martini security

Martini Security SHAKEN Certificate Practices Statement

Version 1.7 • 2 October 2022

Table of Contents

1 Martini Security SHAKEN Certification Practice Statement

1.1 Introduction

Martini Security, LLC ("Martini") has established the Martini Security SHAKEN Public Key Infrastructure ("Martini Security SHAKEN PKI"). This CPS outlines the principles and practices related to the "Martini Security SHAKEN PKI certificate issuance services and describes the practices used to comply with the STI-PA SHAKEN Certificate Policy and other applicable policies.

This practice statement is designed to be read in conjunction with the STI-PA Shaken Certificate Policy. All defined terms and acronyms in the CP have the same definitions in this document unless redefined in §1.6 of this document.

The Martini Security SHAKEN PKI conforms to the current version of the guidelines adopted by the STI-PA when issuing SHAKEN certificates. If any inconsistency exists between this CPS and the STI-PA Certificate Policy and operational requirements the associated requirement or guideline document shall take precedence.

This CPS is only one of several documents that control Martini Security SHAKEN PKI certification services. Other important documents include both private and public documents, such as the agreements with its customers, Martini Security's privacy policy and its terms of use. Martini Security may provide additional certificate policies or certification practice statements for other use cases. These supplemental policies and statements are available to applicable users or relying parties.

Document	**Status**	**Location**
Certification Policy (Governing document)	Public	Shaken Policy Management Authority Repository
Certification Practice Statement (This document)	Public	Martini Security Repository
Subscriber Agreement	Public	Martini Security Repository
Terms of Use	Public	Martini Security Website
Privacy Policy	Public	Martini Security Website
CA Procedure Documents Confidential	Presented to auditors accordingly	

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

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CPS is divided into nine primary components that cover the security controls and practices and procedures for certificate issuance services within the Martini Security PKI. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement "Not applicable" or "No stipulation."

1.2 Overview

Martini Security SHAKEN PKI only issues certificates via 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]. The only entities that provide a valid STI-PA issued SPC token, as defined in [ATIS-1000080] and [ATIS-1000092], are able to acquire a certificate.

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; State: WA; Locality: Seattle; Organization: Martini Security, LLC; Common Name: Martini Security SHAKEN R1	Algorithm: EC Public Key (1.2.840.10045.2.1) Named Curve: Prime256v1 (1.2.840.10045.3.1.7)	6077e368b0a0e4b6 076eaa07ce67d665 2ef310c4757776b7 6af84a6a9e003cdf	3 May 2022 15:31:00 GMT To 3 May 2047 21:31:00 GMT
Subordinate CA	C: US; State: WA; Locality: Seattle; Organization: Martini Security, LLC; Common Name: Martini Security SHAKEN G2	Algorithm: EC Public Key (1.2.840.10045.2.1) Named Curve: Prime256v1 (1.2.840.10045.3.1.7)	bf818ddbd3ae492e 4a85331b85b52f4d 2cdef8287bf910b5 9e247b6c132fa7fd	2 Oct 2022 10:40:00 GMT To 1 Oct 2047 10:40:00 GMT

The OID for this CPS is 1.3.6.1.4.1.57973.1.7 {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) Martini Security(57973) Documentation(1) This Document(7)}. Subsequent revisions to this CPS may have new OID assignments.

Certificate profiles described in Section 7.1 and each certificate issued under this CPS includes OID for the CP [2.16.840.1.114569.1.1.3] in certificatePolicies extension.

1.3 Document Name and Identification

This document is the Martini Security SHAKEN Certificate Practices Statement and was approved for publication by the Martini Security Policy Authority. The following revisions were made to the original document:

Date	Changes	Version
09/30/2021	Initial Draft	.1
10/11/2021	Add certificates info	1
05/03/2022	Address Shaken PMA feedback	1.1
05/26/2022	Address Shaken PMA feedback	1.2
07/19/2022	Address Shaken PMA feedback	1.3
08/24/2022	Address Shaken PMA feedback	1.4
08/29/2022	Address Shaken PMA feedback	1.5
09/01/2022	Address Shaken PMA feedback	1.6
10/02/2022	Fix typos, remove G1 issuer, add G2 issuer, update certificate repository URL schema	1.7

1.4 PKI Participants

1.4.1 Certification Authorities

This CPS applies to Martini Security SHAKEN PKI.

1.4.2 Registration Authorities

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

1.4.3 Subscribers

See definition of “Subscriber” in Section 1.8.1 Definitions.

1.4.4 Relying Parties

See definition of “Relying Party” in Section 1.8.1 Definitions.

1.4.5 Other Participants

Martini Security SHAKEN PKI vendors and service providers with access to confidential information or privileged systems are required to operate in compliance with the Martini Security SHAKEN PKI CPS.

1.5 Certificate Usage

1.5.1 Appropriate Certificate Usage

Subscriber usage of Private Keys and Certificates is governed by the Martini Security’s Subscriber Agreement and CPS.

Specifically the above agreements limits relying parties to use end-entity Certificate to authenticating caller metadata via signing SHAKEN PASSporTs, as described in ATIS-1000074, and any other PASSporT extensions defined for use in the SHAKEN ecosystem. Then, the SHAKEN PASSporTs are used by a Relying Party to determine the authenticity of the calling party in the SP’s VoIP network, as described in ATIS-1000074.

1.5.2 Prohibited Certificate Uses

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

1.6 Policy Administration

1.6.1 Organization Administering the Document

This CPS document is maintained by the Martini Security PMA.

1.6.2 Contact Person

Martini Security, LLC Attention: PKI Policy Management Authority 100 S KING ST STE 100-1006 Seattle, WA 98104-2885 USA

206-445-STIR(7847) Toll-Free 855-445-STIR(7847)

Web: www.martinisecurity.com

Email for policy questions: shaken-pma[@]martinisecurity.com

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

1.6.3 Entity Determining CPS Suitability for the Policy

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

1.6.4 CPS Approval Procedures

Martini Security regularly monitors for changes to the SHAKEN Certificate Policy. Upon formal notice of the publication of a new SHAKEN CP, Martini Security will submit a revised CPS to the PMA within 45 days. Upon approval of the revised CPS, all certificates issued by the Martini PKI will conform to the requirements in that CPS within 90 days.

For all other changes Martini Security PMA has a formal review process and only updates the CPS upon approval by the Martini Security PMA.

1.7 References

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

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

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

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

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

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

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

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

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

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

1.8 Definitions and Acronyms

1.8.1 Definitions

[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 >.

Term	Definition
ACME Protocol	A protocol used for validation, issuance, and management of certificates. The protocol is an open standard managed by the IETF.
Applicant	An entity applying for a certificate.
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Repository	A repository of information about Martini Security certificates.
Company Code	A unique four-character alphanumeric code (NXXX) assigned to all SPs [ATIS-0300251].
Delegate Certificate	A certificate whose parent certificate contains a TNAuthList extension, as defined in [draft-ietf-cert-delegation] and [ATIS-1000092].
Key Pair	A Private Key and its associated Public Key.
PASSporT	A token object that conveys cryptographically-signed information about the participants involved in communications. The extension is defined, corresponding to the SHAKEN specification, to provide both a
Policy and Legal Repository	A repository of policy and legal documents related to the Martini Security PKI. It is located at: https://martinisecurity.com/repository
Policy Management Authority	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	The key in a Key Pair that must be kept secret. Used to create digital signatures that can be verified by the corresponding Public Key or to decrypt messages encrypted by the corresponding Public Key.
Public Key	The only key in a Key Pair that can safely be publicly disclosed. Used by Relying Parties to verify digital signatures from the corresponding private key or to encrypt messages that can only be decrypted by the corresponding private key.
Relying Party	An entity that relies upon information contained within certificates issued by the Martini Security SHAKEN PKI.
Root CA	A top-level Certification Authority whose Root Certificate is distributed by the STI-PA and that issues Subordinate CA Certificates.
Martini Security certificates	A certificate issued by Martini Security
Service Provider	A telecommunications service provider serving customers with phone numbers from the NANPA.
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].

Term	Definition
Service Provider Code 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).
Secure Telephone Identity Certificate	A certificate containing a TNAuthList extension as defined in [RFC 8226] and [ATIS-1000080]. The TNAuthList contains a single SPC value that identifies the SHAKEN SP holding the certificate.
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].
Trusted Contributor	A contributor who performs in a Trusted Role. Trusted Contributors may be employees, or contractors. Trusted Contributors must be properly trained and qualified, and have the proper legal obligations in place before performing in a Trusted Role.
Trusted Role	A role which qualifies a person to access or modify Martini Security SHAKEN PKI systems, infrastructure, and confidential information.

See STI-PA CP 1.3 for additional definitions.

1.8.2 Acronyms

Acronym	Definition
ATIS	ATIS Alliance for Telecommunications Industry Solutions
ACME	Automated Certificate Management Environment
CA	Certificate Authority
CP	Certificate Policy
CPA	Certification Practice Statement
OCN	Operating Company Number
HSM	Hardware Security Module
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
SHAKEN	Signature-based Handling of Asserted information using toKENs
SP	Service Provider
SPC	Service Provider Code
STI	Secure Telephone Identity
STI-CA	Secure Telephone Identity Certification Authority
STI-CR	Secure Telephone Identity Certificate Repository

Acronym	Definition
STI-PA	Secure Telephone Identity Policy Administrator
STI-GA	Secure Telephone Identity Governance Authority

See https://www.atis.org/glossary for a list of common communications terms and definitions.

2 Publication and Repository Responsibilities

2.1 Public Repositories

Martini Security CPS, Privacy Policy, and Subscriber Agreement are made publicly available in the Repository, which can be found at:

https://martinisecurity.com/repository

2.2 Publication of Certification Information

Records of all Martini Security Root and Subordinate CA certificates are available in the Certificate Repository:

https://martinisecurity.com/repository

All end-entity certificates issued by Martini Security are published, on behalf of the subscribers, to a certificate repository. The URL (https://p.mtsec.me/{CAID}/{CERTID}.pem) is returned to the applicant at issuance time.

The subscriber obligations are for publication of certificate information governed by the Martini Security's Subscriber Agreement.

Specifically the subscriber agreement obligates the subscriber to:

Immediately request your certificate be revoked by the STI-PA either directly, or request Martini Security, via ACME client software, to do on your behalf if: (i) there is any actual or suspected misuse or Key Compromise of the Private Key associated with the Public Key included in Your Certificate, or (ii) any information in Your Certificate is, or becomes, misleading, incorrect or inaccurate.

2.3 Time or Frequency of Publication

New or updated Martini Security CPS, Terms of Service, Privacy Policy, and Subscriber Agreement are made publicly available as soon as possible. This typically means within seven days of receipt or approval. The Martini Security PMA will submit CPS documents at least annually to the PMA for approval. Once approved they will be published.

New or updated Martini Security Root and Subordinate CA certificates are made publicly available as soon as possible. This typically means within seven days of creation. New Root CA certificates are provided to the STI-PA within 7 days of creation.

All certificates are published to the certificate repository (STI-CR) at the time of issuance.

2.4 Access Controls on Repositories

Read only access to the Policy and Legal Repository and certificate repository (CTI-CR) is unrestricted. Write access is protected by logical and physical controls.

3 Identification and Authentication

Martini Security CA supports the Automated Certificate Management Environment (ACME) [RFC 8555] protocol, as well as the ACME extension for token authorization using the SPC as described in [ATIS-1000080], [ATIS-1000092] and [draft-ietf-acme-authority-token-tnauthlist]. The fingerprint in the SPC token is based on the public key associated with the SP's account ACME credentials.

3.1 Naming

3.1.1 Types of Names

The certificate profiles defined in Section 7.1 include distinguished names and subject alternative names that are compliant with both ATIS 1000080 and the CP.

Specifically the requirements listed in those documents include ensuring:

- The subject is unique for each certificate
- The subject DN contains a Country RDN
- The subject DN contains Common Name RDN
- The subject DN Common Name includes the text string "SHAKEN", followed by a single space, followed by the SPC value identified in the TNAuthList of the End-Entity certificate (e.g., "CN=SHAKEN 1234")
- The subject DN Serial Number RDN contains a unique string
- The subject DN Common Name RDN indicates if a certificate is a root or intermediate certificate
- The subject DN contains an Organization RDN including the legal name of the service provider

3.1.2 Need for Names to be Meaningful

Martini Security certificates include "Subject" and "TNAuthList" fields which identify the subject entity. The subject entity is identified using an Organization name, its OCN and a list of Service Provider Codes (SPCs).

Martini Security certificates include an "Issuer" field which identifies the issuing entity. The issuing entity is identified using a distinguished name.

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

Subject names are unique per certificate. Each subject name includes the subject country, the Entity Name found in their FCC registration and the SPC value identified from the SPC token, and a unique string.

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

The STI-CR URL is unique per certificate. This is accomplished by using the first two-bytes of the issuer certificate serial as the first URL fragment and the base64 encoding of first nine-bytes of certificate serial number as the second URL fragment. For example:

https://p.mtsec.me/{CAID}/{CERTID}

3.1.6 Recognition, Authentication, and Role of Trademarks

Not applicable.

3.2 Initial Identity Validation

Applicants must provide a valid SPC token issued by the STI-PA bound to their ACME account key.

3.2.1 Method to Prove Possession of Private Key

Each ACME exchange for the purposes of requesting certificate issuance includes a CSR which contains a public key and a signature made with the corresponding private key. Prior to certificate issuance the public key is used to verify the signature on the CSR.

Each ACME request is authenticated by means of an ACME "account key pair." The applicant uses the private key in this key pair to sign all messages. The public key associated with this account key pair is used to verify each message prior to relying on the message.

3.2.2 Authentication of Organization Identity

Applicants provide the FCC Form 499 Filer ID number of the organization they would like a certificate for and using this information the FCC Form 499 Filer Database is used determine:

- If FCC registration is current
- The Legal Name of Reporting Entity
- The Headquarters Address of Reporting Entity
- The CORESID of the Reporting Entity

Using the CORESID the FCC Registration Database is used to determine the email address of the registered organization contact.

The applicant is then provided with a cryptographically generated short-lived, one-time use code that they must provide to the registered organization contact out of band.

An email is then sent to the registered organization contact notifying them that the applicant has requested the ability to acquire certificates on behalf of their organization. This mail includes a link where they can provide the code provided to the applicant

The verification is put into a pending state to provide the applicant an opportunity to provide the code to the registered organization contact. If the registered organization contact provides this code to the URL provided in the notification mail before the code expires the applicant is approved to submit requests for certificates on behalf of the organization.

If the applicant is authenticated using the email of the registered organization contact the verification of the code is not required.

Martini Security SHAKEN PKI only issues certificates via 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]. As a result all orders include a SPC Token which is validated prior to certificate issuance.

The country relative distinguished name included in the Subject is validated based on the Headquarters Address in the FCC Form 499 Filer Database and is limited to the US.

The following sources of information are used when issuing certificates:

- FCC Form 499 Filer Database
- FCC Registration Database
- SPC Token

Each source being the most authoritative sources available for each of the elements relied upon.

3.2.3 Authentication of Individual Identity

Applicants authenticate using Google Sign-In and then both the FCC Form 499 Filer Database and FCC Registration Database are used to verify the applicants affiliation with the organization.

If the Applicants email address matches the email in the FCC Registration Database an the MX records associated with the email address are checked to ensure that they point at ASPMX.L.GOOGLE.COM or a subdomain.

3.2.4 Non-verified Subscriber Information

Not applicable. No unverified information is included in certificates.

3.2.5 Validation of Authority

Applicants authenticate using Google Sign-In and then both the FCC Form 499 Filer Database and FCC Registration Database are used to verify the applicants affiliation with the organization.

3.2.6 Criteria for Interoperation

Not applicable.

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 Request

Identification and authentication for revocation requests is performed by Martini Security in compliance with Section 4.9 of this document.

Identification and authentication are not required when revocation is being requested by Martini Security.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Any applicant that is approved by the registered organization contact, and has a valid SPC token may submit an application for a certificate via the ACME protocol. Issuance will depend on proper validation and compliance with Martini Security policies.

4.1.2 Enrollment Process and Responsibilities

The enrollment process involves the following steps, in no particular order:

- Generating a key pair using secure methods
- Submitting a request for a certificate containing all necessary information, including the public key, and SPC Token.
- Agreeing to the relevant Subscriber Agreement

The applicant procedures outlined in ATIS-1000080 and ATIS-1000092 are followed in order to create an ACME account.

There are two roles associated with the application for a certificate. - The individual requesting the certificate (the applicant) - The registered organization contact (the organization contact).

The same entity may perform both roles.

4.2 Certificate Application Processing

Martini Security 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

Approval requires successful completion of validation per Section 3.2.2 as well as compliance with all CA policies.

4.2.2 Approval or Rejection of Certificate Applications

Certificate requests that do not meet the issuance requirements will be rejected and a reason for the rejection is provided.

4.2.3 Time to Process Certificate Applications

Once an account is authorized certificate requests are typically processed within a few seconds but will take no longer 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] and [RFC 8555] are followed.

- For issuing intermediate STI certificates the procedures in [ATIS-1000092] are followed.

For CP revisions that place new requirements on end-entity certificates, Martini Security CA shall comply with the new requirements for all newly assigned certificates within 90 days of the approval of 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 CA Actions During Certificate Issuance

At a high level, the following steps are taken during issuance of a Subscriber Certificate. Martini Security's automated processes confirm that the applicant is authorized, that all information that will appear in the certificate is correct, and that the applicant has a valid SPC token.

This validation is done according to the procedures in ATIS-1000080 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 wellknown URL and made available to the Subscriber.

4.3.2 Notification to Subscriber by the 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

See Section 2.2.

4.4.2 Publication of the Certificate by the CA

See Section 2.2 of this document for Root and Subordinate CA certificate publication information.

All Subscriber Certificates are made available to Subscribers via the ACME protocol.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.2.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscriber usage of Private Keys and Certificates is governed by the Martini Security's Subscriber Agreement.

Specifically the subscriber agreement requires subscribers to:

- hold the Private Key corresponding to the Public Key listed in their Certificate
- warrant to to public-at-large that they will take, all appropriate, reasonable, and necessary steps to maintain control of, secure, properly protect and keep secret and confidential the Private Key corresponding to the Public Key in their certificate (and any associated activation data or device, e.g. password or token).

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] and [ATIS-1000092], 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 verifier 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 certificate currently in use. It is recommended that the Subscriber request issuance of the new certification at 24 hours prior to expiration.

4.6.2 Who May Request Renewal

Not applicable. Renewals are not supported.

4.6.3 Processing Certificate Renewal Requests

Not applicable. Renewals are not supported.

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable. Renewals are not supported.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable. Renewals are not supported.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not supported.

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 CA

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

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.8 Certificate Modification

Certificate modification requests are not supported.

4.8.1 Circumstance for Certificate Modification

Not applicable. Certificate modification requests are not supported.

4.8.2 Who May Request Certificate Modification

Not applicable. Certificate modification requests are not supported.

4.8.3 Processing Certificate Modification Requests

Not applicable. Certificate modification requests are not supported.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable. Certificate modification requests are not supported.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable. Certificate modification requests are not supported.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable. Certificate modification requests are not supported.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable. Certificate modification requests are not supported.

4.9 Certificate Revocation and Suspension

The model for managing and communicating the status of revoked certificates is in the form of a indirect Certificate Revocation List (CRL) that is maintained by the STI-PA as described in ATIS-1000080. As such all revocations performed by or through Martini Security are proxied to the STI-PA via the APIs they provide.

Certificate suspension is not supported.

4.9.1 Circumstances for Revocation

An end entity certificate shall be revoked by the STI-GA for any reason. For example if there is reason to be believed there has been a compromise of a Subscriber's private key. Other example reasons for the STI-GA to perform certificate revocation include:

- Affiliation Changed, where, due to an organizational name change, the certificate's Subject Name field no longer identifies the certificate holder.
- Superseded, where the certificate has been replaced with a new certificate.
- Cessation of operation, where the Subscriber holding the certificate is ceasing operation.
- Privilege Withdrawn, where the Subscriber holding the certificate is no longer authorized to obtain STI certificates.

In the event that Martini Security should receive a valid revocation request via the ACME protocol, Martini Security will present the requested revocation to the STI-GA for processing.

If Martini Security ceases operation or loses its authority to issue STI certificates the STI-GA will no longer be listed on the Trusted STI-CA List and our certificates will no longer be trusted.

A subordinate CA certificate shall be revoked by the STI-GA for any reason. For example if there is reason to be believe there has been a compromise of a CA's private key. Other example reasons for the STI-GA to perform certificate revocation include:

- Cessation of operation, where the CA in question is ceasing operation.
- Privilege Withdrawn, where the CA in question is no longer authorized to obtain issued certificates.

4.9.2 Who Can Request Revocation

A Subscriber can request revocation of a certificate via the STI-PA for a certificate which it has authority. 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 Martini Security assists in requesting revocation of any certificate via the ACME API if 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 Martini Security 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. No other information is required in such cases.

Certificates may be administratively revoked by Martini Security or the STI-GA via revocation request to STI-PA if it is determined that the Subscriber has failed to meet obligations under the CP, this CPS, the relevant Subscriber Agreement, or any other applicable agreement, regulation, or law. Certificates may also be administratively revoked at the discretion of Martini Security management via revocation request to STI-PA.

4.9.3 Procedure for Revocation Request

A Subscriber can request revocation of a certificate via the STI-PA for a certificate which it has authority. 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 Martini Security assists in requesting revocation of any certificate via the ACME API if 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 Martini Security 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. No other information is required in such cases.

4.9.4 Revocation Request Grace Period

There is no grace period for a revocation request. A revocation request must be made as soon as circumstances requiring revocation are confirmed.

4.9.5 Time within which the Revocation Request must be Processed

Revocation requests will be processed within 24 hours of receiving the request.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties should verify the validity of certificates via the distributed Certificate Revocation List (CRL) that is maintained by the STI-PA. Relying Parties who cannot or choose not to check certificate expiration or revocation status, but decide to rely on a certificate anyway, do so at their own risk.

See Section 4.5.2.

4.9.7 CRL Issuance Frequency (If Applicable)

Not Applicable. Martini Security does not provide revocation status checking capability.

4.9.8 Maximum Latency for CRLs (If Applicable)

Not Applicable. Martini Security does not provide revocation status checking capability.

4.9.9 Online Revocation/Status Checking Availability

Not Applicable. Martini Security does not provide revocation status checking capability.

Instead an indirect CRL maintained by the is used by the SHAKEN PKI for revocation status checking. All certificates issued by the STI-PA included a 'cRLDistributionPointName' field which points to the URL where the CRL for that certificate's status can be checked. The processing of this indirect CRL is specified by ATIS-1000080.

4.9.10 Online Revocation Checking Requirements

Not Applicable. Martini Security does not offer revocation status checking capability.

4.9.11 Other Forms of Revocation Advertisements Available

Not Applicable. Martini Security does not offer revocation status checking capability.

4.9.12 Special Requirements Re-key Compromise

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

4.9.13 Circumstances for Suspension

Not Applicable. Certificate suspension is not supported.

4.9.14 Who Can Request Suspension

Not Applicable. Certificate suspension is not supported.

4.9.15 Procedure for Suspension Request

Not Applicable. Certificate suspension is not supported.

4.9.16 Limits on Suspension Period

Not Applicable. Certificate suspension is not supported.

4.10 Certificate Status Services

Not Applicable. Martini Security does not operate revocation services.

The SHAKEN PKI defines an indirect CRL model, as defined in [RFC 5280] in which the Subscribers and STI-CAs provide any revoked end entity and intermediate certificates to the STI-PA for inclusion in the CRL. The processing of this indirect CRL is specified by ATIS-1000080. The URL to the CRL is provided to the Subscriber when they request a SPC token from the STI-PA. Intermediate and end-entity certificates will all include the URL to the STI-PA CRL in the 'cRLDistributionPointName' field.

4.10.1 Operational Characteristics

Not Applicable. Martini Security does not operate revocation services.

4.10.2 Service Availability

Not Applicable. Martini Security does not operate revocation services.

4.10.3 Optional Features

Not Applicable. Martini Security does not operate revocation services.

4.11 End of Subscription

A Subscriber's subscription ends once all of Subscriber's Martini Security certificates have expired or been revoked.

Prior to expiration of a Subscriber's certificate, Martini Security may send Subscriber a notice regarding upcoming Certificate expiration if a contact email address was provided.

4.12 Key Escrow and Recovery

Not applicable. Key escrow and recovery is not supported.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable. Key escrow and recovery is not supported.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable. Session key encapsulation and recovery is not supported.

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

5.1.1 Site Location and Construction

Martini Security PKI Facilities are located in the United States, as are all copies of Martini Security CA Private Keys.

Martini Security maintains at least two PKI Facilities at all times for the sake of redundancy.

PKI Facilities are constructed so as to prevent unauthorized entry or interference.

PKI Facilities are monitored at all times (24x7) so as to prevent unauthorized entry or interference.

5.1.2 Physical Access

Physical access to Martini Security PKI Facilities is restricted to authorized employees, vendors, and contractors, for whom access is required in order to execute their jobs. Access restrictions are strongly enforced via multi-factor authentication mechanisms.

5.1.3 Power and Air Conditioning

Redundant power sources are readily available at each PKI Facility, and are designed to meet Martini Security's operating requirements.

Air conditioning systems at each PKI Facility are designed to meet Martini Security's operating requirements.

5.1.4 Water Exposures

Martini Security PKI Facilities are designed to protect Martini Security infrastructure from water exposure/damage.

5.1.5 Fire Prevention and Protection

Martini Security PKI Facilities are designed to prevent fire and provide suppression if necessary.

5.1.6 Media Storage

Martini Security PKI Facilities are designed to prevent accidental damage or unauthorized access to media.

No clear text private keys are stored on media, when ciphertext of keys are stored on media the HSM mechanisms are used to protect the corresponding Key Encryption Key (KEK).

5.1.7 Waste Disposal

Martini Security prohibits any media that contains or has contained sensitive data from leaving organizational control in such a state that it may still be operational, or contain recoverable data. Such media may include printed documents or digital storage devices. When media that has contained sensitive information reaches its end of life, the media is physically destroyed such that recovery is reasonably believed to be impossible.

All media sanitization methods utilized are compliant with the requirements specified in NIST SP 800-88.

5.1.8 Off-site Backup

Martini Security maintains multiple copies of Martini Security CA Private Keys at multiple PKI Facilities. All copies are stored on devices meeting FIPS 140 Level 3 criteria.

All operational systems are either idempotent, maintaining no data or replicated in real time to redundant systems in different facilities.

5.2 Procedural Controls

5.2.1 Trusted Roles

All persons, employees or otherwise, with the ability to materially impact the operation of Martini Security PKI systems and services, or the ability to view CA confidential information, must do so while designated as serving in a Trusted Role.

Trusted Roles include, but are not limited to:

Role	Responsibilities
Management	May view confidential information but may not directly impact CA operations. Strong decision-making authority.
Security Officers	May view confidential information but may not directly impact CA operations. Strong decision-making authority.
Systems Administrators	May view confidential information and directly impact CA operations. Decision-making authority is limited.
Engineering Liaisons	May view confidential information but may not directly impact CA operations. No decision-making authority.
Security Auditors	May view confidential information but may not directly impact CA operations. No decision-making authority.

These example roles map to the roles in the CPS as follows:

Role	Role defined in CPS
Management	CA Administrators
Security Officers	CA Administrators
Systems Administrators	CA Administrators
Engineering Liaisons	CA Operations Staff
Security Auditors	Security Auditors

Each of the above Trusted Roles requires an appropriate level of training and legal obligation.

Some trusted role operations include:

- The validation, authentication, and handling of information in Certificate Applications,
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, or enrollment information,
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository,
- Access to safe combinations and/or keys to security containers that contain materials supporting production services,
- Access to hardware security modules (HSMs), their associated keying material, and activation

data,
- Installation, configuration, and maintenance of the CA,
- Access to restricted portions of the certificate repository,
- The ability to grant physical and/or logical access to the CA equipment.

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

In some cases some staff may serve in multiple roles and in such cases audit records are maintained capturing which role they are performing as during a given task.

5.2.2 Number of Persons Required Per Task

A number of tasks require at least two people in Trusted Roles to be present, such tasks include but are not limited to:

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

5.2.3 Identification and Authentication for Each Role

Anyone performing work in a Trusted Role must identify and authenticate themselves before accessing Martini Security PKI systems or confidential information.

Staff authenticate themselves using a unique credential that is distinct from any credential they use to perform non- trusted role functions. This credential is managed in such a way that it is protected to the same level or greater than the system being accessed.

CA equipment and systems require strong authenticated access control for remote access using multi-factor authentication. CA equipment and systems require token based authenticated access control for local access.

Individuals holding trusted roles are appointed to the trusted role by the Policy Authority. These appointments shall be periodically reviewed for continued need, and renewed as appropriate. The approval by the policy authority is recorded in an append only log protected with strong access control.

Individuals holding trusted roles shall accept the responsibilities of the trusted role, and this acceptance is recorded in an append only log protected with strong access control.

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

5.2.4 Roles Requiring Separation of Duties

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

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Martini Security management is responsible for making sure that Trusted Contributors are trustworthy and competent, which includes having proper qualifications and experience.

Martini Security management ensures this with appropriate interviewing practices, training, background checks, and regular monitoring and review of Trusted Contributor job performance.

Individuals appointed to any trusted role at least meet the following minimum criteria:

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

5.3.2 Background Check Procedures

Trusted Contributors must undergo a background check prior to performing in a trusted role. Martini Security management will review the results of background checks for problematic issues prior to approving performance of a trusted role.

Background checks include, but are not limited to, criminal background and employment history.

5.3.3 Training Requirements

Trusted Contributors must be trained on topics relevant to the role in which they will perform.

Training programs are developed for each role by Martini Security management and Security Officers.

5.3.4 Retraining Frequency and Requirements

Training is repeated for each Trusted Contributor on an annual basis and covers topics necessary to maintain skill level requirements.

Training is also offered whenever changes in the industry or operations require it in order for contributors to competently perform in their trusted roles.

All contributors responsible for PKI Trusted Roles are made aware of changes in the CA operation prior to accessing related systems. Any significant change to the operations has a corresponding training program, and the execution of the training is documented. Examples of such changes are CA software or hardware upgrades, changes in CA operational procedures, changes in automated security systems, and relocation of equipment.

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

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Action will be taken to safeguard Martini Security and its subscribers whenever Martini Security Trusted Contributors, whether through negligence or malicious intent, fail to comply with Martini Security policies including this CPS.

Actions taken in response to non-compliance may include termination, removal from trusted roles, or reporting to legal authorities.

Once management becomes aware of non-compliance the Trusted Contributor(s) in question will be removed from trusted roles until a review of their actions is complete.

5.3.7 Independent Contractor Requirements

Independent contractors who are assigned to perform Trusted Roles are subject to the duties and requirements specified for such roles in this CPS and the accompanying CP. This includes those described in Section 5.3. Potential sanctions for unauthorized activities by independent contractors are described in Section 5.3.6.

5.3.8 Documentation Supplied to Personnel

Trusted Contributors are provided with all documentation necessary to perform their duties. This always includes, at a minimum, a copy of the Martini Security CP, CPS, and Information Security Policy.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit logs are generated for all events related to CA security and certificate issuance. Logs are automatically generated whenever possible. When it is necessary to manually log information, logs are kept on paper with written confirmation from a witness and securely stored. All audit logs, electronic or otherwise, shall be retained and made available to compliance auditors upon request.

At a minimum, each audit record includes:

- Date and time of entry,
- Identity of the person (or machine) making the entry,
- Responsible user or process,
- Description of the entry,
- Success or failure indicators.

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

As 100% of issuance is automated, 100% operational audit logs are used to automatically assess, via tooling, that verifies each step associated with a certificate issuance has been performed and logged.

Any identified exceptions trigger a manual review of logs and any significant findings are explained in the audit log summary tracked in an append only log protected with strong access control.

Actions taken as a result of these reviews are documented in an associated ticket tracking system.

All alerts generated by such systems shall be analyzed by CA operations staff on a daily basis.

5.4.3 Retention Period for Audit Log

Audit logs are retained for at least seven years and six months and will be made available to compliance auditors upon request.

5.4.4 Protection of Audit Log

Operational audit logs, whether in production or archived, are protected using both physical and logical access controls.

Read access to security audit data is limited to those in the Security Auditor role. Audit data automatically gets replication at the byte level from an underlying distributed file system that it's built on. The log is based on database mutations to files in a filesystem, and the filesystem takes care of replicating and recovering the files in the event of disk failures. This mechanism also provides a mechanism for detecting tampering.

Write access to the log is limited to those systems authorized to log and they are only permitted to append to the log.

When used, physical logbooks leverage tamper evident bags, and physical safes for protection. Less sensitive audit records are protected using an online append only log protected implemented with strong access controls. The append only nature ensures data can not be removed or added without being detected.

At the end of the retention period multiple trusted roles are required to destroy audit records of any type.

5.4.5 Audit Log Backup Procedures

Martini Security makes daily backup copies of audit logs to multiple facilities.

5.4.6 Audit Collection System (Internal vs. External)

Audit data is automatically generated and reported/recorded by operating systems, CA software applications, and network devices. Systems are in place to ensure proper reporting and recording of audit data, and the failure of such systems may lead to suspension of CA services until proper audit log reporting is restored.

Tooling is used to automatically validate appropriate records for each operation that were tracked. Any findings are automatically filed as a ticket for manual review.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Audit logs are monitored by Trusted Contributors, including operations and engineering staff. Anomalies indicating attempted breaches of CA security are reported and investigated.

Vulnerability assessments for Martini Security infrastructure are conducted at least annually.

Martini Security Security Officers perform a risk assessment at least annually. This risk assessment:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.5 Records Archival

5.5.1 Types of Records Archived

Martini Security archives all audit logs, the contents of which are described in Section 5.4.1. Martini Security may also archive any other information deemed critical to understanding the historical performance of the CA's duties.

Examples include:

- 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
- Auditor reports
- Any changes to the Audit parameters, e.g. audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- All changes to the trusted public keys, including additions and deletions
- Remedial action taken as a result of violations of physical security
- Violations of CP
- Violations of CPS

5.5.2 Retention Period for Archive

Martini Security retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years and six months after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

Archives are protected from unauthorized modification or destruction by strong security and environmental controls.

5.5.4 Archive Backup Procedures

Archives are backed up automatically each day.

5.5.5 Requirements for Time-Stamping of Records

Records are time-stamped as they are created.

Machine-created records use system time, which is synchronized automatically with third-party time sources. Machines without network access have the time set manually.

Manual records use a manually entered date and time, complete with time zone in use.

5.5.6 Archive Collection System (Internal or External)

All sensitive records systems are replicated in real time to redundant systems in different facilities or manually archived into an system that uses an append only log to make changes detectable.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to verify archived information in each system is available to operational staff and those in Trusted Roles such as Security Auditors. The method varies system to system, for example in the case of a record stored in a git repository, git log can be used to check the integrity of the repository.

5.6 Key Changeover

When a CA certificate is nearing expiration, a key changeover procedure is used to transition to a new CA certificate. The following steps constitute a key changeover procedure:

Sometime prior to CA certificate expiration, the private key associated with the expiring certificate is no longer used to sign new certificates.

A new key pair is generated and a new CA certificate is created containing the new key pair's public key and is published to the Martini Security Repository. This new key pair is used to sign new certificates.

No Subscriber certificates will be issued that extend beyond the expiration date of the CA certificate.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Martini Security has created and maintains incident response procedures for a range of potential compromise and disaster situations. Such situations include, but are not limited to, natural disasters, security incidents, and equipment failure. Incident response plans are reviewed, potentially updated, and tested on at least an annual basis.

Once such a security incident is confirmed certificate issuance is immediately stopped. Should a compromise be detected then an independent third-party investigation will be performed in order to determine the nature and the degree of damage. In such events the PMA will be notified within 24 hours.

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

In the event that computing resources, software, and/or data are corrupted or otherwise damaged, Martini Security will assess the situation, including its impact on CA integrity and security, and take appropriate action. This may include rebuilding associated systems from the ground up, restoring archived data or other similar action. CA operations may be suspended until mitigation is complete. Subscribers may be notified if corruption or damage has a material impact on the service provided to them. See Section 5.7.3.1 for Root CA Compromise Procedures.

5.7.3 Entity Private Key Compromise Procedures

5.7.3.1 Root CA Compromise Procedures

In the event that a Martini Security CA Private Key is compromised, or suspected to be compromised, Martini Security will immediately launch a thorough investigation. Forensic evidence will be collected and secured as quickly as possible. If it cannot be determined with a high degree of certainty that the private key in question was not compromised, then the following steps may be taken in whatever order is deemed most appropriate by Martini Security Security Officers:

- Notify the PMA within 24 hours of confirmation of the compromise and scope of incident,
- Request the PMA to remove trust in or revoke the private key in question,
- Martini Security will notify Subscribers relying on the integrity of the key in question.

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

Martini Security maintains multiple geographically diverse facilities, each of which is capable of operating Martini Security CA systems independently. In the event that a disaster entirely disables one facility, Martini Security CA operations will fail over to another facility.

Should failover be insufficient Martini Security maintains a Disaster Recovery plan that would enable it to rebuild its operations. Should such a failure occur the STI-PA and Subscribers would be notified within 24 hours of confirming the need to execute this plan.

Should Martini Security not be able to reconstitute services within 18 hours the STI-PA may decide to remove trust in Martini Security. At which point all Martini Security issued certificates would become untrusted.

If Martini Security cannot reconstitute services within eighteen (18) hours, then the inoperative status of the CA shall be reported to the PMA.

5.8 CA Termination

In the event that Martini Security CA services are to be terminated:

All affected parties, including STI-PA and Subscribers, will be provided with notice as far in advance as reasonably possible.

A termination plan will be created and reviewed by the Martini Security PMA and then be submitted to the PMA for approval.

If a suitable successor entity exists, the following steps will be taken:

- Martini Security CA Private Keys, records, logs, relevant confidential information, and other critical documentation will be transferred to the successor organization in a secure and compliant manner.
- Arrangements will be made for compliant continuation of CA responsibilities.

If a suitable successor entity does not exist, the following steps will be taken:

- All certificates issued will be revoked.
- Martini Security CA Private Keys will be destroyed.
- CA records, logs, relevant confidential information, and other critical documentation will be transferred to a third party or government entity with appropriate legal controls in place to protect information while allowing its use in compliance with relevant policies and the law.

5.9 CA Authority to Issue Certificates is Withdrawn

STI-PA may decide to remove trust in Martini Security at any time. Should this occur all Martini Security issued certificates would become untrusted.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Martini Security CA Private Keys are generated by HSMs meeting the requirements of Section 6.2.1. This occurs during a ceremony meeting the requirements of this CPS and the STI-PA CP.

The key generation ceremony utilizes Systems Administrators, Security Officers and Management trusted roles to ensure procedures are followed and audit records include a cryptographic attestation from the HSM demonstrating keys were generated in accordance to Section 6.2.1.

Martini Security never generates or has access to Subscriber Private Keys. Subscriber Public Keys are communicated to Martini Security electronically via the ACME protocol.

The subscriber agreement outlines the subscriber's obligations. This includes among other obligations that their keys are to be generated by them or their ACME Client Software running on their systems.

6.1.2 Private Key Delivery to Subscriber

Not applicable. Only subscriber generates the key pair.

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber Public Keys are communicated to Martini Security electronically via the ACME protocol.

6.1.4 CA Public Key Delivery to Relying Parties

Martini Security Public Keys provided to Relying Parties are available in the Repository.

6.1.5 Key Sizes

SHAKEN R1 Root CA ECDSA Private Keys are at least 256 bits in length.

SHAKEN G2 Subordinate CA ECDSA Private Keys are at least 256 bits in length.

STI certificates under this policy contain ECDSA public keys that are at least 256 bits in length.

When STI certificates are generated only the SHA256 hashing algorithm will be used in the associated signatures.

6.1.6 Public Key Parameters Generation and Quality Checking

Martini Security uses HSMs conforming to FIPS 186-4, capable of providing random number generation and on-board creation of at least 256-bit ECDSA keys.

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

See Section 7.1, Certificate Profiles.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Martini Security uses HSMs meeting FIPS 140-2 Level 3 (or higher) requirements.

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

Martini Security has put into place security mechanisms which require multiple people performing in Trusted Roles in order to access perform operations with CA Private Keys, both physically and logically. This is true for all copies of Private Keys, in production or backups, on-site or off-site.

6.2.3 Private Key Escrow

Martini Security does not escrow CA Private Keys and does not provide such a service for Subscribers.

6.2.4 Private Key Backup

Martini Security CA Private Keys are copied to multiple geographic locations. All CA private keys are managed and protected under the same controls.

6.2.5 Private Key Archival

Martini Security does not archive private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Martini Security CA Private Keys are generated inside HSMs and are only transferred between HSMs for redundancy or backup purposes. When transferred, keys are encrypted prior to leaving HSMs and unwrapped only inside destination HSMs. Keys never exist in plain text form outside of HSMs.

6.2.7 Private Key Storage on Cryptographic Module

Martini Security CA Private Keys are stored on HSMs meeting the requirements stated in Section 6.2.1.

6.2.8 Method of Activating Private Key

Martini Security CA Private Keys are always stored on HSMs and activated using the mechanisms provided by the HSM provider.

6.2.9 Method of Deactivating Private Key

Martini Security CA Private Keys are always stored on HSMs and deactivated using the mechanisms provided by the HSM provider.

6.2.10 Method of Destroying Private Key

Martini Security CA Private Keys are always stored on HSMs and destroyed using the mechanisms provided by the HSM provider.

The subscriber agreement outlines the subscriber's obligations. This includes among other obligations that Subscriber will destroy their private keys when they are no longer needed or when the certificates to which they correspond expire or are revoked.

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

See Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity periods of Martini Security Root CAs, Subordinate CAs, and Subscriber Certificates are profiled in Section 7.1 of this document.

Martini Security Root and Subordinate CA key pairs have lifetimes corresponding to their certificates. Subscriber key pairs may be reused indefinitely provided that there is no suspicion or confirmation of Private Key compromise.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Access control mechanisms provided by the HSM provider are used to control usage of CA key material.

6.4.2 Activation Data Protection

Usage of credentials that allow usage of CA key material is protected from unauthorized disclosure via a combination of physical and logical means.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Martini Security CA infrastructure and systems are appropriately secured in order to protect CA software and data from unauthorized access or modification. Access to systems is secured via multi-factor authentication whenever possible. Security updates are applied in a timely fashion. Vulnerability scans are run regularly.

6.5.1.1 Access Control

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

6.5.1.1.1 Access Control Policy and Procedures

Each trusted role employee job function has document roles and responsibilities and a mapping to each role to specific employees and associated accounts.

6.5.1.1.2 Account Management

Operational Staff's access is limited to the functionality required to perform their role.

A record of accounts is maintained, along with the conditions and procedures to follow when creating new accounts, groups and roles. Each group and role is mapped to the business function involved in operating the CA.

The principle of least privilege is used when creating users, groups and roles. Membership to a group or assignment to a role is justified based upon business need and tracked in a ticket system. When a user no-longer requires an account, role assignment or group membership their permissions are updated.

Annually all active accounts are reviewed and matched to associated business justifications, any accounts, role assignments or group memberships found that do not have adequate justification are removed and if appropriate a ticket is filed to investigate why the permission was not removed earlier.

Tooling is used to disable accounts for users who have not been active in 30 days. All logon attempts to access any deactivated account are logged.

All account administration activities are be logged and made available for inspection by appropriate security personnel. Account administration activities that are audited include account creation, modification, enabling, disabling, group or role changes, and removal actions.

No Guest, Anonymous, or defaults accounts for any system are allowed. Account sharing is prohibited.

6.5.1.1.3 Least Privilege

The principle of least privilege is applied to all account and access control operations. Each user or system only has the necessary permissions to accomplish assigned tasks.

Users are required to non-privileged accounts or roles when accessing non-privileged functions (such as reading email).

6.5.1.1.4 Access Control Best Practices

Martini Security follows industry best practices for managing access control. Some such examples include:

- 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 toCA 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

When users selectable passwords are used, a robust password policy is applied. See the minimum password practices outlined in Section 6.5.1.1.4 for more information.

Separate accounts and passwords are used for users in trusted roles for non-privileged activities. Each role has a corresponding number of accounts necessary to perform which is documented.

In systems supporting failed authentication counters, they are set to 5 unsuccessful login, where this is not supported additional mitigating controls are applied.

Restoring access when an account is locked requires a separate person in a trusted role to perform the restoration for a timeout period to be reached, depending on system capabilities and security requirements..

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

CA systems are be configured, operated, and maintained so as to ensure the continuous logical separation of CA operations processes and their assigned resources.

This separation is be enforced by:

- Physical and logical isolation mechanisms, such as dedicated systems, micro services, and/or virtualization,
- Fine grained permissions are applied to individual components to ensure access to assigned resources is minimized,
- Software is designed such that interference from another processes is limited by inter-process communication authentication and fine grained permissions,
- Components are designed to be independent from each other such that errors in one component do not propagate to others,
- Logically isolating all trusted components from untrusted components via a network or access control boundary.

6.5.1.2.2 Malicious Code Protection

Systems are defined as idempotent and are regularly re-deployed via Continuous Integration. The continuous integration system is hardened and all code / changes are required by a trusted role prior to deployment.

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

All sensitive information is protected with fine grained ACLs to users, groups or roles with least privileged access.

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.

The technical mechanisms are used to prevent, and detect unauthorized changes or access to sensitive information.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Martini Security has developed policies and procedures to effectively manage the acquisition and development of its CA systems.

Martini Security systems and software are custom built and designed to perform associated CA functions. All software is built using modern development processes that can largely be framed as a mix of waterfall and incremental development. Processes used in development include industry best practices robust test coverage, scenario coverage, fuzzing, security assessments, code reviews and detailed issue tracking.

When third-party vendors are used, selection includes an evaluation of reputation in the market, ability to deliver a quality product, vulnerability history, and the likelihood of remaining viable in the future. Physical product deliveries are received by Trusted Contributors and inspected for evidence of tampering. HSMs are shipped in tamper-evident packaging and tamper bag serial numbers are confirmed with the vendor upon reception.

Martini Security maintains a CA testing environment separate from the production environment. The testing environment reasonably emulates the production environment but does not have access to Martini Security CA Private Keys used in trusted certificates. The purpose of this testing environment is to allow extensive but safe testing of software and systems that are or will be deployed to the CA production environment.

Martini Security has developed and maintains appropriate change control policies and procedures to be followed any time CA systems are modified. Changes to Martini Security CA systems require review by qualified Trusted Personnel who are different from the person requesting the change. Change requests are documented, as are any subsequent required reviews or approvals.

When Martini Security develops software to be used in CA operations, software development policies are put into place and methodologies are followed in order to ensure software quality and integrity. This always includes a requirement for peer review of code changes. Code commit privileges are granted only to qualified and trusted contributors. Nobody with the ability to deploy software to Martini Security PKI systems (e.g. Systems Administrators) may have the ability to unilaterally commit code to core CA software. The reverse is also true.

6.6.2 Security Management Controls

Martini Security has mechanisms in place to control and monitor security-related configuration of CA systems. Equipment, software and configuration is installed and deployed using a documented change control process and a configuration management system. Software integrity is verified upon deployment using checksums.

Trusted systems are deployed in an idempotent fashion to limit the ability of an attacker to install or modify association binaries or configuration. Associated systems only contain the software necessary to perform their specific functions.

Network logical access controls utilizing mutual authentication using X.509 certificates, combined with system hardening techniques such as only exposing specific ports, deploying only the software necessary for operations of individual services, disabling unused features, and logical network segmentation are utilized to ensure only authorized components can interact with each system. These mitigations are tested via automatic tooling on a regular basis.

6.6.3 Life Cycle Security Controls

Martini Security scans all online CA operations systems for vulnerabilities using commercially available security vulnerability testing and analysis tools on a regular basis. Each finding from

scanning activities results in a ticket being filed which kicks off a process to assess the severity and relevance of the associated finding.

Should the finding be determined to be valid it is prioritized based on the risk level. A remediation plan is created and the highest criticality issues will be resolved within 72 hours if feasible. If a vendor patch is required, the patch, when released, is tested before it is deployed into production. Final remediation of the issue is tracked in the associated ticketing system.

We both minimize dependencies and explicitly track each for relevant product vulnerability, or service breach notifications and vendor notification on a regular basis to feed into the aforementioned process.

We employ extensive monitoring and use these to both ensure scalable, reliable services, but also to identify statistical anomalies in usage that may be useful for identifying misconfigurations, changes in environments, or compromise. Regardless of the severity any identified issues are resolved on a priority basis as quickly as possible.

6.7 Network Security Controls

Martini Security implements reasonable network security safeguards and controls to prevent unauthorized access to CA systems and infrastructure.

Martini Security's network is multi-tiered and utilizes the principle of defense in depth.

Martini Security implements reasonable network security safeguards to ensure production environments and logs are regularly scanned and/or reviewed for operational anomalies that may be indicative of a compromise.

Additionally, dependencies are tracked and CVEs and vendor-provided security updates are reviewed regularly for applicability and deployment.

Identified potential compromises and vulnerabilities are tracked in a ticket tracking system and managed to resolution via that system. Decisions to patch, remediate, or otherwise are also tracked in the same ticket tracking system.

6.8 Time-Stamping

See Section 5.5.5.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

All fields are as specified in RFC 5280, including fields and extensions not specifically mentioned. Extensions are not marked critical unless specifically described here as critical.

Root CA Certificate

Field or extension	Value
Serial Number	Must be unique, with 64 bits of output from a CSPRNG
Issuer Distinguished Name	C: US; State: WA; Locality: Seattle; Organization: Martini Security, LLC; Common Name:Martini SHAKEN R<n>, where n is an integer representing the instance of the Root CA Certificate. For example, Martini Shaken R1, Martini Shaken R2, etc.
Subject Distinguished Name	Same as Issuer DN
Validity Period	Up to 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.

Subordinate CA Certificate

Field or extension	Value
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; State: WA; Locality: Seattle; Organization: Martini Security, LLC; Common Name: SHAKEN G<n>, where n is an integer representing the instance of the Subordinate CA Certificate. For example, Martini SHAKEN G2, Martini SHAKEN G3, etc.
Validity Period	Up to 5 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.
Authority Key Identifier	Critical: False. Must be SHA1 hash of Issuer public key.
Certificate Policies	Critical: False. 2.16.840.1.114569.1.1.3
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]

Subscriber Certificate

Field or extension	Value
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}
Validity Period	Up to 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. 2.16.840.1.114569.1.1.3
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 Number(s)

All certificates use X.509 version 3.

7.1.2 Certificate Extensions

See Section 7.1.

7.1.3 Algorithm Object Identifiers

Name	Object Identifier
ecdsa-with-SHA256	1.2.840.10045.4.3.3

7.1.4 Name Forms

Martini Security only issues certificates with the name forms captured in Section 7.1.

7.1.5 Name Constraints

Not applicable.

7.1.6 Certificate Policy Object Identifier

See Section 7.1.

7.1.7 Usage of Policy Constraints Extension

Not Applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

See Section 7.1.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

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 Assessments

8.1 Frequency or Circumstances of Assessment

Martini Security performs a self audit annually to ensure:

1. Requirements of ATIS-1000080, ATIS-1000084, RFC 8555 and other associated RFCs are met,
2. The requirements of the STI-PA CP are met,
3. The requirements of the Martini Security CPS are met,
4. Security review of practices is performed.

If requested by the PMA, Martini Security shall retain an independent auditor for a period of time who shall assess the Issuing STI-CA's compliance with this CP and its CPS.

On an annual basis, due by February 15, the Martini Security CA shall submit to the PMA a CP Compliance Attestation in accordance with CP requirements, that shall include:

- 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 activity for STI-PA.
- Identification/notification of any material changes in technology architecture or business processes supporting the STI-CA activity for STI-PA.

8.2 Identity/Qualifications of Assessor

The auditor must have:

- Demonstrated competence in the field of compliance audits,
- Be thoroughly familiar with the CA's CPS and this CP,
- Perform such compliance audits as a regular ongoing business activity,
- Have appropriate professional experience and certifications,
- And a PKI subject matter specialist.

8.3 Assessor's Relationship to Assessed Entity

The auditor is selected annually and shall either be a private firm that is independent of Martini Security, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation.

In either case, the auditor must not have been involved in the development or maintenance of the entity's CA Facility or CPS. The PMA is ultimately responsible for determining if the auditor meets the requirements specified in the CPS.

8.4 Topics Covered by Assessment

The scope of the assessment will include the CA's published practices, the integrity of the Issuing PKI operations, and conformity with the governing CP requirements.

8.5 Actions Taken as a Result of Deficiency

Identified issues in all categories are tracked in an associated ticket system and managed to close.

If an audit identifies material noncompliance with applicable law, this CP, the CPS, or any other contractual obligations, then the auditor will be required to promptly notify both Martini Security and the PMA.

As a result of any such findings, Martini Security will develop a plan to address any identified noncompliance and submit the plan to the PMA for approval.

8.6 Communication of Results

Annual reports of summarizing findings, and overall posture are produced and presented to management.

By February 1 of each year Martini Security submits a copy of this report to the PMA. This report will minimally 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 activity for STI-PA,
- Identification/notification of any material changes in technology architecture or business processes supporting the STI-CA activity for STI-PA,
- If the STI-CA identifies they are not in compliance with the CP, if they had any security incidents, or if there was a significant change in technology architecture or business.

Within 30 days of completion of the audit and identification of corrective measures will be provided to the PMA, or any other entities entitled by law, regulation, or agreement.

9 Other Business and Legal Matters

9.1 Fees

Martini Security pricing is available on its website (https://www.martinisecurity.com/pricing)

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 Confidentiality of Business Information

No stipulation.

9.2.1 Scope of Confidential Information

Confidential information minimally includes materials relating to business & marketing plans, intellectual property, financial data, research data, operational playbooks, secrets such as pins/passwords/combinations and cryptographic keys, information received from third-parties, restricted personal data and information received from Third-Parties.

9.2.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.2.3 Responsibility to Protect Confidential Information

Martini Security employees, agents, and contractors are responsible for protecting confidential information and are bound by Martini Security's policies with respect to the treatment of confidential information or are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.3 Privacy of Personal Information

Martini Security follows the privacy policy posted on its website (https://www.martinisecurity.com/privacy_policy) when handling personal information.

9.3.1 Privacy Plan

No stipulation.

9.3.2 Information Treated as Private

No stipulation.

9.3.3 Responsibility to Protect Private Information

No stipulation.

9.3.4 Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4 Intellectual Property Rights

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

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

9.5 Representations and Warranties

9.5.1 CA Representations and Warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, Martini Security does not make any representations or warranties regarding its products or services. Martini Security represents and warrants, to the extent specified in this CPS, that:

- Martini Security complies, in all material aspects, with the this CPS,
- All certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements found herein,
- and Martini Security will maintain a repository of public information on its website.

9.5.2 Relying Party Representations and Warranties

Each Relying Party represents and warrants that, prior to relying on an Martini Security 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 Martini Security's limitations on its liability related to the use of certificates,
3. Has read, understands, and agrees to this CPS,
4. Verified both the Martini Security certificate and the certificates in the certificate chain,
5. Will not use Martini Security certificate 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 Martini Security certificate 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.

9.5.3 Subscriber Representations and Warranties

1. Each Subscriber warrants to Martini Security and the public-at-large that Subscriber is the legitimate registrant of the organization that is, or will be, the subject of the Martini Security certificate issued to Subscriber, or that Subscriber is the duly authorized agent of such registrant.
2. Each Subscriber warrants that all information in the Martini Security 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 Martini Security 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 Martini Security 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 Martini Security is entitled to revoke Subscriber's Martini Security certificates immediately if the Subscriber violates the terms of the Subscriber Agreement or if Martini Security discovers that any of Subscriber's Martini Security certificates are being used to enable criminal activities such as phishing attacks, or fraud.

9.6 Disclaimers of Warranties

Martini Security certificates and services are provided "as-is." Martini Security disclaims any and all warranties of any type, whether express or implied, including and without limitation any implied warranty of title, non-infringement, merchantability, or fitness for a particular purpose, in connection with any Martini Security service or Martini Security certificate.

9.7 Limitations of Liability

Subscribers should see the subscriber agreement at https://www.martinisecurity.com/repository on details on limitations of liability.

Relying parties should see the CP on details on limitations of liability.

9.8 Indemnities

9.8.1 Indemnification by CA

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

9.8.2 Indemnification by Subscribers

Each Subscriber will indemnify and hold harmless Martini Security and its directors, officers, employees, agents, and affiliates from any and all liabilities, claims, demands, damages, losses, costs, and expenses, including attorneys' fees, arising out of or related to: (i) any misrepresentation or omission of material fact by Subscriber to Martini Security irrespective of whether such misrepresentation or omission was intentional, (ii) Subscriber's violation of the Subscriber Agreement, (iii) any compromise or unauthorized use of an Martini Security certificate or corresponding Private Key, or (iv) Subscriber's misuse of an Martini Security certificate. If applicable law prohibits Subscriber from providing indemnification for another party's negligence or acts, such restriction, or any other restriction required by law for this indemnification provision to be enforceable, shall be deemed to be part of this indemnification provision.

9.8.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify Martini Security, its partners, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any service terms applicable to the services provided by Martini Security or its affiliates and used by the Relying Party, this CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.9 Term and Termination

This CPS and any amendments to this CPS are effective when published to the Martini Security online repository and remain in effect until replaced with a newer version.

9.9.1 Term

This CPS and any amendments to this CPS are effective when published to the Martini Security online repository and remain in effect until replaced with a newer version.

9.9.2 Termination

This CPS and any amendments remain in effect until replaced with a newer version.

9.9.3 Effect of Termination and Survival

Martini Security will communicate the conditions and effect of this CPS's termination via the Martini Security Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the certificate is revoked or expired, even if this CPS terminates.

9.10 Individual Notices and Communications with Participants

Martini Security accepts notices related to this CPS at the locations specified in Section 1.6.2 of this CPS. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from Martini Security. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 1.6.2 of this CPS using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. Martini Security may allow other forms of notice in its Subscriber Agreements.

Additionally Martini Security will notify the PMA at least one month in advance of any planned updates or changes with the potential to affect the SHAKEN PKI operational environment or compliance with the CP, including:

1. Additions or changes of Root CAs
2. Additional CPs at the Root CA level
3. Changes in Certificate issuance procedures
4. Terminations or transition of ownership of Root CAs

9.11 Amendments

9.11.1 Procedure for Amendment

This CPS is reviewed at least annually and may be reviewed more frequently. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place that are

designed to reasonably ensure that this CPS is not amended and published without the prior authorization of the Martini Security PMA. As per Section 1.6.4 this approval process is ultimately governed by the PMA.

STI-CAs shall notify the PMA at least two weeks prior to implementation of any planned change to the infrastructure that has the potential to affect the SHAKEN PKI operational environment, and all new artifacts, including CA root certificates, produced as a result of the change will be provided to the PMA within 24 hours following implementation.

9.11.2 Notification Mechanism and Period

Martini Security posts CPS revisions to its Repository. Martini Security does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice.

9.11.3 Circumstances Under which OID Must be Changed

The PMA is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.12 Dispute Resolution Procedures

Any claim, suit or proceeding arising out of this CPS or any Martini Security product or service must be brought in a state or federal court located in San Jose, California. Martini Security may seek injunctive or other relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of its, its affiliates, or any third party's intellectual property or other proprietary rights.

9.13 Governing Law

The laws of the state of Washington, United States of America, govern the interpretation, construction, and enforcement of this CPS and all proceedings related to Martini Security products and services, including tort claims, without regard to any conflicts of law principles. The United Nations Convention for the International Sale of Goods does not apply to this CPS.

9.14 Compliance with Applicable Law

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

9.15 Miscellaneous Provisions

No stipulation.

9.15.1 Entire Agreement

Martini Security 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.

9.15.2 Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of Martini Security. Unless specified otherwise in a contract with a party, Martini Security does not provide notice of assignment.

9.15.3 Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.15.4 Force Majeure

Martini Security 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 Martini Security's reasonable control. The operation of the Internet is beyond Martini Security's reasonable control.