and shall describe them.

4.6.1 Circumstance for Certificate Renewal

A Subscriber must request issuance of a new certificate prior to the expiration date of the certificate currently in use. It is recommended that the Subscriber request issuance of the new certificate at least 24 hours prior to expiration.

4.6.2 Who May Request Renewal

Only the Subscriber that is the holder of the expiring certificate can request a new certificate.

4.6.3 Processing Certificate Renewal Requests

The process for renewing a certificate follows the procedures for initial issuance per the previous Sections.

4.6.4 Notification of New Certificate Issuance to Subscriber

The process shall follow that described in Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The process follows that described in Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

The process follows that described in Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Per Section 4.4.3, no other entities shall be notified of certificate issuance.

4.7 Certificate Re-key

This Section describes the requirements for certificate re-key. Certificate re-key is the issuance of a new certificate to replace an old one for the reasons given in Section 4.7.1. Unlike with certificate renewal, the public key must be changed.

4.7.1 Circumstance for Certificate Re-key

Re-key of a certificate must be performed in the following situations:

1. Knowledge or suspicion of compromise or loss of the associated private key; or
2. The expiration of the cryptographic lifetime of the associated key pair.

A CA or SP may perform the certificate re-key operation for other reasons (e.g., an SP could choose to always re-key its short-lived certificates.

Information on maximum key lifetimes can be found in Section 6.3.2. A CA re-key operation requires the reissuance of all certificates issued by the re-keyed entity. It must be performed in a way that preserves the capability of Relying Parties to validate certificates whose validation path includes the re- keyed entity.

If the re-key is based on a suspected compromise, then the previous certificates shall be revoked per the procedures in Section 4.9.

4.7.2 Who May Request Certification of a New Public Key

A certificate re-key may be requested only by the holder of the certificate. In the SHAKEN PKI model, Subscribers with a currently valid certificate must request a new public key prior to expiration of the current public key.

4.7.3 Processing Certificate Re-keying Request

The process for re-keying a certificate follows the procedures for initial issuance per the previous Sections.

4.7.4 Notification of New Certificate Issuance to Subscriber

The CA shall describe how the subscriber is informed of the re-key of its certificate and the contents of the certificate.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Failure to object within 2 business days to the certificate or its contents when it is received by the Subscriber constitutes acceptance of the certificate.

4.7.6 Publication of the Re-keyed Certificate by the CA

All CA certificates shall be published as specified in Section 2.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

No entities other than those described in previous Sections (e.g., Subscribers) shall be notified of the new certificate issuance.

4.8 Certificate Modification

Subscriber certificates must not be modified. If certificate information is not correct, then a new certificate must be requested. For example, if the Subscriber name changes, then the Subscriber shall undergo the initial registration process again with the CA and then follow the procedures described in Sections 4.2 through 4.4. The previous certificate must be revoked and follow the procedures in Section 4.9.

4.8.1 Circumstance for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

The process described in Section 4.3.2 shall be followed.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

The model for managing and communicating the status of revoked certificates is in the form of a distributed Certificate Revocation List (CRL) that is maintained by the STI-PA as described in ATIS-1000080. The STI-PA authenticates all revocation requests.

4.9.1 Circumstances for Revocation

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period. Prior to revoking a certificate, the STI-PA shall verify that the revocation request was made by either the certificate Subscriber or by an entity with the legal jurisdiction and authority to request revocation

The following reasons for revocation are supported through the STI-PA UI:

- Key Compromise
- CA Compromise
- Affiliation Changed
- Superseded
- Cessation of Operation
- Certificate Hold
- Privilege Withdrawn

4.9.2 Who can Request Revocation

Either the CA or a Subscriber can request revocation of an end entity certificate. In addition, a third party (i.e., CST-GA, CRTC, or other regulatory bodies as identified in the policies) could also revoke a certificate.

4.9.3 Procedure for Revocation Request

An entity requesting a certificate revocation (see Section 4.9.2 for the list of such requestors) must submit a request for revocation of an end entity certificate to the issuing CA. The CPS shall describe the procedures for making the request, identifying the specific certificate, and establishing the reason for revocation. In the case that the CA supports the ACME protocol, the procedures described in [RFC8555] shall be followed.

4.9.4 Revocation Request Grace Period

There is no grace period for a revocation request. Once a certificate has been identified and the revocation requestor has been verified, the CA shall revoke the certificate immediately.

4.9.5 Time within which CA must Process the Revocation Request

The CA shall specify its expected revocation timing in its CPS. The timing shall consider the process of notifying the STI-PA.

4.9.6 Revocation Checking Requirement for Relying Parties

A relying party shall acquire and check the CRL, which is managed by the STI-PA, when the relying party validates a certificate.

4.9.7 CRL Issuance Frequency (If Applicable)

The STI-PA maintains the CRL and updates the CRL and makes it available within a 24-hour timeframe

4.9.8 Maximum Latency for CRLs (If Applicable)

Not applicable.

4.9.9 On-line Revocation/Status Checking Availability

The URL to the CRL maintained by the STI-PA is included in the ‘cRLDistributionPointName’ field in the issued certificate. The relying party accesses the list via an HTTPS interface as described in ATIS-1000080.

4.9.10 On-line Revocation Checking Requirements

The SHAKEN PKI defines an indirect CRL model in which the Subscribers and CAs provide any revoked end entity certificates to the STI-PA for inclusion in the CRL. The URL to the CRL is provided to the Subscriber when they request a SPC token from the STI-PA. This URL is included in the ‘cRLDistributionPointName’ field in the end entity certificate so that during path validation, the relying party can check whether the end entity certificate in the certification path have been revoked.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Re-key Compromise

Not applicable.

4.9.13 Circumstances for Suspension

The SHAKEN PKI model does not support suspension of certificates.

4.9.14 Who can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

As stated in Section 4.9.10, each Subscriber includes the URL to the CRL in the ‘cRLDistributionPointName’ in the STI end entity certificate. A CA shall not issue a certificate to a Subscriber that does not include this field in the Certificate Signing Request (CSR).

4.10.1 Operational Characteristics

Not applicable.

4.10.2 Service Availability

Not applicable.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

The subscription ends when the certificate is revoked or expires. The CPS shall describe the procedure to handle the end of subscription.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys shall never be escrowed. Under no circumstances shall a Subscriber's private key be held in trust by a third party.

Subscriber key management keys may be escrowed to provide key recovery. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the Subscriber. CAs that support private key escrow for key management keys shall document their specific practices in their CPS and key escrow documentation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

CAs that support session key encapsulation and recovery shall identify the document describing the practices in the applicable CPS. Components that support session key recovery shall meet the security requirements for the CAs stated in Section 6.

5 Facility, Management, and Operational Controls

This Section describes the technical and administrative security controls used by the CA for key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving. The CPS shall describe the controls and procedures for all the areas identified in this Section.

5.1 Physical Security Controls

For directly operated physical systems, the CA shall maintain security controls for its facilities hosting the CA operation. For physical systems that are not under the direct control of the CA, an equivalent description of security guarantees and/or highly available, geo-redundant operation shall be provided. The controls employed for the CA operation shall be specified in its CPS. The following items shall be documented:

5.1.1 Site Location and Construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house sensitive information. The site whether directly operated or operated by an external party shall provide protection against unauthorized access to CA equipment and records. CAs in the SHAKEN ecosystem shall be located in Canada.

5.1.2 Physical Access

Physical access to equipment hosting the CA shall be limited to authorized personnel. The security mechanisms shall be commensurate with the level of threat in the equipment environment. The CPS shall describe the physical access controls for relevant facility rooms to the extent relevant to directly operated physical systems. The CPS shall describe the security mechanisms in place to prohibit unauthorized access to equipment hosting the CA.

5.1.3 Power and Air Conditioning

For directly operated physical systems, the CA shall have backup power capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

For directly operated physical systems, the CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors). Potential water damage from fire prevention and protection measures (i.e., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

For directly operated physical systems, the physical systems hosting the CA shall comply with local commercial building codes for fire prevention and protection.

5.1.6 Media Storage

For directly operated physical systems, media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access.

Media containing private key material shall be handled, packaged, and stored in a manner compliant with the requirements for the sensitivity level of the information it protects or to which it provides access. Storage protection of CA private key material shall be offline and follow the stipulations in Section 5.1.2 for physical access.

5.1.7 Waste Disposal

For directly operated physical systems, CA and Operations Staff shall remove and destroy normal office waste in accordance with local policy. Media used to collect or transmit privacy information shall be destroyed such that the information is unrecoverable at any time prior to disposal of the physical medium itself. Sensitive media and paper shall be destroyed in a manner that renders the information printed on it unrecoverable by any means. Destruction of media and documentation containing sensitive information, such as private key material, shall employ methods commensurate with those in SP 800-88.

5.1.8 Off-site Backup

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

The data backup media shall be stored in a manner appropriate for storage of information of the same value of the information that will be protected by the certificates and associated private keys issued or managed using the equipment with a minimum requirement of transferring, handling, packaging, and storage of the information in a manner compliant with requirements for sensitive material identified in Section 6.5.1.6.

5.2 Procedural Controls

The CPS shall provide information on the trusted roles (e.g., system administrator). For each role, the CPS shall provide the responsibilities, and the identification and authentication requirements. The CPS shall include separation of duties and the number of individuals required to perform a task.

5.2.1 Trusted Roles

A trusted role--if performed by person versus a secure, autonomous computer program or process--is one in which the person acting in that role performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The only trusted roles defined by this policy are CA Administrators, CA Operations Staff, and Security Auditors. Operations performed by those in trusted roles include:

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

The CA shall maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in CA Administrator, CA Operations Staff, and Security Auditor trusted roles, and shall make them available during compliance audits.

If applicable, the CPS shall define the roles and responsibilities for the CA Administrator, CA Operations Staff, and Security Auditor, noting that some staff may serve in multiple roles.

5.2.2 Number of Persons Required Per Task

If processes are not performed by a secure, autonomous computer program or process, and where multi-party control is required, all participants shall hold a trusted role, with the exception of the Security Auditor who shall be limited to audit functions. If not being performed by a secure, autonomous computer program or process, and physical access is required, the following tasks shall require two or more persons:

- Generation, activation, and backup of CA keys;
- Performance of CA administration or maintenance tasks;
- Archiving or deleting CA audit logs. At least one of the participants in this task shall serve in a Security Auditor role.
- Physical access to CA equipment;
- Access to any copy of the CA cryptographic module.

5.2.3 Identification and Authentication for Each Role

Individuals holding trusted roles shall identify themselves and be authenticated by the CA systems before being permitted to perform any actions set forth above for that role or identity. CA Operations Staff and shall authenticate themselves using a unique credential that is distinct from any credential they use to perform nontrusted role functions. This credential shall be generated and stored in a system that is protected to the same level as the CA system.

CA equipment and systems shall require, at a minimum, strong authenticated access control for remote access using multi-factor authentication. CA equipment and systems shall require, at a minimum, authenticated access control (e.g., strong passwords) for local multi-party access.

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

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

5.2.4 Roles Requiring Separation of Duties

Individuals serving as Security Auditors shall not perform or hold any other trusted role. Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require multi-person control. An individual who performs any trusted role shall only have one identity when accessing CA equipment or systems.

5.3 Personnel Security Controls

Each CA shall maintain personnel security controls for its operation. The personnel controls employed for CA operation shall be specified in its CPS.

5.3.1 Qualifications, Experience, and Clearance Requirements

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

Individuals appointed to any trusted role shall meet the following:

- Be employees of or contractor/vendor of the CA and bound by terms of employment or contract;
- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 5.2.1; and
- Have never been previously relieved of trusted role duties for reasons of negligence or non- performance of duties.

5.3.2 Background Check Procedures

If persons fulfilling Trusted Roles require direct access to information related to secrets (i.e., private keys) that may compromise the integrity of the security of the CA system, they shall pass a background check prior to commencement of employment. The CA shall conduct background checks (in accordance with local privacy laws) which may include the following:

- Confirmation of previous employment;
- Checks of professional references;
- Confirmation of the highest or most relevant educational degree obtained;
- Search of criminal records (local, state or provincial, and national);
- Check of credit/financial records;
- Search of driver’s license records;

- Identification verification via National Identity Check (e.g., Social Insurance Number records), as applicable.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA security principles and mechanisms;
- All PKI software versions in use on the CA system;
- All PKI duties they are expected to perform;
- Certificate lifecycle management;
- Subscriber vetting and identification and validation procedures;
- Disaster recovery and business continuity procedures;
- Stipulations of this policy.

5.3.4 Retraining Frequency and Requirements

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

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

5.3.5 Job Rotation Frequency and Sequence

No Stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative and disciplinary actions, as documented in organization policy, shall be taken against personnel who perform unauthorized actions (i.e., actions not permitted by this CP or other CA security policies) involving the CA's systems, operational processes, security controls the certificate status verification systems, and the certificate repository. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

The CA shall generate audit log files for all events relating to the security of the CA operation. The log information shall be automatically collected. Where this is not possible, the CA shall use a logbook, paper forms or other physical mechanisms to capture the information. Details of how a CA implements the audit logging shall be addressed in its CPS.

The PMA shall have procedures to review the logs on a request basis.

5.4.1 Types of Events Recorded

Audit records shall be generated for the basic operations of the Certification Authority computing equipment.

Audit records shall include the date, time, responsible user or process, success or failure indicators, and summary content data relating to the event.

Auditable events include:

- Access to CA computing equipment (e.g., logon, logout);
- Messages received requesting CA actions (e.g., certificate requests, certificate revocation requests, compromise notifications);
- Subscriber identification information;
- Certificate creation, modification, revocation, or renewal actions;
- Posting of any material to a repository;
- Adding a revoked certificate to the CRL maintained by the STI-PA;
- Any attempts to change or delete audit data;
- Key generation;
- Software and/or configuration updates to the CA; or
- Clock adjustments.

5.4.2 Frequency of Processing Log

The audit log shall be reviewed periodically and before being archived. All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

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

Real-time automated analysis tools should be used. All alerts generated by such systems shall be analyzed by CA operations staff on a daily basis.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained for at least ninety (90) days in addition to being archived as described in Section 5.5. The individual who removes audit logs from the CA system, if performed manually by a person, shall be an official different from the individuals who, in combination, command the CA signature key.

5.4.4 Protection of Audit Log

The security audit data shall not be open for reading by any human, or by any automated process, other than those that perform security audit processing. The log shall not be writable except by the logging mechanism itself. Once written, the log shall not be modifiable by machine or human.

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

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

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

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

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least every thirty (30) days. The backup of the audit log shall be stored securely in an alternate location.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the CA system. Automated audit processes shall be invoked at system or application startup and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed; CA operations shall be suspended until the security audit capability can be restored, except for revocation processing and in the situation where a certificate needed for real-time authentication has expired or is soon to expire,.

5.4.7 Notification to Event-Causing Subject

Not Applicable.

5.4.8 Vulnerability Assessments

The CA operations staff shall routinely test, at least annually, and assess the CA systems to determine if they have any vulnerabilities. Each identified vulnerability shall be prioritized based on its risk level and a remediation plan shall be created. There shall be a patch management process to remediate critical and high rated vulnerabilities as soon as it is feasible or when a vendor patch is released.

5.5 Records Archival

5.5.1 Types of Records Archived

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

- CP
- CPS
- Contractual obligations

- Other agreements concerning operations of the CA
- System and equipment configuration
- Subscriber identity authentication data as per Section 3.2.3
- Documentation of receipt and acceptance of certificates (if applicable)
- Subscriber agreements
- Documentation of receipt of system access tokens
- All Certificate requests for which the authorization failed
- All Certificates issued
- All Certificates revoked
- All Audit logs
- Other data or applications to verify archive contents
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g. audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- All access to any certificate subject private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- Remedial action taken as a result of violations of physical security
- Violations of CP
- Violations of CPS

5.5.2 Retention Period for Archive

Archive records must be kept for a minimum of seven (7) years and six (6) months without any loss of data.

5.5.3 Protection of Archive

The CPS shall describe the archiving process and how the archive is protected. No unauthorized user shall be permitted to write to, modify, or delete the archive.

The archived records may be moved to another offline medium. The contents of the archive shall not be released. 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 system separate from the CA systems with physical and procedural security controls equivalent to or better than those of the CA. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

5.5.4 Archive Backup Procedures

The CPS shall describe how archive records are backed up and how the archive backups are managed.

5.5.5 Requirements for Time-Stamping of Records

The 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 source.

5.5.6 Archive Collection System (Internal or External)

Archive data shall be collected in an expedient manner and on a regular schedule as described in the CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures, detailing how to create, verify, package, transmit, and store the CA archive information, shall be published in the CPS.

5.6 Key Changeover

CAs shall not issue Subscriber certificates that extend beyond the expiration date of the CA's certificates and public keys. Each CA certificate validity period shall extend one user certificate validity period past the last use of the CA private key. To minimize the risk from compromise of a CA's private signing key, the private signing key will change more frequently. When the private signing key changes, the CA shall use only the new key for certificate signing.

The CPS shall describe the procedure to provide a new STI-CA public key to users following a re-key by the STI-CA.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

CA organizations shall have an Incident Response Plan and a Disaster Recovery Plan.

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

The CA shall immediately notify the PMA if any of the following occur:

- Actual or detected compromise of any CA system or subsystem;
- Physical or electronic penetration of any CA system or subsystem;
- Successful denial of service attacks on any CA system or subsystem; or
- Any incident preventing a CA from notifying the STI-PA of a revoked certificate (e.g., compromised credentials).

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

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

- Notify the PMA director as soon as possible using the PMA contact information provided in this document.
- Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup.
- Reestablish CA operations.
- If the CA signing keys are destroyed, reestablish CA operations as quickly as possible, giving priority to the generation of a new CA signing key pair.
- If the integrity of the system cannot be restored, or if the risk is deemed substantial, reestablish system integrity before returning to operation.

5.7.3 Entity Private Key Compromise Procedures

5.7.3.1 Root CA Compromise Procedures

In the case of the Root CA compromise, the CA shall immediately notify the PMA. The CA shall also notify all Subscribers. The PMA shall update the list of trusted STI-CAs and make it available to all Subscribers and

Relying Parties to obtain the new list of Trusted STI-CAs. The caList has an expiration period, configured to 24 hours, and the SPs periodically retrieve it via REST API. Therefore, such an update will only reflect the next time the SPs can retrieve the caList.

Initiation of notification shall be made at the earliest feasible time and shall not exceed twenty-four (24) hours beyond determination of the actual compromise or loss unless otherwise required by law enforcement. If the cause of the compromise can be adequately addressed, and it is determined that the PKI can be securely re-established, the CA shall then generate a new Root CA certificate and update its account with the STI-PA per the established CPS procedures.

5.7.3.2 Intermediate CA Compromise Procedures

In the event of an Intermediate CA key compromise, the CA shall notify the PMA and the root CA. The root CA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner and within eighteen (18) hours after the notification. The Compromised CA shall also investigate and report to the PMA and Superior CA what caused the compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the compromise can be adequately addressed and it is determined that the CA can be securely re-established, then the CA shall be re-established. Upon re-establishment of the CA, new Subscriber certificates shall be requested and issued.

5.7.4 Business Continuity Capabilities After a Disaster

CAs shall be required to maintain a Disaster Recovery Plan. The CA Disaster Recovery Plan shall be coordinated with any overarching Enterprise Disaster Recovery Plan that the broader organization may have. The Disaster Recovery Plan shall identify what management and operations procedures are in place to mitigate risks to facilities, systems, networks, and application controls. It shall also identify procedures for annual testing of processes to restore service, individuals on call for management, response and recovery activities, and the order of restoral of equipment and services.

In the case of a disaster in which the CA equipment is damaged and inoperative, the CA operations shall be re-established as quickly as possible, giving priority to the ability to revoke Subscriber's certificates. If the CA cannot re-establish revocation capabilities within eighteen (18) hours, then the inoperative status of the CA shall be reported to the PMA and Superior CA. The PMA shall decide whether to declare the CA private signing key as compromised and the CA keys and certificates need to be reissued or allow additional time for reestablishment of the CA's revocation capability.

In the case of a disaster in which a CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the CA shall request that its certificates be revoked. The CA installation shall then be completely rebuilt by re-establishing the CA's equipment, generating new private and public keys and being re-certified. Finally, all Subscribers will be notified that certificates need to be re-issued. In the case of subscribers that maintain their own repositories, it is recommended that any certificates issued by that CA be revoked.

5.8 CA Termination

When a CA operating under this CP terminates operations before all certificates have expired, entities shall be given as much advance notice as circumstances permit. The CA shall notify the PMA using documented contact information.

Prior to termination the CA shall revoke all unexpired certificates within the repository it maintains. The CA shall archive all audit logs and other records prior to termination. The CA shall destroy all private keys upon termination. The CA archive records shall be transferred to the PMA. If a Root CA is terminated, the root CA shall be removed from the list of trusted CAs. In that case, any certificates that have not been revoked will be invalid once the relying parties receive the updated list.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Cryptographic keying material used by CAs to sign certificates shall be generated by cryptographic modules validated to FIPS 140 Level 3, or some other generally accepted conformance to X.509 related standards.

CA key pair generation shall create a verifiable audit trail demonstrating that the security requirements for the documented procedures were followed. The CPS description of the procedure shall be detailed enough to show that appropriate role separation was used.

Subscriber key pair generation shall be performed by the Subscriber.

6.1.2 Private Key Delivery to Subscriber

This is not applicable in the case that only the Subscriber generates the key pair.

6.1.3 Public Key Delivery to Certificate Issuer

When the Subscriber generates the key pair, the public key and the Subscriber’s identity need to be delivered securely to the CA for certificate issuance. In the case that the ACME protocol is supported, this is provided to the CA during account creation.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of a root CA shall be provided to the Subscribers acting as relying parties in a secure manner so that it is not vulnerable to modification or substitution.

When a CA updates its signature key pair, the key rollover certificates may be signed with the CA’s current private key; in this case, secure out-of-band mechanisms are not required.

6.1.5 Key Sizes

CAs that generate STI certificates under this policy shall use the SHA-256 algorithm when generating digital signatures. ECDSA signatures on certificates shall use SHA-256.

6.1.6 Public Key Parameters Generation and Quality Checking

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

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

Public keys that are bound into CA certificates shall be used only for signing CA certificates. CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this policy. In addition, *anyExtendedKeyUsage* shall not be asserted in extended key usage extensions.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CAs shall use cryptographic modules validated to [FIPS 140] Level 3, or some other generally accepted conformance to X.509 related standards for signing operations.

6.2.2 Private Key (n out of m) Multi-person Control

CAs may employ multi-person controls to constrain access to their private keys, but this is not a requirement all CAs in the PKI. The CPS for each CA shall describe which, if any, multi-person controls it employs.

6.2.3 Private Key Escrow

CA private keys shall never be escrowed.

6.2.4 Private Key Backup

The CA private signature keys shall be backed up under the same control as the original signature key. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original. Backup procedures shall be included in the CA's CPS.

6.2.5 Private Key Archival

CA private signature keys and Subscriber private signature keys shall not be archived. CAs that retain Subscriber private encryption keys for business continuity purposes shall archive such Subscriber private keys in accordance with Section 5.5.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4. At no time shall the CA private key exist in plaintext outside the cryptographic module.

All other keys shall be generated by a cryptographic module. In the event 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 form outside the cryptographic module boundary.

Transport keys used to encrypt private keys shall be handled in the same way as the private key.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140 (or other generally accepted secure storage methods).

6.2.8 Method of Activating Private Key

If private key activation is applicable to the CA use of a cryptographic module, the Subscriber must be authenticated with the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Method of Deactivating Private Key

If private key activation is applicable to the CA use of a cryptographic module, 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 cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 Method of Destroying Private Key

Individuals in trusted roles or automated computer processes shall destroy CA private signature keys when they are no longer needed. If applicable, subscribers shall either surrender their cryptographic module to CA personnel for destruction or subscribers shall destroy their private signature keys when they are no longer needed or when the certificates to which they correspond expire or are revoked. Physical destruction of any hardware is not required.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival described in Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The usage period for the Root CA key pair is a maximum of twenty-five (25) years.

For all other CAs operating under this policy, the usage period for a CA key pair is a maximum of twelve (12) years. The CA private key may be used to sign certificates for at most <9> years. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

Subscriber public keys in certificates other than code signing certificates have a maximum usage period of three (3) years. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

Subscriber activation data may be user-selected. The strength of the activation data shall meet or exceed the requirements for authentication mechanisms stipulated for Level 3 in FIPS 140, or some other equivalent standard. 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.

6.4.2 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 either:

- memorized;
- biometric in nature; or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module and shall not be stored with the cryptographic module.

6.4.3 Other Aspects of Activation Data

No additional stipulations.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The CPS shall document the technical controls covering all the of the areas identified in this Section of the CP.

6.5.1.1 Access Control

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

6.5.1.1.1 Access Control Policy and Procedures

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

6.5.1.1.2 Account Management

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

Section 5.2.1 of this document defines roles and job functions for personnel that the CA shall use when defining access control mechanisms. The CA shall employ the principle of least privilege when creating users and assigning them to groups and roles; membership to a group or role shall be justified based upon business need. The CA shall take appropriate action when a user no longer requires an account, their business role changes, or the user is terminated or transferred. The CA shall annually review all active accounts to match active authorized users with accounts and disable or remove any accounts no longer associated with an active authorized user.

Automated systems shall be employed to maintain access for only those users who are still authorized to use the information system. After thirty (30) days of inactivity, an account shall be automatically disabled and attempts to access any deactivated account shall be logged. The user can contact CA personnel to have the account reactivated.

All account administration activities shall be logged and made available for inspection by appropriate security personnel. Account administration activities that shall be audited include account creation, modification, enabling, disabling, group or role changes, and removal actions. See Section 5.4 for detailed requirements for these logs.

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

6.5.1.1.3 Least Privilege

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

6.5.1.1.4 Access Control Best Practices

The following are best practices for access control:

- Unique User IDs is associated with each individual user.
- All user activity shall be traceable to an individual.
- No shared or default accounts shall be used.
- There is a process to track the assignment and configurations of administrative privileges to CA operations systems. The principle of least privilege shall be followed.
- There is an authorization process to approve users and their associated privileges.
- There is a process to establish, change, deactivate and remove UserIDs and privileges.
- Passwords shall be at least 8 characters with associated complexity and usage rules.
- Passwords are never stored or transmitted in cleartext.
- There are defined session timeouts (15 minutes) during periods of user inactivity.
- There shall be a limit on failed login attempts (5). If there is a lockout, an administrator needs to reset the password.
- For remote access from external public networks, multi-factor authentication shall be used.
- There shall be logging of all failed login attempts and changes in administrative privileges.

6.5.1.1.5 Authentication: Passwords and Accounts

When the authentication mechanism uses user selectable passwords, strong passwords shall be employed, as defined in the CA password policy referenced in the CPS. Passwords for CA authentication operational systems shall be different from CA enterprise systems.

The CA shall have the minimum number of user accounts that are necessary to its operation. Account access shall be locked after five (5) unsuccessful login attempts. Restoration of access shall be performed by a different person who holds a trusted role or restore access after a timeout period.

6.5.1.1.6 Permitted Actions without Identification or Authentication

The CA shall document in the CPS a specific list of actions that can be performed on specifically enumerated information systems without identification or authentication, such as accessing a publicly available website. Furthermore, the CA shall document and provide supporting rationale in its security policy and procedures an enumerated list of user actions and systems not requiring identification or authentication (i.e., anonymous access to a public website) and not related to the CA operation.

6.5.1.2 System Integrity

6.5.1.2.1 System Isolation and Partitioning

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

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

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

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

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

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

6.5.1.2.2 Malicious Code Protection

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

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

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

Anti-malware tools shall alert CA Administrators of any malware detected by the tools.

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

6.5.1.2.3 Software and Firmware Integrity

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

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

6.5.1.2.4 Information Protection

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

6.5.2 Computer Security Rating

No specific stipulation. The CPS should indicate any rating applicable to their CA.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The system development controls must address all aspects related to the development and change of the CA system through aspects of its life-cycle.

The CA system shall be implemented and tested in a non-production environment prior to implementation in a production environment. No change shall be made to the production environment unless the change has gone through the documented change control process.

In order to prevent incorrect or improper changes to the CA system, the CA system shall require multi-party control for access to the CA system when changes are made.

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

Hardware and software procured to operate the CA shall be purchased from authorized vendors in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device). The hardware and software shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

Hardware and software updates shall be purchased or developed in the same manner as original equipment and shall be installed by trusted and trained personnel in a defined manner.

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

6.6.2 Security Management Controls

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

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

To validate the integrity of the CA system, automated tools that validate all static files on a component shall be in operation to notify operators when a protected file has changed.

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

6.6.3 Life Cycle Security Controls

The CA shall scan all online CA operations systems for vulnerabilities using commercially available security vulnerability testing and analysis tool on a regular basis (i.e., monthly) The use of multiple vulnerability testing tools for testing the most sensitive systems is strongly encouraged.

Each vulnerability found shall be entered into a vulnerability tracking database, along with the date and time and the specific system. The vulnerabilities shall be prioritized based on the risk level. A remediation plan shall be created to address at least the critical and high rated vulnerabilities within 72 hours if feasible. If a vendor patch is required, the patch, when released shall be tested before it is deployed into production. Remediation shall be entered into the vulnerability database as well (including date and time).

The CA staff shall monitor relevant product and vendor notification portals on a regular basis for updates to product packages installed on CA systems (including networking hardware). CAs shall subscribe to these notification portals identifying software and firmware updates and patches and having a patch management and maintenance program that covers obtaining and testing those updates and patches, for deciding when to install them, and finally for installing them without undue disruption. A log shall be kept of the notifications, the decision to apply/not apply including reason, and the application of relevant updates/patches. The CPS shall describe in detail the security lifecycle management activities and procedures.

From time to time, the CA may discover unintentional errors in configuration files, either because of human error, source data error, or changes in the environment, which have made an entry erroneous. The CA shall correct such errors as soon as possible governed by the documented change management procedure.

Remediation activities should not cause unavailability of revocation activities.

6.7 Network Security Controls

The CPS shall document network security controls protecting the CA operations systems, including the following key principles:

- Defense-in-depth strategy to protect the network elements and externally facing perimeter, systems, applications and interfaces.
- Security devices that are being used including firewalls, Web application firewalls, intrusion detection and prevention technology and denial-of-service protection.
- Threat intelligence monitoring include procedures to update attack signatures in network security devices.
- Network segmentation to protect the CA operations systems from the enterprise systems.
- Security access controls for accessing network management tools and information.
- Network security monitoring approach.

6.8 Time-Stamping

The CP shall address the requirements for the use of timestamps. System clocks used for time-stamping shall be maintained in synchrony with an authoritative time standard (e.g., through the use of Network Time Protocol (NTP) [RFC 5905]).

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Certificates issued by the CA shall adhere to the X.509 v3 certificate profile documented in RFC 5280. The CA shall support the certificate extensions defined and described for STIR Identity Credentials: Certificates [RFC 8226] and SHAKEN Governance Model and Certificate Management [ATIS-1000080].

The CPS shall have the following Sections addressing their compliance to the standards:

- Version number(s)
- Certificate extensions
- Algorithm object identifiers
- Name forms
- Name constraints
- Certificate policy object identifier
- Usage of Policy constraints extension
- Policy qualifiers syntax and semantics
- Processing semantics for the critical Certificate Policies extension

7.2 CRL Profile

The CRL for the SHAKEN ecosystem in Canada is maintained by the STI-PA as defined in [ATIS-1000080]. The CRL issued by the STI-PA also includes the crlExtensions CRLNumber as per RFC 5280. This extension is updated when the CRL is updated, or when the CRL expires and a new one is generated. The format required for entries in the CRL provided by the CA is described in the following Sections.

7.2.1 Version Numbers

CRL V2.

7.2.2 CRL and CRL Entry Extensions

When a CA revokes a certificate, the procedures described in Section 4.9 shall be followed. The CA shall notify the STI-PA and provide the following information, which is included in the CRL entries:

- Certificate’s Serial Number;
- Revocation Date;
- Reason;
- Certificate Issuer.

7.3 OCSP Profile

Not applicable.

8 Compliance Audit and Other Assessment

The CA policies shall be designed to meet the requirements based on [ATIS-1000080] and [ATIS-1000084], as well as generally accepted and published industry standards. All Issuing CAs shall ensure that audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

8.1 Frequency or Circumstances of Assessment

If requested by the PMA, Issuing CAs shall retain an independent auditor for a period of time who shall assess the Issuing CA’s compliance with this CP and its CPS. This audit must cover each operations server that is specified in a certificate issued by the Issuing CA.

8.2 Identity/Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA’s CPS and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor shall have appropriate professional certifications such as a Certified Information System Auditor (CISA) or IT security specialist, and shall have available a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor either shall be a private firm that is independent from the Issuing CA being audited or shall be sufficiently organizationally separated from the CA to provide an unbiased, independent evaluation. To ensure independence and objectivity, the compliance auditor must not have worked with the CA in developing or maintaining the entity’s CA Facility or CPS. The PMA shall determine whether a compliance auditor meets this requirement.

8.4 Topics Covered by Assessment

The audit must conform to industry standards, cover the Issuing CA's compliance with its business practices disclosure, and evaluate the integrity of the Issuing CA’s PKI operations in compliance with the SHAKEN PKI model. The audit must verify that each Issuing CA is compliant with this CP.

8.5 Actions Taken as a Result of Deficiency

If an audit reports a material noncompliance with applicable law, this CP, the CPS, or any other contractual obligations related to the Issuing CA’s services, then (1) the auditor shall document the discrepancy, (2) the auditor shall promptly notify the Issuing CA and the PMA, and (3) the Issuing CA and the PMA shall develop a plan to rectify the noncompliance. The PMA shall also notify the CST-GA. body. The Issuing CA shall submit the plan to the PMA for approval. The PMA may require additional action, if necessary, to rectify any significant issues created by the non-compliance, including requiring revocation of affected Certificates.

8.6 Communication of Results

The Audit Compliance Report and identification of corrective measures shall be provided to the PMA within thirty (30) days of completion.

The results shall also be communicated to any third-party entities entitled by law, regulation, or agreement to receive a copy of the audit results.