martini
security

Martini Security SHAKEN Subscriber Agreement

Version 1.1 • 3 May, 2022

Table of Contents

Martini Security SHAKEN

Subscriber Agreement

This Subscriber Agreement (“Agreement”) is a legally binding contract between you and, if applicable, the company, organization or other entity on behalf of which you are acting (collectively, “You” or “Your”) and Martini Security, LLC (“Martini Security,” “We,” or “Our”) regarding Your and Our rights and duties relating to Your acquisition and use of SHAKEN digital certificates issued by Martini Security. If you are acting on behalf of a company, organization or other entity, You represent that you have the authority to bind such entity to this Agreement.

1. Definitions and Terms

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 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 [draftietf-cert-delegation] and [ATIS-1000092].
Key Pair	A Private Key and its associated Public Key.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key or if there is clear evidence that the specific method used to generate the Private Key was flawed.
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
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.
Public Key Cryptography	A type of cryptography that uses a Key Pair to securely encrypt and decrypt messages. One key encrypts a message, and the other key decrypts the message. One key is kept secret (the Private Key), and one is made available to others (the Public Key). These keys are, in essence, large mathematically-related numbers that form a unique pair. Either key may be used to encrypt a message, but only the other corresponding key may be used to decrypt the message.
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 Secure Telephone Identity Certificate issued by Martini Security
The Secure Telephone Identity Governance Authority	The STI-GA is a governing body helping the industry achieve success in mitigating the problem of unwanted robocalling.
Service Provider	A telecommunications service provider serving customers with phone numbers from the NANPA.
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.

Term	**Definition**
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].
Validity Period	The intended term of validity of a Certificate, beginning with the date of issuance ("Valid From" or "Activation" date), and ending on the expiration date indicated in such Certificate ("Valid To" or "Expiry" date).

2. Effective Date, Term, and Survival

2.1 Effective Date of Agreement

This Agreement is effective once You request that Martini Security issue a Martini Security Certificate to You.

2.1 Term

Each of Your Certificates will be valid for the Validity Period indicated in such Certificate unless revoked earlier. This Agreement will remain in force during the entire period during which any of Your Certificates are valid, continuously so as to include any renewal periods (including automatic renewals). Once You no longer possess any valid Martini Security Certificate, this Agreement will terminate.

2.1 Survival

Sections in this Agreement concerning privacy, indemnification, disclaimer of warranties, limitations of liability, governing law, choice of forum, limitations on claims against Martini Security, and prohibitions on the use of fraudulently-obtained Certificates and expired Certificates shall survive any termination or expiration of this Agreement.

3. Your Warranties and Responsibilities

3.1 Warranties

By requesting, accepting, or using a Martini Security Certificate:

- You warrant to Martini Security and the public-at-large that You are the legitimate registrant of the organization, or are going to be, represented in the subject of Your Certificate, or that You are the duly authorized agent of such registrant.
- You warrant to Martini Security and the public-at-large that all information in Your Certificate regarding your organization is accurate, current, reliable, complete, and not misleading.
- You warrant to Martini Security and the public-at-large that all information You have provided to Martini Security is, and You agree that all information you will provide to Martini Security at any time will be, accurate, current, complete, reliable, and not misleading.
- You warrant to Martini Security and the public-at-large that You rightfully hold the Private Key corresponding to the Public Key listed in Your Certificate.
- You warrant to Martini Security and the public-at-large that You have taken, and You agree that at all times You 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 Your Certificate (and any associated activation data or device, e.g. password or token).
- You warrant to Martini Security and the public-at-large that You will destroy the private key associated with your certificates when they are no longer needed or when the certificates which associated the keys expire or are revoked.

3.2 Changes in Certificate Information

If at any time You no affiliated with the organizations associated with any of Your Certificates, or if any of the warranties in Section 3.1 above are no longer true with respect to any of Your Certificates in any other way, You will immediately request that Martini Security revoke the affected Certificates. You may request replacement Martini Security before revoking the affected Certificates, provided that the warranties in Section 3.1 above are true with respect to the replacement Certificates.

3.3 Certificate Issuance

The contents of Your Certificates will be based on the information You or Your ACME Client Software sends to Martini Security.

If Martini Security accepts your request for a Martini Security Certificate, Martini Security will create Your Certificate and it will be provided to You through the ACME protocol. If Martini Security is unable to confirm your identity or authorization, Your request may be denied.

Martini Security may, in its sole discretion, refuse to grant Your request for a Martini Security Certificate, including for any lawful reason stated or not stated in this Agreement.

3.4 Key Pair Generation

Your Key Pair (Public and Private Keys) will be generated by You or Your ACME Client Software on Your systems. You will submit the corresponding Public Key to Martini Security and it will be incorporated into Your Certificate. Martini Security will store Your Certificate in its Certificate Repository. Martini Security will not have access to Your Private Key. Your Private and Public Keys will remain Your property.

3.5 Inspection and Acceptance of Certificates

You warrant to Martini Security and the public-at-large, and You agree, that You will immediately inspect the contents of Your Certificate (“Initial Inspection”), and immediately request revocation if you become aware of any inaccuracies, errors, defects, or other problems (collectively, “Certificate Problems”) with Your Certificate. Your ACME Client Software may perform this task for You. You agree that You will have accepted Your Certificate when You first use Your Certificate or the corresponding Private Key after obtaining Your Certificate, or if You fail to request revocation of Your Certificate immediately following Initial Inspection.

3.6 Installation and Use of Your Certificate

You may reproduce and distribute Your Certificate on a nonexclusive and royalty-free basis, provided that it is reproduced and distributed in full and in compliance with this Agreement. You warrant to Martini Security and the public-at-large, and You agree, that You will install Your Certificate only on servers that are accessible to the organizations listed in Your Certificate, and that you will use Your Certificate solely in compliance with all applicable laws and solely in accordance with this Agreement. Your Certificate will remain the property of Martini Security, subject to Your right to use it as set forth in this Agreement.

The purpose of Your Certificate is limited 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.

Martini Security is not responsible for any legal or other consequences resulting from or associated with the use of Your Certificate. You agree that You will not use Your Certificate for any purpose requiring fail-safe performance, such as the operation of public utilities or power facilities, air traffic control or navigation systems, weapons systems, or any other systems, the failure of which would reasonably be expected to lead to bodily injury, death or property damage.

You warrant to Martini Security and the public-at-large, that You agree, to use the certificates strictly in such manners and use cases as set forth by the STI-GA.

3.7. When to Revoke Your Certificate

You will 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.

You also acknowlege that your certificate will be revoked by the STI-PA for any reason, for example if there any of the followiung is actual or suspected:

- 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.

3.8 When to Cease Using Your Certificate

You warrant to Martini Security a and the public-at-large, and You agree, that You will promptly cease using Your Certificate (i) if any information in Your Certificate is, or becomes, misleading, incorrect, or inaccurate, or (ii) upon the revocation or expiration of Your Certificate.

3.9 When to Cease Using Your Private Key

You warrant to Martini Security and the public-at-large, and You agree, that You will promptly cease all use of the Private Key corresponding to the Public Key included in Your Certificate upon revocation of Your Certificate for reasons of known or suspected Key Compromise.

3.10 Indemnification

You agree to 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 You to Martini Security, irrespective of whether such misrepresentation or omission was intentional, (ii) your violation of this Agreement, (iii) any compromise or unauthorized use of Your Certificate or corresponding Private Key, or (iv) Your misuse of Your Certificate. If applicable law prohibits a party 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.

4. Martini Security's Rights and Responsibilities

3.10 Privacy

Because others may rely on your use of Your Certificates to identify the origin of telecommunications, much of the information You send to Martini Security will be published by Martini Security and will become a matter of public record. Martini Security's collection, storage, use, and disclosure of such information are governed by Martini Security at: https://www.martinisecurity.com/privacy_policy.

4.2 Certificate Repository

During the term of the Agreement, Martini Security will operate and maintain a secure online Repository that is available to authorized relying parties that contain: (i) all past and current Martini Security (including, as applicable, Your Certificate). Martini Security will publish Your Certificate in a Certificate Repository. Martini Security will allow the public to access this information.

4.3 Suspension and Revocation

You acknowledge and accept that Martini Security may immediately suspend Your Certificate if any party notifies Martini Security that Your Certificate is invalid or has been compromised. Martini Security will determine, in its sole discretion, whether to revoke Your Certificate. If You or Your agent requests that Your Certificate be revoked, Martini Security will revoke Your Certificate. If a request for revocation is signed by your Private Key, then Martini Security will automatically deem the request to be valid. You also acknowledge and accept that Martini Security may, without advance notice, immediately revoke Your Certificate if Martini Security determines, in its sole discretion, that: (i) Your Certificate was not properly issued or was obtained through misrepresentation, concealment, or fraud; (ii) Your Certificate has become, or appears to have become, unreliable; (iii) the security of the Private Key corresponding to Your Certificate has been or may be stolen, lost, or otherwise compromised, or subject to unauthorized use; (iv) any information in Your registration with Martini Security or Your request for a Martini Security Certificate has changed or has become false or misleading; (v) You have violated any applicable law, agreement (including this Agreement), or other obligation; (vi) Your Certificate is being used, or has been used, to enable any criminal activity; (vii) You request revocation; (viii) Martini Security is legally required to revoke Your Certificate pursuant to a valid court order issued by a court of competent jurisdiction; (ix) this Agreement has terminated; or (x) there are other reasonable and lawful grounds for revocation. Martini Security will provide notice of revocation via email to the email address of record.

4.4 IMPORTANT DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN MARTINI SECURITY'S CERTIFICATE POLICY AND CERTIFICATE PRACTICE STATEMENT, MARTINI SECURITY CERTIFICATES AND SERVICES ARE PROVIDED "AS-IS" AND 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.

MARTINI SECURITY CANNOT ACCEPT ANY LIABILITY FOR ANY LOSS, HARM, CLAIM, OR ATTORNEY'S FEES IN CONNECTION WITH SUCH CERTIFICATES. ACCORDINGLY, YOU AGREE THAT MARTINI SECURITY WILL NOT BE LIABLE FOR ANY DAMAGES, ATTORNEY'S FEES, OR RECOVERY, REGARDLESS OF WHETHER SUCH DAMAGES ARE DIRECT, CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR COMPENSATORY, EVEN IF MARTINI SECURITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION ON LIABILITY APPLIES IRRESPECTIVE OF THE THEORY OF LIABILITY, I.E., WHETHER THE THEORY OF LIABILITY IS BASED UPON CONTRACT, WARRANTY, INDEMNIFICATION, CONTRIBUTION, TORT, EQUITY, STATUTE OR REGULATION, COMMON LAW, OR ANY OTHER SOURCE OF LAW, STANDARD OF CARE, CATEGORY OF CLAIM, NOTION OF FAULT OR RESPONSIBILITY, OR THEORY OF RECOVERY. THE PARTIES AGREE THAT THIS DISCLAIMER IS INTENDED TO BE CONSTRUED TO THE FULLEST EXTENT ALLOWED BY APPLICABLE LAW.

BY WAY OF FURTHER EXPLANATION REGARDING THE SCOPE OF THE DISCLAIMER, AND WITHOUT WAIVING OR LIMITING THE FOREGOING IN ANY WAY, MARTINI SECURITY DOES NOT MAKE, AND MARTINI SECURITY EXPRESSLY DISCLAIMS, ANY WARRANTY REGARDING ITS RIGHT TO USE ANY TECHNOLOGY, INVENTION, TECHNICAL DESIGN, PROCESS, OR BUSINESS METHOD USED IN EITHER ISSUING MARTINI SECURITY CERTIFICATES OR PROVIDING ANY OF MARTINI SECURITY’S SERVICES. YOU AFFIRMATIVELY AND EXPRESSLY WAIVE THE RIGHT TO HOLD MARTINI SECURITY RESPONSIBLE IN ANY WAY OR SEEK INDEMNIFICATION AGAINST MARTINI SECURITY, FOR ANY INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS, INCLUDING PATENT, TRADEMARK, TRADE SECRET, OR COPYRIGHT.

5. Additional Terms

5.1 Governing Law

The parties agree that the laws of the State of Washington govern this Agreement, irrespective of Washington's choice of law and conflicts of law principles.

5.2. Choice of Forum

Any claim, suit, or proceeding arising out of this Agreement must be brought in a state or federal court located in Seattle, Washington

5.3 Limitation on Claims against Martini Security

Any claim, suit, or proceeding against Martini Security arising out of this Agreement must be commenced within one year of any alleged harm, loss, or wrongful act having occurred.

5.4 No Third-Party Beneficiary

This Agreement does not create rights in favor of any third parties. Furthermore, it is the express intent of the parties that this Agreement shall not be construed to confer any rights on any third party.

5.5 Entire Agreement

This Agreement, together with any documents incorporated by reference in any of the foregoing, constitutes the entire Agreement between You and Martini Security concerning the subject matter hereof.

5.6 Amendment

Martini Security may modify this Agreement from time to time. Each modified version of this Agreement will be posted to Martini Security's website (martinisecurity.com) at least fourteen (14) days before it becomes effective. If such a new version contains material changes and You have provided Martini Security with an email address, Martini Security will send an email to such an address notifying You of such a new version at least fourteen (14) days before it becomes effective. In addition, major changes will be flagged with a new Subscriber Agreement version number in the ACME protocol, so You may be able to configure Your ACME Client Software to notify You of such changes.

5.7 Severability

If any provision of this Agreement is found to be invalid, unenforceable, or contrary to law, then the Agreement will be deemed amended by modifying such provision to the extent necessary to make it valid and enforceable while preserving its intent or, if that is not possible, by striking the provision and enforcing the remainder of this Agreement.

5.8 Authorization to Send Emails

By requesting, accepting, or using a Martini Security's Certificate, You authorize Martini Security to send You emails relating to the renewal or revocation of Your Certificates, or to Your request, acceptance, or use of Martini Security Certificates.

Martini Security may send You such emails using any email address You provide to Martini Security or any commonly-accepted contact email address such as WHOIS domain contacts or common administrative email addresses.