Telecert CPS

Certification Practice Statement for SHAKEN

Version 1.4

Contents

1 Introduction 1
1.1 Overview 1
1.2 Document Name and Identification 2
1.3 PKI Participants 3
1.3.1 Certification Authorities 3
1.3.2 Registration Authorities 3
1.3.3 Subscribers 3
1.3.4 Relying Parties 3
1.3.5 Other Participants 4
1.4 Certificate Usage 4
1.4.1 Appropriate Certificate Usage 4
1.4.2 Prohibited Certificate Uses 4
1.5 Policy Administration 4
1.5.1 Organization Administering the Document 4
1.5.2 Contact Person 4
1.5.3 Entity Determining CPS Suitability for the Policy 5
1.5.4 CPS Approval Procedures 5
1.6 Definitions and Acronyms 5
1.6.1 Definitions 5
1.6.2 Acronyms 9
1.7 References 10
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 12
2.1 Public Repositories 12
2.2 Publication of Certification Information 12
2.3 Time or Frequency of Publication 12
2.4 Access Controls on Repositories 13
3 IDENTIFICATION AND AUTHENTICATION 13
3.1 Naming 13
3.1.1 Type of Names 13
3.1.2 Need for Names to be Meaningful 13
3.1.3 Anonymity or Pseudonymity of Subscribers 13
3.1.4 Rules for Interpreting Various Name Form 13

3.1.5 Uniqueness of Name 14
3.1.6 Recognition, Authentication, and Role of Trademarks 14
3.2 Initial Identity Validation 14
3.2.1 Method to Prove Possession of Private Key 14
3.2.2 Authentication of Organization Identity 14
3.2.3 Authentication of Individual Identity 15
3.2.4 Non-verified Subscriber Information 16
3.2.5 Validation of Authority 16
3.2.6 Criteria for Interoperation 16
3.3 Identification and Authentication for Re-key Requests 16
3.3.1 Identification and Authentication for Routine Re-key 16
3.3.2 Identification and Authentication for Re-key after Revocation 16
3.4 Identification and Authentication for Revocation Requests 16
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 17
4.1 Certification Application 17
4.1.1 Who Can Submit a Certificate Application 17
4.1.2 Enrollment Process and Responsibilities 17
4.2 Certification Application Processing 17
4.2.1 Performing Identification and Authentication Functions 18
4.2.2 Approval or Rejection of Certificate Applications 18
4.2.3 Time to Process Certificate Applications 18
4.3 Certificate Issuance 18
4.3.1 STI-CA Actions During Certificate Issuance 18
4.3.2 Notification to Subscriber by the STI-CA of Issuance of Certificate 19
4.4 Certificate Acceptance 19
4.4.1 Conduct Constituting Certificate Acceptance 19
4.4.2 Publication of the Certificate by the STI-CA 19
4.4.3 Notification of Certificate Issuance by the STI-CA to Other Entities 19
4.5 Key Pair Certificate Usage 19
4.5.1 Subscriber Private Key and Certificate Usage 19
4.5.2 Relying Party Public Key and Certificate Usage 20
4.6 Certificate Renewal 20
4.6.1 Circumstance for Certificate Renewal 20

4.6.2 Who May Request Renewal 20
4.6.3 Processing Certificate Renewal Requests 20
4.6.4 Notification of New Certificate Issuance to Subscriber 20
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 20
4.6.6 Publication of the Renewal Certificate by the STI-CA 20
4.6.7 Notification of Certificate Issuance by the STI-CA to Other Entities 21
4.7 Certificate Re-key 21
4.7.1 Circumstance for Certificate Re-key 21
4.7.2 Who May Request Certification of a New Public Key 21
4.7.3 Processing Certificate Re-keying Request 21
4.7.4 Notification of New Certificate Issuance to Subscriber 21
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 21
4.7.6 Publication of the Re-keyed Certificate by the STI-CA 21
4.7.7 Notification of Certificate Issuance by the STI-CA to Other Entities 21
4.8 Certificate Modification 21
4.8.1 Circumstance for Certificate Modification 21
4.8.2 Who May Request Certificate Modification 22
4.8.3 Processing Certificate Modification Requests 22
4.8.4 Notification of New Certificate Issuance to Subscriber 22
4.8.5 Conduct Constituting Acceptance of Modified Certificate 22
4.8.6 Publication of the Modified Certificate by the STI-CA 22
4.8.7 Notification of Certificate Issuance by the STI-CA to Other Entities 22
4.9 Certificate Revocation and Suspension 22
4.9.1 Circumstances for Revocation 22
4.9.2 Who Can Request Revocation 23
4.9.3 Procedure for Revocation Request 23
4.9.4 Revocation Request Grace Period 23
4.9.5 Time within which the Revocation Request must be Processed 24
4.9.6 Revocation Checking Requirement for Relying Parties 24
4.9.7 CRL Issuance Frequency (If Applicable) 24
4.9.8 Maximum Latency for CRLs (If Applicable) 24
4.9.9 Online Revocation/Status Checking Availability 24
4.9.10 Online Revocation Checking Requirements 24

4.9.11 Other Forms of Revocation Advertisements Available 24
4.9.12 Special Requirements Re-key Compromise 24
4.9.13 Circumstances for Suspension 25
4.9.14 Who Can Request Suspension 25
4.9.15 Procedure for Suspension Request 25
4.9.16 Limits on Suspension Period 25
4.10 Certificate Status Services 25
4.10.1 Operational Characteristics 25
4.10.2 Service Availability 25
4.10.3 Optional Features 25
4.11 End of Subscription 25
4.12 Key Escrow and Recovery 25
4.12.1 Key Escrow and Recovery Policy and Practices 26
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 26
5 MANAGEMENT, OPERATIONAL, and PHYSICAL CONTROLS 26
5.1 Physical Security Controls 26
5.1.1 Site Location and Construction 26
5.1.2 Physical Access 26
5.1.3 Power and Air Conditioning 27
5.1.4 Water Exposures 27
5.1.5 Fire Prevention and Protection 27
5.1.6 Media Storage 27
5.1.7 Waste Disposal 27
5.1.8 Off-site Backup 28
5.2 Procedural Controls 28
5.2.1 Trusted Roles 28
5.2.2 Number of Persons Required Per Task 28
5.2.3 Identification and Authentication for Each Role 29
5.2.4 Roles Requiring Separation of Duties 29
5.3 Personnel Security Controls 29
5.3.1 Qualifications, Experience, and Clearance Requirements 29
5.3.2 Background Check Procedures 30
5.3.3 Training Requirements 30

5.3.4 Retraining Frequency and Requirements 30
5.3.5 Job Rotation Frequency and Sequence 31
5.3.6 Sanctions for Unauthorized Actions 31
5.3.7 Independent Contractor Requirements 31
5.3.8 Documentation Supplied to Personnel 31
5.4 Audit Logging Procedures 32
5.4.1 Types of Events Recorded 32
5.4.2 Frequency of Processing Log 33
5.4.3 Retention Period for Audit Log 33
5.4.4 Protection of Audit Log 33
5.4.5 Audit Log Backup Procedures 34
5.4.6 Audit Collection System (Internal vs. External) 34
5.4.7 Notification to Event-Causing Subject 34
5.4.8 Vulnerability Assessments 34
5.5 Records Archival 35
5.5.1 Types of Records Archived 35
5.5.2 Retention Period for Archive 36
5.5.3 Protection of Archive 36
5.5.4 Archive Backup Procedures 36
5.5.5 Requirements for Time-Stamping of Records 36
5.5.6 Archive Collection System (Internal or External) 36
5.5.7 Procedures to Obtain and Verify Archive Information 37
5.6 Key Changeover 37
5.7 Compromise and Disaster Recovery 37
5.7.1 Incident and Compromise Handling Procedures 38
5.7.2 Computing Resources, Software, and/or Data are Corrupted 38
5.7.3 Entity Private Key Compromise Procedures 39
5.7.4 Business Continuity Capabilities After a Disaster 40
5.8 STI-CA Termination 40
5.9 STI-CA Authority to Issue STI Certificates is Withdrawn 41
6 TECHNICAL SECURITY CONTROLS 41
6.1 Key Pair Generation and Installation 41
6.1.1 Key Pair Generation 41

6.1.2 Private Key Delivery to Subscriber 41
6.1.3 Public Key Delivery to Certificate Issuer 41
6.1.4 CA Public Key Delivery to Relying Parties 42
6.1.5 Key Sizes 42
6.1.6 Public Key Parameters Generation and Quality Checking 42
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 42
6.2 Private Key Protection and Cryptographic Module Engineering Controls 42
6.2.1 Cryptographic Module Standards and Controls 42
6.2.2 Private Key (n out of m) Multi-person Control 43
6.2.3 Private Key Escrow 43
6.2.4 Private Key Backup 43
6.2.5 Private Key Archival 43
6.2.6 Private Key Transfer Into or From a Cryptographic Module 43
6.2.7 Private Key Storage on Cryptographic Module 43
6.2.8 Method of Activating Private Key 44
6.2.9 Method of Deactivating Private Key 44
6.2.10 Method of Destroying Private Key 44
6.2.11 Cryptographic Module Rating 44
6.3 Other Aspects of Key Pair Management 44
6.3.1 Public Key Archival 44
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 45
6.4 Activation Data 45
6.4.1 Activation Data Generation and Installation 45
6.4.2 Activation Data Protection 45
6.4.3 Other Aspects of Activation Data 45
6.5 Computer Security Controls 45
6.5.1 Specific Computer Security Technical Requirements 45
6.5.2 Computer Security Rating 49
6.6 Life Cycle Security Controls 49
6.6.1 System Development Controls 49
6.6.2 Security Management Controls 50
6.6.3 Life Cycle Security Controls 50
6.7 Network Security Controls 50

6.8 Time-stamping 50
7 CERTIFICATE, CRL AND OCSP PROFILES 51
7.1 Certificate Profile 51
7.1.1 Version Numbers 53
7.1.2 Certificate Content and Extensions 53
7.1.3 Algorithm Object Identifiers 53
7.1.4 Name Forms 53
7.1.5 Name Constraints 53
7.1.6 Certificate Policy Object Identifier 53
7.1.7 Usage of Policy Constraints Extension 53
7.1.8 Policy Qualifiers Syntax and Semantics 54
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 54
7.2 CRL Profile 54
7.2.1 Version Numbers 54
7.2.2 CRL and CRL Entry Extensions 54
7.3 OCSP Profile 54
8 COMPLIANCE AUDIT AND OTHER ASSESSMENT 54
8.1 Frequency or Circumstances of Assessment 54
8.2 Identity / Qualifications of Assessor 55
8.3 Assessor's Relationship to Assessed Entity 55
8.4 Topics Covered by Assessment 55
8.5 Actions Taken as a Result of Deficiency 55
8.6 Communication of Results 56
9 OTHER BUSINESS AND LEGAL MATTERS 56
9.1 Fees 56
9.1.1 Certificate Issuance or Renewal Fees 56
9.1.2 Certificate Access Fees 56
9.1.3 Revocation Access Fees 56
9.2 Financial Responsibility 56
9.2.1 Insurance Coverage 56
9.2.2 Other Assets 56
9.2.3 Insurance or Warranty Coverage 57
9.3 Confidentiality of Business Information 57

9.3.1 Scope of Confidential Information 57
9.3.2 Information Not Within the Scope of Confidential Information 57
9.3.3 Responsibility to Protect Confidential Information 57
9.4 Privacy of Personal Information 57
9.4.1 Privacy Plan 57
9.4.2 Information Treated as Private 57
9.4.3 Responsibility to Protect Private Information 57
9.4.4 Disclosure Pursuant to Judicial or Administrative Process 57
9.5 Intellectual Property Rights 58
9.6 Representations and Warranties 58
9.6.1 STI-CA Representations and Warranties 58
9.6.2 Relying Party Representations and Warranties 58
9.6.3 Subscriber Representations and Warranties 59
9.7 Disclaimers of Warranties 59
9.8 Limitations of Liability 60
9.9 Indemnities 60
9.9.1 Indemnification by an Issuing STI-CA 60
9.9.2 Indemnification by Subscribers 60
9.9.3 Indemnification by Relying Parties 60
9.10 Term and Termination 61
9.10.1 Term 61
9.10.2 Termination 61
9.10.3 Effect of Termination and Survival 61
9.11 Individual Notices and Communications with Participants 61
9.12 Amendments 62
9.12.1 Procedure for Amendment 62
9.12.2 Notification Mechanism and Period 62
9.12.3 Circumstances Under which OID Must be Changed 62
9.13 Dispute Resolution Procedures 62
9.14 Governing Law 62
9.15 Compliance with Applicable Law 62
9.16 Miscellaneous Provisions 63
9.16.1 Entire Agreement 63

9.16.2 Assignment 63
9.16.3 Severability 63
9.16.4 Force Majeure 63
9.17 Other Provisions 63

1 Introduction

SSL Corp, operating under the trade name Telecert, has created the Telecert Public Key Infrastructure ("Telecert PKI"). This CPS lays out the standards and procedures for Telecert's certificate issuance services for the Telecert PKI, as well as the practices employed to adhere to the STI-PA SHAKEN Certificate Policy and other relevant policies.

This practice statement should be read together with the STI-PA Shaken Certificate Policy. Unless otherwise defined in §1.6 of this document, all terms and acronyms defined in the CP retain their meanings in this document.

The Telecert PKI complies with the latest version of the STI-PA guidelines for issuing SHAKEN certificates. In case of any inconsistency between this CPS and the STI-PA Certificate Policy and operational requirements, the STI-PA will take precedence.

The Telecert CPS uses the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647). In accordance with RFC 3647, this CPS is organized using numbered paragraphs. To preserve the outline specified by RFC 3647, items that do not currently apply to Telecert PKI have the statement "Not applicable" or "No stipulation".

This CPS applies to all entities and individuals utilizing Telecert PKI certification services.

Other important documents also apply to Telecert PKI certification services. These include public documents (such as agreements with Subscribers and other its customers, Relying Party agreements, and the Telecert privacy policy, and its terms of use) and private documents governing internal operations.

This CPS and related agreements referenced within this document are available online at https://www.telecert.com/repository/.

1.1 Overview

This document is a detailed list of the practices and policies that must be adhered to by the Telecert PKI, as authorized by the STI-PA to serve as trusted STI-CAs in the SHAKEN ecosystem. Only entities that have been granted a valid STI-PA-issued SPC token, as defined in [ATIS-1000074.v003], [ATIS-1000080.v005], and [ATIS-1000092.v002], are eligible to obtain a certificate.

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

1.2 Document Name and Identification

This document is the Telecert Certificate Practices Statement and was approved for publication by the Telecert Policy Management Authority (PMA).

The Telecert CPS serves as Telecert's PKI documentation and regulatory framework. It follows the requirements of the SHAKEN Certificate Policy and acts as the Certification Practice Statement (CPS) for Telecert's operations.

This document is the CPS for the following Certification Authorities:

CA Type	CA Distinguished Name	Key pair type and parameters	SHA-256 Key Fingerprint	Validity Period
Root CA	C=US,ST=Texas,L=Houston,O=SSL Corporation,CN=Telecert SHAKEN Root CA ECC R1	Algorithm: EC Public Key (1.2.840.10045.2.1) Named Curve: Prime256v1 (1.2.840.10045.3.1.7)	77:1B:F8:EB:B0:A6:D8:FD:14:5E:58:FC:DB:13:4C:18:E4:03:27:6F:6A:ED:B6:F6:0B:D1:AE:45:34:AA:2C:A2	1 Nov 2023, 4:05 p.m. to 25 Oct 2048, 4:05 p.m.
Issuing CA	CN=Telecert SHAKEN Issuing CA ECC 1,O=SSL Corporation,L=Houston,ST=Texas,C=US	Algorithm: EC Public Key (1.2.840.10045.2.1) Named Curve: Prime256v1 (1.2.840.10045.3.1.7)	E0:05:D5:12:C5:E1:28:EB:80:03:8E:3C:A7:1F:26:E4:2C:C7:28:3C:85:87:9F:4A:96:A2:F2:2C:27:3E:3F:5C	6 Feb 2024, 3:09 p.m. to 4 Feb 2029, 3:09 p.m.

Version Control

Version	Date	Information
1.0	**October 6, 2023**	PMA Approved Version
1.1	**November 2, 2023**	Updates per v1.4 of the SHAKEN CP
1.2	**December 12, 2023**	Additional improvements to allign with v1.4 of the SHAKEN CP

Version	Date	Information
1.3	**March 1, 2024**	Updates per feedback by SHAKEN PMA
1.4	**April 3, 2024**	Updates per feedback by SHAKEN PMA

This version of the Telecert CPS has been assigned the following Object Identifier [OID]: 1.3.6.1.4.1.38064.1.2.1.1.4 {iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) SSL.com (38064) certificationServicesProvision (1) Other Policies (2) Telecert CPS (1) Version (1.4)}.

Subsequent revisions to this CPS will contain new OID extensions corresponding to the Telecert CPS version.

Certificate profiles described in Section 7.1 and each Subordinate CA and end-entity certificate issued under this CPS includes OID for the CP [2.16.840.1.114569.1.1.4] in the *certificatePolicies* extension.

1.3 PKI Participants

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

1.3.1 Certification Authorities

This CPS applies to Telecert PKI.

1.3.2 Registration Authorities

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

1.3.3 Subscribers

The Subscribers are the SPs that request end-entity STI Certificates in order to sign a PASSporT (including SHAKEN [RFC 8588]) in the SIP [RFC 3261] Identity header field [RFC 8224], or intermediate STI Certificates to be used as the parent certificate of delegate certificates issued to VoIP Entities as specified in [ATIS-1000092.v002].

See also the definition of “Subscriber” in Section 1.6.1 Definitions.

1.3.4 Relying Parties

The relying parties are those parties that use a Subscriber’s certificate to verify the authenticity of the calling party identity per the procedures defined in [RFC 8224], [ATIS-1000074.v003] and [ATIS-100092.v002].

See also the definition of “Relying Party” in Section 1.6.1 Definitions.

1.3.5 Other Participants

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

In accordance with Telecert’s Subscriber Agreement and CPS, the use of Private Keys and Certificates by subscribers is regulated. These agreements specify that relying parties are restricted to employing end-entity Certificates solely for the authentication of caller metadata through the signing of SHAKEN PASSporTs, as outlined in [ATIS-1000074.v003], along with any other PASSporT extensions designated for use within the SHAKEN ecosystem. Subsequently, Relying Parties utilize the SHAKEN PASSporTs to verify the authenticity of the calling party within the SP’s VoIP network, as described in [ATIS-1000074.v003].

The STI-GA acknowledges the recognition of the following additional PASSporT extensions: ‘div’ [ATIS1000085.v002], ‘rph’ [ATIS-1000078], and ‘rcd’ [ATIS-1000094]. These extensions are validated using end entity certificates within the Telecert PKI trust model. Meanwhile, intermediate STI Certificates within the same model are exclusively designated for signing delegate certificates issued by Subscribers to VoIP Entities, in accordance with [ATIS-1000092.v002]. Furthermore, non-revoked certificates may be used to process requests for certificate renewal or rekey functions, as detailed in Section 3.3.

1.4.2 Prohibited Certificate Uses

Any use other than described in Section 1.4.1, or outside of the SHAKEN eco-system, or not allowed by STI-GA policies are prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS document is maintained by the Telecert PMA.

1.5.2 Contact Person

The Telecert PMA can be contacted via the following methods:

- Mail: 3100 Richmond Ave, Suite 405, Houston, Texas 77098, USA
- Email: legal@ssl.com
- Phone: +1-877-775-7328

• Fax: +1-832-201-7706

Contact information for Certificate Problem Reports can be found at:
https://www.telecert.com/revoke/

1.5.3 Entity Determining CPS Suitability for the Policy

The PMA is responsible for determining the suitability of this CPS.

1.5.4 CPS Approval Procedures

Telecert maintains consistent oversight of modifications to the SHAKEN Certificate Policy. When officially informed of a new SHAKEN CP publication, Telecert will present an updated CPS to the PMA within 45 days. After the revised CPS gains approval, all certificates issued by the Telecert PKI will align with the new CPS requirements within 90 days.

Regarding other alterations, the Telecert PMA employs a structured review process, updating the CPS solely upon approval from the Telecert PMA.

1.6 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.

1.6.1 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.

ACME Protocol: A protocol used for validation, issuance, and management of digital certificates. The protocol is an open standard that is managed by the IETF.

Applicant: An entity applying for a certificate.

Basic Constraints extension: The Basic Constraints extension identifies whether the subject of the certificate is a CA.

(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.

Certificate Chain: See Certification Path.

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].

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].

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].

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].

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 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].

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

Delegate Certificate: A certificate whose parent certificate contains a TNAuthList extension, as defined in [RFC 9060] and [ATIS-1000092.v002].

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.

End Entity STI Certificate: An STI Certificate containing a Basic Constraints extension with a CA boolean set to false.

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.

Intermediate STI Certificate: An STI Certificate containing a Basic Constrains extension with a CA boolean set to true.

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. NOTE: Region is not intended to be a region within a country (e.g., a region is not a state within the US).

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 STI-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 relying on certificate-provided information, including another entity's public key value [RFC 5217]. Relying parties are those who use a Subscriber's certificate to authenticate the calling party's identity as specified in [RFC 8224], [ATIS-1000074.v003], and [ATIS-100092.v002].

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

Secure Telephone Identity (STI) Certificate: A certificate containing a TNAuthList extension as defined in [RFC 8226] and [ATIS-1000080.v005]. The TNAuthList contains a single SPC value that identifies the SHAKEN SP holding the certificate. All STI Certificates include the Basic Constraints extension.

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. The SPC token also contains a CA boolean that authorizes the SHAKEN SP to obtain end entity STI Certificates (CA boolean false), or intermediate STI Certificates (CA boolean true).

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 an end entity STI Certificate in order to sign a PASSporT (including SHAKEN [RFC 8588]) in the SIP [RFC 3261] Identity header field [RFC 8224], or requests an intermediate STI Certificate to be used as the parent certificate to delegate certificates issued to VoIP entities [ATIS-1000092.v002].

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].

Trusted Role: A role performed by a person who can introduce security problems if not carried out properly, whether accidentally or maliciously.

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.

VoIP Entity: A non-STI-authorized end-user entity or another calling entity that acquires delegated telephone numbers from a TN Service Provider, for example, call centers, value-added service providers, and VoLTE subscribers.

1.6.2 Acronyms

Short Term	Explained Term
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
CSR	Certificate Signing Request
DN	Distinguished Name
ECDSA	Elliptic Curve Digital Signature Algorithm
FCC	Federal Communications Commission
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

Short Term	Explained Term
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-GA	Secure Telephone Identity Governance Authority
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

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.v003, Signature-based Handling of Asserted Information using Tokens (SHAKEN).[1]

ATIS-1000080.v005, Signature-based Handling of Asserted Information using Tokens (SHAKEN): Governance Model and Certificate Management.[1]

ATIS-1000084.v003, Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrator.[1]

ATIS-1000092.v002, Signature-based Handling of Asserted Information using Tokens (SHAKEN): Delegate Certificates.[1]

ATIS-0300251.a.2020, Codes for Identification of Service Providers for Information Exchange.[1]

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

FIPS 140-2, Security Requirements for Cryptographic Modules.[3]

FIPS 186-4, Digital Signature Standard (DSS).[3]

NIST SP 800-88, Guidelines for Media Sanitization.[3]

NIST SP 800-147, BIOS Protection Guidelines.[3]

NIST SP 800-147B, BIOS Protection Guidelines for Servers.[3]

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 5480, Elliptic Curve Cryptography Subject Public Key Information.[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]

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]

RFC 9060, STIR Certificate Delegation.[2]

X.501, ITU-T Recommendation X.501 (2005) | ISO/IEC 9594-2:2005, Information technology - Open Systems Interconnection The Directory: Models.[4]

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.
3. This document is available from the National Institute of Standards and Technology (NIST) at: https://csrc.nist.gov/publications.
4. This document is available from the ITU-T at: http://www.itu.org.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

In the SHAKEN ecosystem, the responsibility for publishing public certificates into a certificate repository (STI-CR) that is publicly accessible to all relying parties lies with the SP. As an STI-CA, Telecert does not maintain an STI-CR.

2.1 Public Repositories

Telecert has established a centralized repository that provides access to various documents pertaining to the company's policies and practices, such as this CPS, agreements for Subscribers and Relying Parties, and root Certificates. The repository can be accessed through the following URL: https://www.telecert.com/repository/.

2.2 Publication of Certification Information

Telecert reminds all Subscribers that they are required to publish all end-entity certificates that they receive from an STI-CA via a publicly available certificate repository system (STI-CR). The Subscriber shall ensure certificates are published in a repository accessible to all relying parties within the VoIP network for the validity period of the end entity certificate.

The Subscriber shall notify and provide the STI-PA with any revoked certificates that shall be placed on the CRL via the STI-PA UI. It is required that the certificate being revoked be uploaded as part of the revocation process.

2.3 Time or Frequency of Publication

The Subscriber is required to make any issued certificate publicly available within 24 hours of its issuance.

New or revised Telecert CPS, Terms of Service, Privacy Policy, and Subscriber Agreement are promptly accessible to the public, generally within seven days of receipt or approval. The Telecert PMA submits CPS documents for approval by the PMA as required by publication of a new CP, or changes to the policy/processes of the Telecert PKI.

Newly created Telecert Root CA certificates are delivered to the STI-PA within 7 days of approval by the PMA and at least 1 week prior to the expiration of the current root being stored by the STI-PA for distribution to the SPs.

2.4 Access Controls on Repositories

Unrestricted access for reading is granted to the Telecert Policy and Legal Repository as well as the Subscriber's certificate repository (CTI-CR). However, access to writing is safeguarded through both logical and physical controls.

3 IDENTIFICATION AND AUTHENTICATION

The following sub-sections describe the procedures used to authenticate the identity and other attributes of an SP prior to issuing certificates to the SP. This includes Telecert's support for 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.v005], [ATIS-1000092.v002] and[draft-ietf-acme-authority-tokentnauthlist]. The fingerprint in the SPC token is based on the public key associated with the SP's account ACME credentials.

3.1 Naming

3.1.1 Type of Names

Telecert Certificates must comply with the rules for naming and identification, which require assigning to each Subscriber a Distinguished Name (DN) that conforms to the ITU X.501 standard. Issuer and subject DNs shall include single country name (C), which shall be "US" for all certificates produced under this policy, single organizationName (O), and single commonName (CN) naming attributes. The organizationName and commonName values will meet all requirements in regulatory documents, [ATIS-100080.v005] and [ATIS-100092.v002]. Telecert may include the 'serialNumber' attribute to distinguish among successive instances of certificates issued to the same entity.

3.1.2 Need for Names to be Meaningful

Telecert's issued certificates must have a unique, clear, and unequivocal Distinguished Name (DN). Telecert will ensure that certificates utilize a meaningful, unambiguous, and unique Distinguished Name (DN).

3.1.3 Anonymity or Pseudonymity of Subscribers

Not applicable.

3.1.4 Rules for Interpreting Various Name Form

No stipulation.

3.1.5 Uniqueness of Name

The complete combination of Subject Attributes (Distinguished name) must be distinct within Telecert's PKI. Unique elements/attributes of the certificate depend on the certificate type.

RDN	Value
Country	US
Organization	{Legal Name of Reporting Entity}
Common Name	SHAKEN {OCN}
Serial Number	{Unique string}

3.1.6 Recognition, Authentication, and Role of Trademarks

No additional stipulations.

3.2 Initial Identity Validation

Telecert supports the SHAKEN model for identification, which 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

To apply for a Telecert certificate, an Applicant is required to provide a Certificate Signing Request (CSR) to prove their ownership of the Private Key that corresponds to the Public Key to be included in the requested certificate. Each ACME request is authenticated using an ACME account key pair. The applicant uses the private key of this pair to sign all messages. The public key taken from the CSR will be used to verify each such message prior to issuance, as verification of ownership of the private key.

3.2.2 Authentication of Organization Identity

The certificate subject's distinguished name (DN) must include the Country (C) naming attribute along with other Subject Identity Information. Telecert is responsible for confirming the identity of the service provider (SP) and verifying the authenticity of the SP Applicant Representative's certificate request through a verification procedure outlined in the Telecert's CPS. At the very least, this process entails validating the SP and ensuring the possession of a valid SPC token.

Telecert will verify the legal existence, legal name, assumed name, legal form, and requested address of the organization, and confirm the authority of the requesting party. Any document used for these purposes shall be inspected by Telecert for any alteration or falsification.

Telecert allows Applicants to provide the FCC Form 499 Filer ID number of the organization they would like a certificate for. Telecert will use this information with the FCC Form 499 Filer Database to determine the following:

- Current registration by the Applicant with the FCC
- The full Legal Name of the Applicant Organization
- The Primary (Headquarters) Address of the Applicant Organization
- The CORESID of the Applicant Organization

Telecert will use the CORESID along with the FCC Registration Database to determine the email address of the registered contact at the Applicant Organization.

The Applicant Representative will be provided with a one-time use, short lived, cryptographically generated code that they must provide to the registered contact at the organization, out of band.

Telecert will then send an email to the registered organization contact notifying them that the applicant has requested the ability to acquire certificates on behalf of their organization. Included in the email will be a secure, unique link where the contact may enter the code provided to the applicant. Provided that the code is submitted within a set time period not to exceed 30 days, the applicant is approved to submit requests for certificates on behalf of the organization.

3.2.3 Authentication of Individual Identity

Telecert shall verify the Applicant's name and the authenticity of the certificate request.

Telecert SHALL verify:

- the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). Telecert SHALL inspect the copy for any indication of alteration or falsification.

- the Applicant's address using a form of identification that the CA determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. Telecert MAY rely on the same government-issued ID that was used to verify the Applicant's name.

Telecert shall rely on strong identity proofing, based on a face-to-face meeting with the Applicant, or a procedure that provides an equivalent assurance. The latter may include any of the following:

- means of secure video communication;

- use of identity verification software/AI;

- hybrid or other methods.

After successful verification of the Applicant's identity, Telecert may then uses both the FCC Form 499 Filer Database and FCC Registration Database to verify the applicant's affiliation with

the organization. Alternatively, Telecert may contact the organization using already authenticated means of communication to verify the authority of the Applicant.

3.2.4 Non-verified Subscriber Information

Certificates shall not contain information that has not been verified.

3.2.5 Validation of Authority

Telecert is committed to verifying the authorization of all certificate requests. Telecert will perform ID verification on applicant representatives and verify their affiliation to the subject organization via industry-standard methods such as confirmation via Reliable Means of Communication, or confirmation via FCC Form 499 Filer Database and/or FCC Registration Database.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

Not applicable. Re-key requests are not supported.

3.3.1 Identification and Authentication for Routine Re-key

Not applicable. Re-key requests are not supported.

3.3.2 Identification and Authentication for Re-key after Revocation

Not applicable. Re-key requests are not supported.

3.4 Identification and Authentication for Revocation Requests

Revocation requests shall be performed by STI-CA subscribers directly to the STI-PA via their STI-PA account. The specific certificate to be revoked needs to be identified, and the reason for revocation and invalidity date need to be documented. STI-CA subscribers shall notify the STI-PA as soon as possible in the case that a certificate is required to be revoked. This should be performed via the STI-PA UI, which requires the actual certificate being revoked to be uploaded as part of the revocation process. However, should any revocation request be made directly to Telecert, the request will be sent onward to the STI-PA as per the requirement in Section 4.9.2.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The chapter outlines the policy, procedures, and requirements necessary for managing Certificates throughout their entire life cycle.

4.1 Certification Application

4.1.1 Who Can Submit a Certificate Application

Applicants must have a valid SPC Token issued by the STI-PA in order to request certificates from Telecert. 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.v005] and [ATIS-1000092.v002], to prove that it is authorized to obtain STI Certificates.

4.1.2 Enrollment Process and Responsibilities

Prior to the issuance of a certificate, Telecert shall obtain the following documentation from the Applicant:

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

In particular, to obtain a Telecert certificate, the enrollment process shall include the following steps:

- Submission of the certificate application
- Creation of a Key Pair using secure methods
- Delivery of the SPC Token and the Public Key of the Key Pair to Telecert
- Acceptance of the applicable Subscriber Agreement
- Payment of any applicable fees

Please note that the sequence of these events may differ based on the method used and the product ordered. Telecert will obtain any additional documentation and perform any other necessary steps to meet the requirements for the requested product.

For certificates issued with the ACME protocol, the procedures outlined in [ATIS-1000080.v005] and [ATIS-1000092.v002] shall be followed in order to create an account with Telecert.

4.2 Certification Application Processing

Telecert performs all identification and authentication functions in accordance with the STI-PA CP. This includes validation per CPS Section 3.2.2.

Certificate information is verified using data and documents obtained no more than 90 days prior to issuance of the certificate.

4.2.1 Performing Identification and Authentication Functions

The procedures outlined in Chapter 3 shall be followed for the initial identity verification of the applicant and validation or the organizational identity. It is mandatory that successful validation is achieved through these identification and authentication procedures, as well as compliance with all CA policies, before issuing any certificate.

4.2.2 Approval or Rejection of Certificate Applications

Telecert will decline any certificate request with information that cannot be verified. Furthermore, Telecert reserves the right to refuse the request for any certificate that could harm, reduce, or otherwise negatively impact Telecert's business or reputation, based on its own discretion. Telecert shall provide a reason for rejecting a certificate application.

4.2.3 Time to Process Certificate Applications

After validation of the applicant and the organization's identities, an account will be considered authorized. Once an account has been authorized, certificate requests will typically be processed within a few seconds, but such processes will not take more than 24 hours.

4.3 Certificate Issuance

In the case of STI-CAs that support the ACME protocol, the procedures for certificate issuance depend on the type of STI Certificate as follows:

- For issuing end entity STI Certificates, the procedures described in [ATIS- 1000080.v005] and [RFC 8555] shall be followed.
- For issuing intermediate STI Certificates, the procedures in [ATIS-1000092.v002] shall be followed.

For CP revisions that place new requirements on end-entity certificates, Telecert shall comply with the new requirements for all newly assigned certificates within 90 days of the approval of the revised CPS.

For certificates issued under a previous version of the CP, the new requirements will not need to be applied until 90 days after the effective date of the new CP and until those certificates are renewed or re-keyed.

4.3.1 STI-CA Actions During Certificate Issuance

Telecert is obligated to validate all information provided before issuing any certificate. Telecert will only issue a certificate if it determines that the request is acceptable.

This validation is done according to the procedures in [ATIS-1000080.v005] and [RFC 8555].

Once authorized and validated the certificate is signed by a Subordinate CA in an HSM. After issuance is complete, the certificate is stored in a database, published to a well known URL and made available to the Subscriber.

4.3.2 Notification to Subscriber by the STI-CA of Issuance of Certificate

Subscriber certificates are made available to Subscribers via the ACME protocol as soon after issuance as reasonably possible. Typically, this happens within a few seconds.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

As detailed in Section 2.2.

4.4.2 Publication of the Certificate by the STI-CA

Telecert shall make all Subscriber Certificates available via the ACME protocol.

Section 2.2 of this document has information about the publishing of Root and Subordinate CA Certificates.

4.4.3 Notification of Certificate Issuance by the STI-CA to Other Entities

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

4.5 Key Pair Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers who use certificates issued through the Telecert PKI must ensure that the Private Key for the certificate is protected. This includes:

- Taking measures to secure the Private Key and any copies to prevent disclosure or compromise
- Using the Private Key and/or certificate only in accordance with the relevant terms of service and/or Subscriber Agreement
- Discontinuing use of the Private Key after the expiration or revocation of the associated certificate
- Informing the issuing entity and the STI-PA if the Private Key is compromised

- Using the certificate only as applicable and for the intended purpose specified in the key usage field of the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Any SP that receives a SIP Identity header field with a STI Certificate signed PASSporT must verify the information. Before using the STI public key certificate, the SP shall perform digital signature per procedures defined in [ATIS-1000074.v003] and [ATIS-1000092.v002], as well as ensure that the certificate was issued by a STI-CA that is on the list of Trusted Root CAs, as provided by the STI-PA, and the certificate is not included in the CRL. The Relying Party shall ensure that the list of Trusted Root 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

Certificate renewal requests are treated as applications for new certificates.

4.6.1 Circumstance for Certificate Renewal

A Subscriber must request issuance of a new certificate prior to the expiration date of the current certificate. Subscribers are recommended to request issuance of the new certificate at least 24 hours prior to expiration of the existing certificate.

4.6.2 Who May Request Renewal

Not applicable. Renewals are treated as applications for new certificates and may only be requested by the Subscriber.

4.6.3 Processing Certificate Renewal Requests

Not applicable. Renewals are treated as applications for new certificates.

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

As detailed in Section 2.2.

4.6.6 Publication of the Renewal Certificate by the STI-CA

Telecert shall make all Subscriber Certificates available via the ACME protocol.

4.6.7 Notification of Certificate Issuance by the STI-CA to Other Entities

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

4.7 Certificate Re-key

Certificate re-keys are treated as applications for new certificates.

4.7.1 Circumstance for Certificate Re-key

Not applicable. Certificate re-keys are treated as applications for new certificates.

4.7.2 Who May Request Certification of a New Public Key

Not applicable. Certificate re-keys are treated as applications for new certificates.

4.7.3 Processing Certificate Re-keying Request

Not applicable. Certificate re-keys are treated as applications for new certificates.

4.7.4 Notification of New Certificate Issuance to Subscriber

Not applicable. Certificate re-keys are treated as applications for new certificates.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Not applicable. Certificate re-keys are treated as applications for new certificates.

4.7.6 Publication of the Re-keyed Certificate by the STI-CA

Not applicable. Certificate re-keys are treated as applications for new certificates.

4.7.7 Notification of Certificate Issuance by the STI-CA to Other Entities

Not applicable. Certificate re-keys are treated as applications for new certificates.

4.8 Certificate Modification

Certificate modification is not supported.

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

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the STI-CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the STI-CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

The Telecert CPS defines "revocation" as the addition of the serial number of a certificate issued via the Telecert PKI to a Certificate Revocation List (CRL), an Online Certificate Status Protocol (OSCP), and any other relevant database that is used for blocklisting, as described in [ATIS-1000080.v005].

Telecert is responsible for verifying all revocation requests. Certificates eligible for inclusion in the Telecert managed CRL encompass end-entity or intermediate certificates authorized through SPC tokens or approved Telecert's intermediate STI Certificates. Delegate Certificates generated following the procedures outlined in [ATIS-1000092.v002] are exempt from inclusion in the Telecert's CRL.

4.9.1 Circumstances for Revocation

An Intermediate CA Certificate or End Entity Certificate shall be revoked if there is reason to be believe there has been a compromise of the respective private key (RFC 5280 CRLReason #1). Other reasons for certificate revocation include:

- Affiliation Changed (RFC 5280 CRLReason #3), where, due to an organizational name change, the certificate's Subject Name field no longer identifies the certificate holder.

- Superseded (RFC 5280 CRLReason #4), where the certificate has been replaced with a new certificate.
- Cessation of operation (RFC 5280 CRLReason #5), where the Subscriber holding the certificate is ceasing operation.
- Privilege Withdrawn (RFC 5280 CRLReason #9), where the Subscriber holding the certificate is no longer authorized to obtain STI Certificates.

In addition to the above, an Intermediate CA Certificate or End Entity Certificate may also be revoked for policy violations or any other reason.

Note that if Telecert ceases operation or loses its authority to issue STI Certificates, the CA's intermediate certificates are not revoked; Certificates issued by the CA become untrusted by virtue of the removal of the CA from the Trusted STI-CA List.

4.9.2 Who Can Request Revocation

A certificate revocation can be initiated by a Subscriber with the appropriate authorization. Furthermore, a third party (such as STIGA, FCC, or other regulatory bodies specified in the policies) also holds the authority to revoke a certificate. When needed, the STI-CA can request the revocation of an end-entity or intermediate certificate it issued through the STI-PA.

4.9.3 Procedure for Revocation Request

Revocation of a certificate issued via the Telecert PKI may be initiated by the Subscriber by submitting a request to the STI-PA. In addition, a third party (i.e., STI-GA, FCC, or other regulatory bodies as identified in the policies) may also request that the STI-PA revoke a certificate.

Anyone can request assistance with revocation of any certificate from Telecert via the ACME API, provided that they can sign the revocation request with the private key associated with the certificate. These requests are proxied to the STI-PA. No other information is required in such cases.

Subscribers can request that Telecert assists in requesting revocation of certificates belonging to their accounts via the ACME API if they can sign the revocation request with the associated account private key. These requests are proxied to the STI-PA, including the specific certificate, the reason for revocation, and invalidity date.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation requests. A request for revocation must be made as soon as circumstances requiring revocation have been confirmed. Once a certificate has been identified and the revocation requester has been verified, the STI-PA shall revoke the certificate immediately by adding it to the CRL.

4.9.5 Time within which the Revocation Request must be Processed

The expected revocation timing is guided by the process per Section 4.9.4 and the revocation requestor. The timing shall consider the process of notifying the STI-PA.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties 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 Online Revocation/Status Checking Availability

Not Applicable. Telecert does not provide revocation status checking capability. Instead a 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.v005].

4.9.10 Online Revocation Checking Requirements

The Telecert PKI does not make provisions for the support of certificate status services such as Online Certificate Status Protocol (OCSP). The Telecert PKI defines an indirect CRL model in which the Subscribers can provide any revoked end-entity or intermediate certificates and STI-CAs provide any revoked intermediate certificates to the STI-PA for inclusion in the CRL. The URL to the CRL is included in the SPC token provided by the STI-PA. The STI-CA includes the URL from the token in the 'cRLDistributionPointName' field in the end entity certificate so that during path validation, the Relying Party can check whether the end entity certificate or any intermediate 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 Telecert PKI does not support Certificate suspension.

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

The Telecert PKI does not support certificate status services such as OCSP.

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

Subscribers are provided with two choices for concluding a certificate subscription. A certificate subscription will be considered terminated under the following circumstances:

1. The certificate is revoked before the date indicated in the notAfter field.
2. The certificate reaches its notAfter date and naturally expires.

Either of these options will result in the termination of the subscription. Telecert may notify Subscribers regarding the requirement for certificate renewal prior to its expiration. These notifications can be conveniently set up through the Subscriber's Telecert Account.

4.12 Key Escrow and Recovery

Not Applicable. The Telecert PKI does not support key escrow.

4.12.1 Key Escrow and Recovery Policy and Practices

Not Applicable. The Telecert PKI does not support key escrow.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not Applicable. The Telecert PKI does not support key escrow.

5 MANAGEMENT, OPERATIONAL, and PHYSICAL CONTROLS

This Section describes the technical and administrative security controls used by Telecert for key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving.

5.1 Physical Security Controls

As described in the following subsections, Telecert maintains security controls for all facilities hosting Telecert operations, including those that are not under the direct control of Telecert.

5.1.1 Site Location and Construction

Telecert PKI Facilities are located in the United States, as are all copies of Telecert CA Private Keys. Telecert conducts its operations from a secure commercial datacenter. Secure areas within the datacenter encompass critical facilities, equipped with suitable security barriers and entry controls. These measures are implemented to safeguard against unauthorized access, damage, and any form of interference.

5.1.2 Physical Access

The equipment owned by Telecert is subject to stringent physical security measures to prevent unauthorized access. These measures include:

1. Two-factor access control, which requires both physical cards and biometric readers to gain entry.
2. 24-hour video surveillance to monitor and record all activities.
3. Continuous human security presence to ensure vigilant oversight and maintain logs of access.

Rooms dedicated to support and vetting, where PKI functions take place, are secured with controlled access and keyed-lock doors. The building security system logs the usage of access cards for these areas. Additionally, video monitoring is implemented to record all entry and exit activities. It is imperative to note that unauthorized personnel seeking access to the secure data

center or the PKI operational area will never be left unsupervised, ensuring constant oversight by an authorized individual.

5.1.3 Power and Air Conditioning

The equipment utilized by Telecert is housed in a facility that employs uninterrupted power supply (UPS) units and automatic backup generators. These power sources ensure the availability of multiple redundant power options, guaranteeing continuous operation. Additionally, the heating, cooling, and ventilation (HVAC) systems within the facility are adequately designed to support the efficient functioning of the Certification Authority (CA) system.

5.1.4 Water Exposures

The equipment utilized by Telecert is located within a facility that offers safeguards against water-related incidents and exposures. Measures are in place to protect the equipment from any potential water damage.

5.1.5 Fire Prevention and Protection

The equipment used by Telecert is housed in a facility that is equipped with automatic engineered fire suppression systems specifically designed to protect and preserve electronic equipment. These systems are in place to promptly detect and suppress fires, ensuring the safety and integrity of the equipment.

5.1.6 Media Storage

Telecert ensures that all media utilized is handled and stored securely to safeguard against damage, theft, and unauthorized access. In particular, media containing Private Key material is stored offline in a secured environment. Access to private key materials is documented and all items are handled, packaged, and stored in accordance with the sensitivity level of the information it protects or grants access to. The storage protection measures employed for CA Private Key material are aligned with the specifications outlined in Section 5.1.2. These practices guarantee the integrity and confidentiality of the stored data and uphold the required security standards.

5.1.7 Waste Disposal

Paper documents or any other printed material containing Telecert PKI information or other confidential data are subjected to secure disposal methods such as shredding or destruction through an approved service. Removable media that contain Telecert PKI information or related confidential data are securely disposed of by completely destroying the media or by utilizing approved utilities to wipe or overwrite the data stored on the removable media. These practices ensure the complete eradication of sensitive information and maintain the confidentiality and integrity of Telecert's PKI operations, commensurate with those in SP 800-88.

5.1.8 Off-site Backup

A system backup shall be made when a Telecert system is activated. Telecert operational system backups shall be made at least once per week.

Telecert utilizes an off-site location for the storage and retention of backup software and data related to the Telecert PKI. This off-site storage facility is accessible to authorized personnel round the clock, 24 hours per day and 7 days per week, allowing for seamless retrieval of software and data when needed. The off-site storage facility adheres to robust physical security measures, ensuring the appropriate levels of protection against fire incidents and unauthorized access. These precautions are in place to maintain the integrity and availability of Telecert's PKI backup resources and to safeguard the stored data.

5.2 Procedural Controls

5.2.1 Trusted Roles

Within the PKI ecosystem, individuals perform their designated functions within clearly defined trusted roles. These roles are established and upheld to ensure shared responsibility, restrict individual actions, and securely separate duties and functions within the PKI framework. Trusted roles encompass various responsibilities, including but not limited to:

- **CA Administrator**: Authorized to install, configure and maintain the CA systems used for Certificate life-cycle management.
- **RA Administrator**: Certificate generation and revocation, and end entity creation and deletion.
- **System Administrator**: Responsible for operating the CA and RA systems on a day-to-day basis.
- **Network Administrator**: Responsible for operating networking equipment on a day-to-day basis.
- **Validation Specialist**: Responsible for validating the authenticity and integrity of data to be included within Certificates.
- **Security Auditor**: Responsible for internal auditing of PKI operations and responsible for administering the implementation of the security practices. This sensitive role shall not be combined with any other sensitive role, e.g. the Security Auditor shall not also be a CA Administrator. Security Auditors shall review, maintain, and archive audit logs, and perform or oversee internal audits (independent of formal compliance audits) to ensure that Telecert is operating in accordance with the CPS.

5.2.2 Number of Persons Required Per Task

Active participation by Telecert personnel is mandatory for PKI-sensitive operations. Such participation necessitates the involvement of at least two trusted individuals, who will fulfill their specified roles to carry out the required duties. To ensure the security of CA Private Keys, backup, storage, and recovery procedures must be executed by personnel in trusted roles, employing dual control measures within a physically secured environment.

It is important to note that multi-party control should not be established using personnel serving solely in the Security Auditor role, except for audit functions. The following tasks specifically require the involvement of two or more individuals:

- Generation, activation, and backup of CA keys.
- Performance of CA administration or maintenance tasks.
- Archiving or deleting CA audit logs, with at least one participant fulfilling the role of Security Auditor.
- Physical access to CA equipment.
- Access to any copy of the CA cryptographic module.

5.2.3 Identification and Authentication for Each Role

All individuals authorized in trusted roles must properly authenticate themselves before performing their duties. Background checks are performed on all Trusted Role personnel.

Trusted Role personnel authenticate themselves using unique credentials that are distinct from any credential they use to perform non-trusted role functions. This credential is coupled with multi-factor authentication to insure authorized use. Individuals holding trusted roles are appointed to the trusted role by the Policy Management Authority. These appointments shall be periodically reviewed for continued need, and renewed as appropriate. The approval by the policy authority is recorded in a secured ticketing system.

Users requiring access to a sensitive resource are required to authenticate themselves to all associated systems.

5.2.4 Roles Requiring Separation of Duties

Any trusted role as defined in Section 5.2.1 intrinsically possesses duties and/or capabilities separate from those in other trusted roles. All trusted role personnel have only one identity when accessing CA systems.

5.3 Personnel Security Controls

Telecert shall maintain personnel security controls for its operation. The personnel controls employed for CA operation are specified in the following subsections.

5.3.1 Qualifications, Experience, and Clearance Requirements

Telecert ensures that the identity and reliability of all personnel, including employees, agents, and independent contractors, are verified before engaging their services.

For individuals occupying trusted roles, as defined in Section 5.2.1, Telecert requires them to possess relevant experience and be deemed qualified for the role. Prior to performing any duties within the trusted role, personnel are required to undergo Telecert training to ensure their preparedness and competence. Telecert also performs background checks and periodic

reviews of Trusted Role job performance to ensure that only the highest quality personnel fulfill the role.

5.3.2 Background Check Procedures

Background check procedures shall apply to all CA personnel as part of Telecert's policies to ensure the integrity, suitability and trustworthiness of individuals.

Before being assigned a trusted role and being granted access to CA information, individuals shall pass through a thorough vetting process that includes, but is not limited to, the following:

- Identity verification (through government issued photo identification);
- Examination of one's public record (through research of previous employment history, relevant qualifications and criminal records).

If deemed necessary to ensure the identity and integrity of the candidate, Telecert may also check professional references, verify employment history, confirm educational degrees, verify identification via a National Identity Check (e.g., Social Security Administration records), or any combination thereof.

5.3.3 Training Requirements

Telecert is committed to delivering comprehensive training to all personnel involved in information verification duties. This training encompasses various essential areas, including, but not limited to:

- 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 CPS.

Telecert ensures that all personnel engaged in validation duties receive appropriate training and maintain a suitable skill level. The training program includes an initial examination and periodic retraining sessions to align with any changes in PKI operations. Thorough documentation is maintained for all training activities conducted.

5.3.4 Retraining Frequency and Requirements

Personnel holding any Trusted Role are required to consistently maintain skill levels commensurate with their respective roles. They are also obliged to undergo periodic retraining specific to their roles. Telecert's retraining programs are designed to encompass and address any pertinent changes in the Telecert PKI and related operations.

To ensure compliance and record-keeping, Telecert diligently maintains records of all retraining activities performed by personnel. This approach guarantees that the necessary skill levels are upheld and that individuals remain up to date with the evolving requirements of their Trusted Roles within the organization.

5.3.5 Job Rotation Frequency and Sequence

No Stipulation.

5.3.6 Sanctions for Unauthorized Actions

Failure by Telecert employees and agents to comply with the Telecert CP/CPS, whether due to negligence or malicious intent, may result in administrative or disciplinary actions. These actions can include the termination of employment or agency, as well as potential criminal sanctions.

If a Telecert employee holding a Trusted Role is found to have engaged in unauthorized actions, they will be promptly removed from that role pending the results of an investigation. Telecert management will conduct a thorough review of the incident, examining the underlying details. Once a conclusion has been reached, Telecert management will promptly issue an applicable resolution report.

The resolution process may involve termination, other forms of sanctions, or the individual being demoted to a new non-trusted role within the Telecert PKI. Additionally, retained personnel may be required to undergo additional training programs as determined by Telecert management in order to address any identified shortcomings and prevent future incidents.

5.3.7 Independent Contractor Requirements

All personnel, including independent contractors and personnel from Delegated Third Parties, who are engaged in the issuance of Certificates through the Telecert PKI, are fully bound by Telecert's CPS. This entails complying with the training and skills requirements outlined in Section 5.3.3, as well as abiding by the sanctions specified in Section 5.3.6. Furthermore, these personnel must adhere to the document retention and event logging requirements detailed in Section 5.4.1. The same expectations and obligations that apply to Telecert employees also extend to these individuals, ensuring consistency and adherence to the highest standards across all parties involved in the issuance process.

5.3.8 Documentation Supplied to Personnel

Telecert is committed to providing authorized personnel with all the necessary documentation required to carry out their job functions and duties effectively. All documentation pertinent to the duties, functions, and obligations of personnel utilizing the Telecert PKI and related functions will be readily available to authorized personnel. This documentation will be properly maintained and updated to ensure accuracy and alignment with current operations and processes.

Access to documentation specifically associated with specific Trusted Roles may be restricted to personnel holding those roles. Relevant materials will be systematically disseminated through Telecert's training and retraining programs, ensuring that personnel are equipped with up-to-date information.

Any changes made to the operations, processes, or practices pertaining to the Telecert PKI will be diligently recorded and incorporated into the corresponding documentation, reflecting the most current state of affairs. This practice ensures that personnel have access to accurate and current information in support of their roles and responsibilities.

5.4 Audit Logging Procedures

Telecert generates audit log files for all events relating to the security of the CA operation. The log information is automatically collected. Where this is not possible, Telecert uses a logbook, paper forms or other physical mechanisms to capture the information. Details of how Telecert implements the audit logging are specified in the following subsections.

Procedures are in place for the PMA and internal auditing team to review the logs on a request basis.

5.4.1 Types of Events Recorded

All security-related events concerning the Certificate Systems, Certificate Management Systems, Root CA Systems, and delegated Third Party Systems of Telecert, as well as each Delegated Third Party, are meticulously recorded in audit log files.

Whenever possible, security audit logs are generated automatically. In cases where automatic generation is not feasible, alternative methods such as logbooks, paper forms, or other physical mechanisms are employed.

The retention of all security audit logs is in accordance with the specifications outlined in Sections 5.4.3 and 5.5. These logs are preserved and made available to Qualified Auditors upon request.

Each log entry includes the following essential elements:

- Date and time of the event
- Identity of the person responsible for the journal entry
- Description detailing the nature of the event

By capturing these log elements, Telecert ensures the comprehensive documentation of security-related activities, providing a valuable resource for auditing and maintaining the integrity of the systems involved.

Examples of 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),
- Access to subscriber identification information,
- Certificate creation 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,
- Clock adjustments.

5.4.2 Frequency of Processing Log

Telecert is dedicated to monitoring the integrity of the logging processes for both application and system logs. This is achieved through continuous automated monitoring and alerting mechanisms, or alternatively, through periodic human reviews to ensure the effectiveness of logging and log-integrity functions. If a human review is employed and the system is online, the review process will take place at least once every 31 days.

Following each review, a summary of the findings, if any, will be reported to the appropriate personnel. In cases where investigations are initiated based on reported findings, any resulting recommendations and actions taken to address the identified issues will be meticulously documented. These records are made available to auditors upon request.

By actively monitoring and reviewing the logging processes, Telecert ensures the ongoing accuracy and effectiveness of the logging system, thereby maintaining the integrity and security of its operations. Telecert monitors all alert systems 24 hours a day, 7 days a week.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained for more than ninety (90) days in addition to being archived as described in Section 5.5.

Audit logs are accessible only to Trusted Role members. There is no manual removal of audit log from the CA systems.

5.4.4 Protection of Audit Log

Telecert is responsible for collecting and conducting regular analysis of pertinent audit data to detect any attempts aimed at compromising the integrity of any aspect of the Telecert PKI. Access to Telecert audit logs is restricted solely to authorized personnel and auditors. Audit logs are written only by the logging mechanism and are not modifiable by human or machine.

Telecert retains the authority to determine which audit records may be viewed by others and the specific circumstances under which such records will be made available.

To ensure the integrity and preservation of audit logs, Telecert implements protective measures against unauthorized modification or destruction. Digital logs are maintained in an encrypted format, safeguarding their confidentiality and integrity.

5.4.5 Audit Log Backup Procedures

Telecert conducts a daily onsite backup of the audit log to ensure its preservation and availability. This backup process includes the creation of a weekly copy of the audit log from the Telecert facility. To enhance security and protection, this backup is securely stored at an offsite location dedicated to maintaining the integrity of the data.

5.4.6 Audit Collection System (Internal vs. External)

The security audit process operated by Telecert operates autonomously from the Telecert PKI certificate issuance software. This ensures that the security audit processes initiate upon system start-up and continue uninterrupted until system shutdown. It is of utmost importance that these security audit processes are designed to be immune to any attempts to bypass or circumvent them, reinforcing their effectiveness and reliability in upholding security standards.

5.4.7 Notification to Event-Causing Subject

Not Applicable.

5.4.8 Vulnerability Assessments

Telecert conducts routine vulnerability assessments and penetration tests to ensure the security of all Certificate Systems. These assessments occur at least once a year and encompass a comprehensive examination of potential vulnerabilities and threats.

In addition to the regular assessments, vulnerability assessments may be carried out in the following circumstances:

- After any significant system or network changes as determined by the CA.
- At least once per quarter, targeting both public and private IP addresses identified by the CA as part of their Certificate Systems.

These assessments are designed to identify, review, and address any identified vulnerabilities and threats, following a documented vulnerability correction process. This approach ensures that necessary measures are taken to mitigate risks and enhance the overall security posture of the Certificate Systems.

5.5 Records Archival

5.5.1 Types of Records Archived

Telecert is required to maintain archives of all documentation pertaining to certificate requests, their verification process, and the issuance and revocation of Certificates.

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 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 SHAKEN CP
- Violations of Telecert's CPS

Furthermore, Telecert is obligated to archive the following:

- Documentation pertaining to the security of their Certificate Systems, Certificate Management Systems, and Root CA Systems.
- Documentation related to the verification, issuance, and revocation of certificate requests and Certificates.

Telecert is also authorized to archive any other documents deemed relevant to the operations of the Telecert PKI. By maintaining these archives, Telecert ensures the availability of historical

records necessary for auditing, compliance, and the overall management of the PKI infrastructure.

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

Archives shall be securely retained and safeguarded against any unauthorized modification or destruction for the duration specified in Section 5.5.2. Archives are maintained in a secure storage system separate from the CA systems with physical and procedural security controls equivalent to or better than those of the Telecert PKI.

Telecert is committed to implementing all necessary measures to ensure that only authorized access is granted to the archives. This ensures the integrity and confidentiality of the archived information, promoting the security and trustworthiness of the Telecert operations.

5.5.4 Archive Backup Procedures

Telecert will employ secure and verifiable backup procedures to ensure the availability of a comprehensive and easily accessible backup archive in case of primary archive loss or damage. The backup archive will be stored at a separate and secure location, distinct from the primary archive. Access to the backup archive will be protected by security protocols equivalent to those implemented for the primary archive.

To prevent data loss, maintenance of the backup archive will involve periodic transfer of archived data to new media. This practice ensures the preservation and integrity of the data, safeguarding it against any potential loss or degradation. Telecert's commitment to robust backup procedures guarantees the continuity and resilience of its archival systems.

5.5.5 Requirements for Time-Stamping of Records

All archived documents will incorporate precise timestamps indicating the date and time of their creation, occurrence, or modification. These timestamps will be sourced from a trusted time source, as defined in Section 6.8. By relying on such trusted time sources, Telecert ensures the accuracy and integrity of the timestamps associated with archived documents, enhancing the reliability and traceability of the archival records.

5.5.6 Archive Collection System (Internal or External)

Telecert shall employ internal systems to collect and maintain a primary archive. Audit logs are retained for more than 90 days.

5.5.7 Procedures to Obtain and Verify Archive Information

Access to Telecert's primary and backup archives will be restricted solely to authorized Telecert personnel and qualified auditors.

Upon request and at its discretion, Telecert may release specific records pertaining to requests made by a Subscriber or a Relying Party. However, Telecert will not disclose the archives in their entirety unless mandated by law.

In cases where access or retrieval of requested archival data is necessary, Telecert may require compensation and fees to cover associated costs.

Telecert is committed to ensuring the integrity and readability of both the primary and backup archives. To verify their reliability, periodic random testing will be conducted, thus validating the accuracy and accessibility of the archived data. This practice reinforces Telecert's commitment to maintaining high standards of data integrity and security.

5.6 Key Changeover

Telecert will ensure a secure and well-managed transition of Private Keys for any expiring Root Certificate used within the Telecert PKI.

During the key changeover process, Telecert will maintain concurrent Root Certificates, specifically the expiring Root Certificate with its associated Private Key and the new Root Certificate with the updated Private Key. This coexistence of certificates will be strictly limited to a temporary period, allowing for a seamless transition of functions and services. The temporary period will conclude upon the expiration of the original Root Certificate's Private Key.

Telecert will promptly provide Subscribers and Relying Parties with the new Public Key through the delivery methods outlined in Section 6.1.4, ensuring a smooth and uninterrupted continuation of services.

Similar key changeover and key distribution methods will be employed to manage the expiration of any cross-certified certificates, maintaining the security and reliability of the Telecert PKI ecosystem.

5.7 Compromise and Disaster Recovery

Telecert has established and maintains a comprehensive Business Continuity Plan (BCP) that outlines the necessary steps, procedures, and actions to be taken in the event of incidents or disasters that negatively impact any function of the Telecert PKI. This plan ensures that operations can be restored promptly and efficiently, minimizing any potential disruptions and enabling the continued provision of services to Subscribers and Relying Parties. The BCP serves as a strategic framework, guiding Telecert's response and recovery efforts to effectively address and mitigate the impact of adverse events on the Telecert PKI infrastructure.

5.7.1 Incident and Compromise Handling Procedures

Telecert upholds a set of policies and procedures designed to address potential or actual security compromises, natural disasters, and similar events. These policies encompass an Incident Management Policy (IMP), a Business Continuity and Disaster Recovery Plan, and various other relevant resources. It is important to note that these documents are not limited to the ones mentioned above.

Telecert is committed to regularly reviewing, testing, and updating these policies and procedures as necessary. This ensures their continued effectiveness and alignment with the evolving security landscape and operational requirements. By maintaining a proactive approach to policy and procedure management, Telecert enhances its readiness to respond to unforeseen events and maintain the continuity of its operations. If compromise of a Telecert occurs, certificate issuance by Telecert 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 Telecert private signing key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed.

Telecert shall immediately (within 24 hours) 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 Telecert from notifying the STI-PA of a revoked certificate (e.g., compromised credentials).

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

Telecert's Business Continuity Plan incorporates comprehensive measures to handle incidents involving the corruption of Computing Resources, Software, and/or Data associated with the Telecert PKI. In the event of such incidents, affected operations will be thoroughly investigated and promptly suspended as necessary. The restoration of suspended activities will be prioritized to minimize disruptions while ensuring the secure operation of the Telecert PKI.

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

- Notify the PMA director as soon as possible using the PMA contact information provided in this CP.
- 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.

To validate the effectiveness of the Disaster Recovery Plan, regular testing is conducted at least once every year. This testing enables Telecert to assess the readiness and functionality of the plan, making any necessary adjustments or improvements to enhance its response capabilities. By diligently reviewing and testing the plan, Telecert maintains a high level of preparedness to effectively address any incidents and swiftly restore operations within the Telecert PKI.

5.7.3 Entity Private Key Compromise Procedures

5.7.3.1 Root CA Compromise Procedures

In the case of the Root CA compromise, Telecert shall immediately notify the PMA. Telecert will 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.

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, Telecert shall then generate a new Root CA certificate and update its account with the STI-PA per the established CPS procedures.

CPS changes that place new requirements on an existing root (or issuing) CA will be limited to those that have been evaluated and required to address a security issue within the SHAKEN ecosystem. For such changes, the PMA will coordinate with individual STI-CAs on a practical implementation approach and schedule.

Telecert has established procedures to effectively respond to any incident involving the loss, destruction, compromise, or suspected compromise of a CA Private Key. These procedures also apply to situations where there is a compromise of the algorithms and parameters used to generate the Private Key and certificate. Following a thorough investigation of the incident, appropriate steps will be taken, which may include, but are not limited to:

- Request revocation of the affected CA Private Key
- Notification of all affected Subscribers
- Request revocation of all Certificates signed with the affected CA Private Key

Upon completion of the incident response, should it be secure and appropriate to do so and STI-PA approves, a new Root CA certificate will be created and the STI-PA will be updated with the new root certificate.

5.7.3.2 Intermediate CA Compromise Procedures

See Section 5.7.3.1.

5.7.4 Business Continuity Capabilities After a Disaster

Telecert's Business Continuity Plan is designed to ensure secure continuous operations, and/or timely and secure restoration of affected operations, in the event of an incident or disaster. The Business Continuity Plan identifies what management and operations procedures are in place to mitigate risks to facilities, systems, networks, and application controls. It also identifies 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.

Telecert's CA infrastructure resides in geographically diverse facilities, each of which is capable of operating independently, thus supporting failover in case a disaster renders a facility inoperable.

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. If Telecert cannot re-establish operational capabilities within eighteen (18) hours, then the inoperative status of the CA shall be reported to the PMA. 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 all CA installations are physically damaged and all copies of the Intermediate CA signature key are destroyed as a result, Telecert shall request that its intermediate certificates be revoked. If the Root CA is physically damaged such that all copies of the Root CA signature keys are destroyed, then the root certificate(s) shall be removed from the Trusted STI-CA List. 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.

5.8 STI-CA Termination

In the event that Telecert operating under this CPS terminates operations before all certificates have expired, entities shall be given as much advance notice as circumstances permit. The STI-CA shall notify the PMA using documented contact information, and the STI-PA shall remove the STI-CA from the Trusted STI-CA List. The STI-CA shall archive all audit logs and other records prior to termination. The STI-CA shall destroy all private keys upon termination. The STI-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 STI-CAs. In that case, any certificates that have not been revoked will be invalid once the relying parties receive the updated list.

5.9 STI-CA Authority to Issue STI Certificates is Withdrawn

If Telecert loses its authority to issue STI Certificates, then the STI-PA shall remove the Telecert roots from the Trusted STI-CA list.

6 TECHNICAL SECURITY CONTROLS

Telecert is committed to implementing and upholding suitable technical security controls that govern all operations within the Telecert PKI. These controls are designed to safeguard the integrity, confidentiality, and availability of the PKI infrastructure, ensuring the secure and reliable issuance, management, and revocation of Certificates. Telecert continuously maintains and updates these technical security controls to align with industry best practices and evolving security requirements. By doing so, Telecert ensures a robust and resilient security posture within the Telecert PKI ecosystem.

6.1 Key Pair Generation and Installation

Telecert is responsible for the generation and installation of all CA Key Pairs, which will be conducted in a physically secure environment using secure cryptographic equipment. These tasks will be performed exclusively by personnel occupying trusted roles and following the prescribed methodology outlined in Section 6.1.1. This approach ensures the utmost protection and integrity of the CA Key Pairs, maintaining the security of the Telecert PKI infrastructure.

Access to physical modules shall be controlled as detailed in Section 6.2.

6.1.1 Key Pair Generation

Telecert ensures that CA Key Pairs are exclusively generated within cryptographic modules specified in Section 6.2.

The generation process follows a Key Generation Script ceremony, involving multiple trusted individuals in specific roles. For intermediate CA keys, the process is witnessed by an internal or external audit team. External auditors may also issue an appropriate opinion report for Root Certification Authority or subordinate Authority not under the operator’s control.

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

Public key delivery to Telecert must be by methods conforming to Section 3.2.1, or through other established protocols such as ACME.

6.1.4 CA Public Key Delivery to Relying Parties

Telecert ensures the secure delivery of Public Keys to Relying Parties, minimizing the risk of substitution attacks.

Third parties as well as Subscribers and Relying Parties are authorized to use and distribute the current Telecert Root Certificate. These Root Certificates are readily available and regularly updated in the Telecert repository, ensuring accessibility and proper maintenance.

6.1.5 Key Sizes

For STI Certificates under this CPS, Telecert shall generate digital signatures with: - the Elliptic Curve Digital Signature Algorithm (ECDSA) with Curve P-256 and SHA-256 or ECDSA with Curve P-384 and SHA-384 - a NIST-approved hash function that offers the same security as the elliptic curve used by the CA. For example, the NIST P-256 curve and SHA-256 offer the same security.

6.1.6 Public Key Parameters Generation and Quality Checking

Telecert employs HSMs that adhere to [FIPS 186-4] and [RFC 5480] standards, equipped to deliver random number generation and on-board generation of ECDSA keys, each with a minimum length of 256 bits.

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

The use of a specific public key is constrained by the key usage extension, and all certificates shall include a critical key usage extension.

The private key associated with a CA certificate shall be used only for signing certificates. CA certificates whose subject public key is to be used to verify other certificates shall assert only the *keyCertSign* bit in the key usage extension.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under the SHAKEN CP. In addition, *anyExtendedKeyUsage* shall not be asserted in extended key usage extension.

See Section 7.1, Certificate Profiles for more details.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CA Private Keys are securely stored and utilized exclusively within a Hardware Security Module (HSM) designed for key signing operations. The HSM employed meets the stringent FIPS 140-2 level 3 standards, ensuring the highest level of security for the storage and usage of CA Private Keys.

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

Telecert CA Private Keys, including backups, require activation and access by multiple individuals fulfilling specific trusted roles. This “n-of-m multi-person control” approach ensures that the Private Keys can only be utilized when authorized personnel authenticate using multi-factor authentication methods.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

Telecert ensures the secure and reliable backup of CA Private Keys by multiple authorized individuals holding trusted roles. Backup copies of Telecert CA Private Keys are securely stored, following the procedures outlined in Section 5.1.6 for media storage and encryption. Access to backup copies is strictly limited to authorized personnel.

For Subscriber Certificates, the control of private key backups lies exclusively with the Subscriber, provided it is technically feasible.

Backup keys for Telecert CA Private Keys are stored solely in encrypted form, ensuring they are never stored as plain text outside of a cryptographic module (as described in Section 6.2.1).

At the end of their lifecycle, all copies of the CA Private Keys, including signing keys, are securely decommissioned.

6.2.5 Private Key Archival

Telecert shall not archive Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The transfer of Telecert CA Private Keys to and from hardware security modules is conducted through a secure and verifiable process, involving multiple individuals in designated trusted roles.

During the transfer, Telecert CA Private Keys are maintained exclusively in encrypted form and are never in plain text outside of a cryptographic module (as outlined in Section 6.2.1).

6.2.7 Private Key Storage on Cryptographic Module

Telecert securely generates, stores, and employs CA Private Keys using a dedicated Hardware Security Module, following the guidelines outlined in Section 6.2.1. Root Private Keys are stored in offline cryptographic modules or backup tokens for enhanced security.

6.2.8 Method of Activating Private Key

Telecert activates CA Private Keys following the manufacturer's instructions and specifications for the cryptographic module, employing a secure and verifiable process. This process involves multiple authorized individuals in trusted roles and incorporates multi-factor authentication.

Applicants and Subscribers are advised to adhere to the standards outlined in the relevant Subscriber Agreement to safeguard their Private Keys. The responsibility for protecting Private Keys rests solely with the Subscribers.

6.2.9 Method of Deactivating Private Key

Telecert deactivates CA Private Keys stored in cryptographic hardware when they are not in use, following documented procedures that uphold the necessary physical and logical security controls.

6.2.10 Method of Destroying Private Key

CA Private Keys are securely destroyed when they are no longer required. The destruction process involves:

- Using the secure deletion function of the Hardware Security Module (HSM) to destroy any CA Private Key stored within it, following the manufacturer's instructions. Only the specific instance of the CA Private Key stored in the HSM is destroyed.
- Ensuring the destruction of any other encrypted copies and fragments of the CA Private Key over a reasonable period of time.

When a CA cryptographic device is permanently taken out of service, the CA Private Key used for cryptographic purposes within the device is erased. If the device case provides tamper-evident characteristics and is being permanently removed from service, the case is destroyed.

The destruction of CA Private Keys and cryptographic devices is carried out exclusively by authorized personnel in trusted roles, following documented and verifiable procedures.

Subscribers bear full responsibility for securely and completely destroying all copies and fragments of their Private Key at the end of the Key Pair life cycle.

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

Telecert archives Public Keys as described in Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum validity period of CA Certificates is:

- Twenty-five (25) years for Root CAs,
- Twelve (12) years for Intermediate CAs, and
- Three (3) years for end-entity certificates.

The operational period of Key Pairs is determined based on key size and technological advancements in cryptography to ensure optimal security and efficiency.

Subscribers are advised against reusing Key Pairs when applying for new certificates.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Telecert activates and deploys Telecert CA Private Keys into cryptographic modules following the instructions and specifications provided by the module manufacturer. The initial generation, activation, and installation are performed through a CA key ceremony as outlined in Section 6.1.1.

To ensure secure access to Private Keys generated for Subscribers, separate Activation Data is generated and safeguarded.

Activation data chosen by the user can be customized. The activation data's strength must align with or surpass the authentication mechanism requirements defined for Level 3 in FIPS 140-2 or an equivalent standard. In case transmission of activation data is necessary, it should occur through a securely protected channel, separate in both time and location from the associated cryptographic module.

6.4.2 Activation Data Protection

Telecert safeguards activation data to prevent unauthorized disclosure or compromise. Robust cryptographic and physical access controls are implemented to ensure the protection of CA Private Key activation data.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Telecert PKI systems are appropriately secured in order to protect CA software and data from unauthorized access or modification. Access pathways to systems are secured via multi-factor

authentication whenever possible with unique user logins for each element in the system. Security updates are applied in a timely fashion after testing and vulnerability scans are run regularly. Additional requirements detailed below.

6.5.1.1 Access Control

Access to information such as sensitive details about customer accounts, passwords, and CA-related private keys are carefully guarded and logged. Access to the physical machines housing such information is also closely guarded and logged.

6.5.1.1.1 Access Control Policy and Procedures

Telecert has documented the roles and responsibilities for each trusted role employee job function. Telecert has also created and maintains 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

Access for operational staff and trusted role employees are limited to the functionality required to perform their specific job function.

Telecert maintains a record of accounts, along with the conditions and procedures to follow when creating new accounts, groups and roles. Groups and roles are mapped to the business function involved in operating the CA.

Telecert takes appropriate action when a user no longer requires an account, their business role changes, or the user is terminated or transferred. Telecert 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 are configured to maintain access for only those users who are actively authorized to use the information system. After thirty (30) days of inactivity, inactive accounts are automatically disabled and attempts to access any deactivated account shall be logged.

All account administration activities, including account creation, modification, enabling, disabling, group or role changes, and removal actions, are logged and are available for inspection by appropriate security personnel. Guest, default, and anonymous accounts for logon to CA operations systems disabled and prohibited. Accounts are only assigned to a single user and not shared.

6.5.1.1.3 Least Privilege

All systems utilized in the Telecert PKI, including CA servers, support and vetting workstations are configured, maintained, and secured according to industry best practices, including the principle of least privilege. Each user or system only has the necessary permissions to accomplish assigned tasks and users are required to use non-privileged accounts or roles when accessing non-privileged functions (such as reading email).

6.5.1.1.4 Access Control Best Practices

Telecert follows industry best practices for managing access control. Examples include, but are not limited to:

- Unique User IDs are 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 clear text.
- 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

In situations where Telecert PKI allows user selectable passwords, strong passwords shall be employed, as defined in the CA password policy described in Section 6.5.1.1.4. Passwords for CA authentication operational systems shall be different from CA enterprise systems.

Telecert 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 in a one hour period. Restoration of access shall be performed by a different person who holds a trusted role, or restore access after a timeout period. Whenever possible, multi-factor authentication is implemented for PKI components that support it, including accounts with certificate issuance capabilities.

6.5.1.1.6 Permitted Actions without Identification or Authentication

Not applicable. There are no privileged actions that can be performed without identification or authentication.

6.5.1.2 System Integrity

6.5.1.2.1 System Isolation and Partitioning

Telecert PKI systems are 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 are logically separated from each other and shall be logically separated from any untrusted components of the CA system.

6.5.1.2.2 Malicious Code Protection

Malicious code protection mechanisms are in place to mitigate the risk of malicious code on CA systems.

In particular:

- All CA hosts reside in the High Security Zone (physical protection).
- Insertion of removable media requires physical access to the hosts (hardware).
- Network based Malware Protection, Intrusion Prevention (IPS) and Web application security systems are utilized at boundary points.
- Application whitelisting is utilized for the deployment of any tools to the CA systems, on a need-to-use basis.
- No automated execution of removable media; manual mounting by trusted CA personnel is required.
- Security updates of system components are automatically deployed on a daily basis.

In addition, software deployment adheres to our secure processes and guidelines which requires 2-person review code commit and is exclusively carried out by trusted role personnel.

6.5.1.2.3 Software and Firmware Integrity

All software, including dependencies are maintained in a dedicated source repository and are freshly built as part of each deployment. Commitments into the master branch require third-party trusted role approval.

All firmware on associated hardware is code signed by the hardware manufacturer or the infrastructure operator and are verified prior to installation.

6.5.1.2.4 Information Protection

Telecert shall protect the confidentiality and integrity of sensitive information stored or processed on CA systems that could lead to abuse or fraud. In the most sensitive systems, cache periods are kept to a minimum and in some cases cashes are not used such to ensure the latest information is used to determine if a certificate should be issued.

Sensitive information stored on devices that are not physically protected from potential attackers shall be stored in an encrypted format.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

Telecert's system development controls encompass the following measures (among others):

- Software used for CA systems undergoes a documented development process before implementation.
- Hardware and software components of the CA system are acquired in a manner that minimizes the risk of falsification, modification, or tampering.
- Secure packing methods, including tamper proof packaging where applicable, are employed when shipping and delivering hardware for CA systems, accompanied by comprehensive tracking records.
- The hardware and software utilized in CA systems are dedicated solely to CA operations, with only necessary software, hardware, and network connections installed or permitted.
- All updates to CA systems, whether hardware or software, are documented and performed exclusively by personnel in trusted roles who have appropriate authorization.

These measures ensure the integrity and security of Telecert's CA systems throughout the development lifecycle.

6.6.2 Security Management Controls

Telecert implements comprehensive security controls and monitoring across its systems, specifically focusing on CA software configurations. A well-defined process is followed to authenticate any modifications, installations, and management activities related to software used within or in connection with CA systems. This ensures that only authorized and verified changes are made to maintain the integrity and security of the software environment.

6.6.3 Life Cycle Security Controls

Telecert conducts routine security scans on all online CA operations systems using commercial vulnerability testing tools. Each scan finding triggers a ticket for assessment of severity and relevance. Valid findings are prioritized by risk level, and high-priority issues are addressed within 72 hours if feasible. Vendor patches undergo testing before deployment, and issue resolution progress is tracked via the ticketing system. We minimize dependencies, regularly track product vulnerabilities and breach notifications, and maintain open communication with vendors for efficient issue resolution. Our extensive monitoring detects anomalies, aiding in identifying misconfigurations or compromises. All issues, regardless of severity, are promptly addressed.

6.7 Network Security Controls

Telecert employs practical safeguards and controls within its network to thwart unauthorized access to CA systems and infrastructure. The network architecture is multi-tiered, aligning with the defense-in-depth principle. Robust network security measures are in place to routinely scan and review production environments and logs for operational anomalies that might indicate a breach.

Furthermore, diligent monitoring encompasses tracking dependencies and routinely assessing CVEs and security updates from vendors for suitability and deployment. Any identified potential compromises or vulnerabilities are recorded in a ticket tracking system and addressed through the same system, including decisions on patching, remediation, or other actions.

6.8 Time-stamping

Telecert maintains the accuracy of time sources utilized in all time-stamping operations through trusted and verifiable NTP (Network Time Protocol)[RFC 5905]. To ensure the authenticity of system time, Telecert employs a combination of manual and digital processes. Additional details can be found in Section 5.5.5 of the documentation.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

Certificates issued by the Telecert shall adhere to the X.509 v3 certificate profile documented in RFC 5280. Telecert shall support the certificate extensions defined and described for STIR [RFC 8226], SHAKEN [ATIS-1000080.v005] and [ATIS-1000092.v002].

When issuing STI Certificates to a Service Provider, Telecert shall ensure that the 'cRLDistributionPointName' extension of the issued certificate contains a URL reference to the indirect CRL hosted by the STI-PA. Telecert shall also ensure that the 'cRLDistributionPointName' extension of all STI intermediate certificates in the certification path of the issued certificate contain that same CRL URL value.

(1) Root CA Certificates

Field or extension	Values
Serial Number	Serial Number Must be unique, with 64 bits of output from a CSPRNG
Issuer Distinguished Name	C: US; ST: Texas; L: Houston; O: SSL Corporation; CN: Telecert SHAKEN Root CA ECC R<m>, where m is an integer representing the instance of the Root CA Certificate.
Subject Distinguished Name	Same as Issuer Distinguished Name
Duration	Not greater than 25 years
Key Usage	Critical: True, keyCertSign: True
Basic Constraints	Critical: True, cA: True
Subject Key Identifier	Critical: False. Must be SHA1 hash of Subject public key

(2) Subordinate CA Certificates**

Algorithm	Values
Serial Number	Serial Number Must be unique, with 64 bits of output from a CSPRNG
Issuer Distinguished Name	Same as Issuer Subject DN
Subject Distinguished Name	C: US; ST: Texas; L: Houston; O: SSL Corporation; CN: Telecert SHAKEN Issuing CA ECC <m>, where m is an integer representing the instance of the Subordinate CA Certificate.
Duration	Not greater than 5 years

Algorithm	Values
Key Usage	Critical: True, keyCertSign: True
Basic Constraints	Critical: True, cA: True
Subject Key Identifier	Critical: False, Must be SHA1 hash of Subject public key
Authority Key Identifier	Critical: False, Must be SHA1 hash of Issuer public key
Certificate Policies	Critical: False. 2.16.840.1.114569.1.1.4
CRL Distribution Point	Critical: False. Distribution Point URI: https://authenticate-api.iconectiv.com/download/v1/crl; CRL Issuer Directory Name: [L: Bridgewater; ST: NJ; CN: STI-PA CRL; C: US; O: STI-PA]

(3) Subscriber Certificates**

Algorithm	Values
Serial Number	Serial Number Must be unique, with 64 bits of output from a CSPRNG
Issuer Distinguished Name	Same as Issuer Subject DN
Subject Distinguished Name	C: US; Organization: {Legal Name of Reporting Entity}; Common Name: SHAKEN {OCN}; Serial Number: {Unique string}
Duration	Not greater than 1 year
Key Usage	Critical: True. digitalSignature: True
Basic Constraints	Critical: True, cA: False
Subject Key Identifier	Critical: False, Must be SHA1 hash of Subject public key
Authority Key Identifier	Critical: False. Must be SHA1 hash of Issuer public key
Telephone Number Authorization List	Critical: False. SPC: {OCN}, …
Certificate Policies	Critical: False. 2.16.840.1.114569.1.1.4

Algorithm	Values
CRL Distribution Point	Critical: False. Distribution Point URI: https://authenticate-api.iconectiv.com/download/v1/crl; CRL Issuer Directory Name: [L: Bridgewater; ST: NJ; CN: STI-PA CRL; C: US; O: STI-PA]

7.1.1 Version Numbers

The Telecert PKI issues Certificates that adhere to X.509 Version 3 standards.

7.1.2 Certificate Content and Extensions

Telecert Certificates adhere to RFC 5280 and relevant industry best practices, as shown in Section 7.1.

A tabulated representation of the prevalent certificate profiles utilized by Telecert is provided in Annex A (Telecert Certificate Profiles).

7.1.3 Algorithm Object Identifiers

Name	Object Identifier
ecdsa-with-SHA256	1.2.840.10045.4.3.3

7.1.4 Name Forms

Telecert Certificates facilitate name chaining as defined in RFC 5280. Every issued Certificate includes a distinct and identifying serial number that is greater than 0.

7.1.5 Name Constraints

Telecert reserves the right to issue Certificates with name constraints and/or marked as critical when deemed necessary.

7.1.6 Certificate Policy Object Identifier

The OID assigned to Telecert by IANA is iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) Telecert / SSL.com (38064).

This Certification Practice Statement has been assigned the following Object Identifier [OID]: 1.3.6.1.4.1.38064.1.2.1.1.3 for Telecert CPS Version 1.4.

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

The policy qualifier field of Telecert includes information that relying parties can refer to for identifying potential limitations of a certificate.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

Not applicable.

7.2.1 Version Numbers

Not applicable.

7.2.2 CRL and CRL Entry Extensions

Not applicable.

7.3 OCSP Profile

Not applicable.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

Telecert policies are designed to meet the requirements based on [ATIS-1000080.v005] and [ATIS-1000084.v003], as well as generally accepted and published industry standards. Telecert ensures that audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated. All audit related costs are the responsibility of Telecert.

8.1 Frequency or Circumstances of Assessment

Telecert shall submit to the PMA a CP Compliance Attestation each year by February 15th based on either an independent auditor's or an independent department of Telecert's assessment of the policy compliance of Telecert.

In addition, if requested by the PMA, Telecert shall submit to the PMA a CP Compliance Attestation for a specific period of time. The CP Compliance Attestation shall include the following:

- Confirmation of compliance with the Certificate Policy standards for infrastructure, security, and business process management;
- Identification/notification of any security breach incidents in any environment supporting the STI-CA; and
- Identification/notification of any material changes in technology architecture or business processes supporting the STI-CA.

8.2 Identity / Qualifications of Assessor

External audits must be conducted by a Qualified Auditor who possesses the following attributes:

- Evidenced expertise in conducting compliance audits.
- Comprehensive understanding of the CA's CP/CPS.
- Consistent engagement in compliance audits as part of their routine business operations.
- Relevant professional background and certifications.
- Specialization in PKI subject matter.

8.3 Assessor's Relationship to Assessed Entity

The selection of the auditor occurs on a yearly basis and must either be an external private firm with no affiliation to Telecert, or it must maintain a significant organizational separation from said entities to guarantee an impartial and unbiased evaluation.

In either scenario, the auditor must not have participated in the creation or upkeep of the entity's CA Facility or CPS. The ultimate responsibility for confirming the auditor's fulfillment of the CPS-specified criteria lies with the PMA.

8.4 Topics Covered by Assessment

The assessment will encompass the documented practices of Telecert, the integrity of Issuing PKI operations, and adherence to governing CP requirements, as required by industry standards. The audit will cover each issuing CA (root certificate or subordinate) is compliant with the STI-PA's CP.

8.5 Actions Taken as a Result of Deficiency

In the event of an audit revealing a substantial failure to comply with applicable laws, this CPS, the CP, or any contractual commitments linked to Telecert's services, the following steps will be taken:

- The auditor will document the identified discrepancy.
- The auditor will promptly inform both Telecert and the PMA of the discrepancy.

- Telecert and the PMA will collaborate to establish a corrective plan for addressing the non-compliance.
- Telecert will submit the proposed corrective plan to the PMA for approval.
- If deemed necessary, the PMA may require further actions to rectify significant issues arising from the non-compliance, which may include the revocation of affected Certificates.

8.6 Communication of Results

Within a 30-day period following the conclusion of the audit and the identification of necessary corrective actions, the PMA, along with any other entities entitled by law, regulation, or agreement, will be furnished with the details of the corrective measures.

Telecert publishes letters confirming compliance with annual external Audit Reports in the legal Repository, accessible at https://www.telecert.com/repository.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Telecert pricing is available on its website (https://www.telecert.com).

9.1.1 Certificate Issuance or Renewal Fees

Not applicable.

9.1.2 Certificate Access Fees

Not applicable.

9.1.3 Revocation Access Fees

Not applicable.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No Stipulation.

9.2.2 Other Assets

No Stipulation.

9.2.3 Insurance or Warranty Coverage

No Stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Confidential information encompasses at a minimum, but is not limited to, materials concerning business and marketing plans, intellectual property, financial records, research findings, operational methodologies, sensitive details like PINs/passwords/combinations and cryptographic keys, data obtained from third parties, restricted personal information, and data acquired from third parties.

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

Telecert, along with all employees, agents, and contractors, bears the responsibility of safeguarding confidential information. To achieve this, Telecert implements comprehensive training and enforcement programs for all personnel, ensuring the maintenance and protection of confidential information.

9.4 Privacy of Personal Information

The Telecert Privacy Policy is available for review at https://www.telecert.com/privacy-policy

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information Treated as Private

No stipulation.

9.4.3 Responsibility to Protect Private Information

No stipulation.

9.4.4 Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.5 Intellectual Property Rights

Telecert and/or its business partners own the intellectual property rights in Telecert's services, including the certificates, trademarks used in providing the services, and this CPS. Certificate information is the property of Telecert. Telecert grants permission to reproduce and distribute its certificates on a non-exclusive and royalty-free basis, provided that the certificates are reproduced and distributed in full. End entity Private Keys and Public Keys remain the property of the Subscribers who rightfully hold them.

Notwithstanding the foregoing, any third party software (including open source software) used by Telecert to provide its services is licensed, not owned, by Telecert.

9.6 Representations and Warranties

9.6.1 STI-CA Representations and Warranties

Telecert extends the following certificate warranties to Certificate Beneficiaries upon issuance:

1. The Subscriber party to the Subscriber Agreement or Terms of Use for the Certificate.
2. Application Software Suppliers with whom the Root CA has a contract for Root Certificate inclusion in their distributed software.
3. All Relying Parties who reasonably rely on a Valid Certificate.

Telecert assures Certificate Beneficiaries of compliance with its CPS throughout the Certificate's validity period.

Responsibility for the performance, warranties, liabilities, and indemnification obligations of Subordinate CAs under this CPS lies with Telecert.

9.6.2 Relying Party Representations and Warranties

Each Relying Party represents and warrants that, prior to relying on an Telecert certificate, it:

1. Obtained sufficient knowledge on the use of digital certificates and PKI,
2. Studied the applicable limitations on the usage of certificates and agrees to Telecert's limitations on its liability related to the use of certificates,
3. Has read, understands, and agrees to this CPS,
4. Verified both the Telecert certificate and the certificates in the certificate chain,
5. Will not use Telecert certificates if the certificate has expired or been revoked, and will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on Telecert certificates after considering:
    - Applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
    - The intended use of the certificate as listed in the certificate or this CPS,

- The data listed in the certificate,
- The economic value of the transaction or communication,
- The potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
- The Relying Party's previous course of dealing with the Subscriber,
- The Relying Party's understanding of trade, including experience with computer-based methods of trade, and
- Any other indicator of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a certificate is at a party's own risk.

9.6.3 Subscriber Representations and Warranties

1. Each Subscriber warrants to Telecert and the public-at-large that Subscriber is the legitimate registrant of the organization that is, or will be, the subject of the Telecert certificate issued to Subscriber.
2. Each Subscriber warrants that all information in the Telecert certificate issued to Subscriber regarding Subscriber is accurate, current, reliable, complete, and not misleading.
3. Each Subscriber warrants that all information provided by Subscriber to Telecert is accurate, current, complete, reliable, complete, and not misleading.
4. Each Subscriber warrants that Subscriber rightfully holds the Private Key corresponding to the Public Key listed in the Telecert certificate issued to Subscriber.
5. Each Subscriber warrants that Subscriber has taken all appropriate, reasonable, and necessary steps to secure and keep Subscriber's Private Key secret.
6. Each Subscriber acknowledges and accepts that Telecert is entitled to revoke Subscriber's Telecert certificates immediately if the Subscriber violates the terms of the Subscriber Agreement or if Telecert discovers that any of Subscriber's Telecert certificates are being used to enable criminal activities such as phishing attacks, or fraud.

9.7 Disclaimers of Warranties

Unless explicitly stated in Section 9.6.1 all Certificates, related software, and services are provided on an "as is" and "as available" basis.

Telecert disclaims all express and implied warranties not specified in the CP, including but not limited to warranties of merchantability, fitness for a particular purpose, and non-infringement, to the maximum extent permitted by law.

9.8 Limitations of Liability

Telecert and any Delegated Third Party may allocate liability through contractual agreements for delegated tasks. However, Telecert remains fully responsible for all parties' performance according to this CPS, as if no delegation occurred.

If Telecert has issued and managed the Certificate in accordance with this CPS, liability disclaimers may apply to the Certificate Beneficiaries and other third parties for losses resulting from the use or reliance on the Certificate beyond the scope specified in Telecert's CPS. In case Telecert has not issued or managed the Certificate in compliance with its CPS, Telecert may seek to limit its liability to the Subscriber and Relying Parties through appropriate means for any claims, losses, or damages resulting from the use or reliance on such Certificate, regardless of the cause of action or legal theory involved. Should Telecert choose to limit its liability for non-compliant Certificates, the limitations will be included in Telecert's CPS.

9.9 Indemnities

9.9.1 Indemnification by an Issuing STI-CA

The Telecert CA does not provide any indemnification except as described in Section 9.9.1 of the Certificate Policy.

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall provide indemnification to Telecert, its partners, cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, arising from:

1. Any misrepresentation or omission of material fact by the Subscriber, regardless of intent.
2. The Subscriber's violation of the Subscriber Agreement, this CPS, or applicable laws.
3. The compromise or unauthorized use of a certificate or Private Key due to the Subscriber's negligence or intentional acts.
4. The Subscriber's misuse of the certificate or Private Key.

9.9.3 Indemnification by Relying Parties

To the extent allowed by law, each Relying Party shall indemnify Telecert, its partners, cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, resulting from the Relying Party's:

1. Breach of the Relying Party Agreement, an End-User License Agreement, this CPS, or applicable laws.

2. Unreasonable reliance on a certificate.
3. Failure to verify the certificate's status before use.

9.10 Term and Termination

9.10.1 Term

This version of the Telecert CPS is effective until otherwise communicated through the Telecert repository. (https://www.telecert.com/repository)

9.10.2 Termination

This CPS and any subsequent modifications will remain valid until they are superseded by a more recent version.

9.10.3 Effect of Termination and Survival

Telecert will publicly announce any CA termination through its public repository and notify the Application Software Suppliers with whom it has a Root Certificate distribution agreement.

9.11 Individual Notices and Communications with Participants

Telecert acknowledges receipt of notices pertinent to this CPS at the designated locations outlined in Section 1.6.2 of this CPS. Notices are regarded as effective upon receipt of a valid and digitally signed acknowledgment from Telecert. In cases where no acknowledgment is received within a five-day period, the sender is required to reissue the notice in physical form, sending it to the address specified in Section 1.6.2 via a courier service with delivery confirmation or through certified/registered mail with prepaid postage and requested return receipt.

Alternate methods of notice may be accepted as defined in Subscriber Agreements established by Telecert.

Furthermore, Telecert commits to informing the PMA at least one month prior to implementing any planned changes or updates that could impact the Telecert PKI operational landscape or compliance with the CP. These changes include, but are not limited to:

1. Introducing or modifying Root CAs.
2. Implementing additional CPs at the Root CA level.
3. Altering Certificate issuance procedures.
4. Concluding operations or transitioning ownership of Root CAs.

9.12 Amendments

9.12.1 Procedure for Amendment

Telecert's Policy Management Authority (PMA) holds the authority to enact necessary amendments to this CPS.

Any significant changes made to the Telecert CPS will be duly noted in a version control table integrated into this document.

Minor changes, such as grammatical, syntactical, or spelling corrections, may, at Telecert's discretion, be implemented without prior notice by adding a sub-minor number to the document OID.

Annually, if no other modifications are made, the document's version number will be incremented, and a dated changelog entry will be added to indicate the update.

9.12.2 Notification Mechanism and Period

Telecert posts CPS revisions to its Repository. Telecert does not guarantee a comment period and may make changes to this CPS without notice

9.12.3 Circumstances Under which OID Must be Changed

Telecert retains the right to amend the content of any published CPS. Major changes to the Telecert CPS will also result in the alteration of the OID published through the Telecert repository.

9.13 Dispute Resolution Procedures

Parties are required to notify Telecert and attempt to resolve disputes directly with Telecert before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14 Governing Law

The laws of the State of Texas govern the interpretation, construction, and enforcement of this CP/CPS and all proceedings related to Telecert's products and services, including tort claims, without regard to any conflicts of law principles. The State of Texas has non-exclusive venue and jurisdiction over any proceedings related to this CPS or any Telecert product or service.

9.15 Compliance with Applicable Law

This CPS adheres to all relevant laws and regulations, including United States restrictions on the export of software and cryptography products.

9.16 Miscellaneous Provisions

No stipulation.

9.16.1 Entire Agreement

Telecert requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

Entities operating under this CPS are prohibited from assigning their rights or obligations without obtaining prior written consent from Telecert. Unless explicitly specified in a contract with a party, Telecert does not offer notice of assignment.

9.16.3 Severability

In the event that a competent court or tribunal deems any provision of this CPS as invalid or unenforceable, the remaining portions of the CPS will continue to be both valid and enforceable. Every provision within this CPS that involves liability limitation, warranty disclaimer, or damage exclusion is distinct and can stand independently from any other provision.

9.16.4 Force Majeure

Telecert is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond Telecert's reasonable control. The operation of the Internet is beyond Telecert's reasonable control.

9.17 Other Provisions

No stipulation.

Certificate of Signature and Timestamp

DOCUMENT DETAILS:

Document ID:	91a5d318-1210-443b-b6a8-68ae2a7b8013
SHA1 Hash:	4cd5ff01dff038dac0db6e30568292707b89a7b2
Filename:	Telecert CPS 1.4
Created at:	April 07, 2024 00:32:25 UTC
Esealed at:	April 07, 2024 00:32:39 UTC
Owner Name:	SSL.com Compliance Team
Owner Email:	compliance@ssl.com

CERTIFICATE DETAILS:

Subject DN:	CN=eSigner LLC, OU=eSigner.com e-seal, O=eSigner LLC, L=Houston, ST=Texas, C=US
Serial Number	657077143298596049653533296355610460 04
Issuer DN:	CN=SSL.com Client Certificate Intermediate CA RSA R2, O=SSL Corp, L=Houston, ST=Texas, C=US

Signed with **eSigner.com**