

# **SHAKEN Policy Administrator**

## **Secure Telephone Identity (STI) Certification Authority Methods and Procedures**

**STI-PA Release 2**

iconectiv System Documentation  
STI-PA-US-METHODPROCCA-001  
Issue 4  
October 2021



## Trademark Acknowledgments and Contact Information

- ◆ iconectiv® is a registered trademark of iconectiv, LLC.
- ◆ All brand or product names are trademarks of their respective companies or organizations.

Prepared by:

iconectiv Product Management

# Table of Contents

<b>Executive Summary</b> .....	<b>1</b>
<b>1 Introduction</b> .....	<b>2</b>
<b>2 Contact Information</b> .....	<b>2</b>
<b>3 Certification Authority Registration</b> .....	<b>3</b>
<b>4 Certification Authority Approval</b> .....	<b>3</b>
<b>5 Adding a Certification Authority to the SHAKEN Ecosystem</b> .....	<b>3</b>
<b>6 Procedures for Company Name Change, Business Termination or Sale</b> .....	<b>4</b>
<b>7 Account Management</b> .....	<b>5</b>
7.1 Registering for a Certification Authority Account .....	5
7.2 Submitting Certificate Practice Statement .....	6
7.3 Activating the Certification Authority Account .....	6
7.4 Adding Revoked Certificates to the CRL .....	7
7.5 Account Maintenance .....	7
<b>8 Glossary</b> .....	<b>8</b>
<b>9 References</b> .....	<b>9</b>

## Executive Summary

This document provides the guidelines and procedures to be followed by Certification Authorities (CAs) in the Signature-based Handling of Asserted Information Using toKENs (SHAKEN) ecosystem as introduced in [ATIS-1000074](#), [ATIS-1000080](#) and [ATIS-1000084](#) provide the details on the roles and responsibilities of SHAKEN CAs. These CAs issue Secure Telephone Identity (STI) Certificates to STI Participants (Service Providers and RespOrgs) that are enrolled in the SHAKEN ecosystem. In order to participate in the ecosystem the CAs must be approved by the SHAKEN Policy Management Authority (PMA).

## 1 Introduction

This document describes the process for the approval and enrollment of a Certification Authority as a trusted STI-CA in the SHAKEN ecosystem. In order to be considered for approval as a trusted STI-CA, a CA must submit a Certification Practice Statement (CPS) as a response to the Certificate Policy (CP) established by the PMA. The PMA comprises industry stakeholders, including members of the STI Governance Authority's (STI-GA) Technical WG. The STI-GA is an industry group that was established within the auspice of the Alliance for Telecommunications Industry Solutions (ATIS). The STI-GA provides a venue for Service Provider and RespOrg collaboration in establishing the overall governance to ensure that only approved Service Providers, RespOrgs, and Certification Authorities are enrolled in the SHAKEN ecosystem.

These guidelines are provided as a job aid and user guide. Note, that the complete set of policies that must be followed by a CA are detailed in the CP.

## 2 Contact Information

### iconectiv PMA Director:

100 Somerset Corporate Blvd.  
Bridgewater, NJ 08807

Phone: 1.800.458.4826  
E-mail: PMA@iconectiv.com

### iconectiv STI-PA Administrator (Customer Support):

100 Somerset Corporate Blvd.  
Bridgewater, NJ 08807

Phone: 1.800.458.4826  
E-mail: STI-PA@iconectiv.com

### 3 Certification Authority Registration

The primary input required for the CA's account registration is the CA's CPS. The CPS should follow the outline and provide input based on the SHAKEN CP available at:

<https://authenticate.iconectiv.com>

The details for the account registration are in section [7.1 \[Registering for a Certification Authority Account\]](#).

The CPS can be submitted via email to the STI-PA Admin following registration for an account on the STI-PA website. The STI-PA Admin will contact the CA Registrant to request the CPS, and for additional information required to complete the application.

Once all registration information is received, it will be reviewed by the PMA Director for completeness. The CA will be contacted if additional information is required.

### 4 Certification Authority Approval

The PMA, led by the iconectiv appointed PMA Director, is responsible for ensuring timely review of the submitted CPS. The expected turnaround is 10 business days.

A CA will be notified once they are approved.

### 5 Adding a Certification Authority to the SHAKEN Ecosystem

The CA must provide the root certificate to be loaded into the STI-PA for review. Once the Certification Authority is approved, the CA is added to the STI-PA list of Trusted STI-CAs.

- ◆ The PMA director will notify the STI Participants in the SHAKEN ecosystem of the addition.
- ◆ The CA information will be added to the public STI-PA website.

The CA will receive instructions via email for logging into the STI-PA portal and activating their account. Refer to section [7.3 Activating the Certification Authority Account](#) for procedure details.

## 6 Procedures for Company Name Change, Business Termination or Sale

Once a CA has been added to the ecosystem they must notify the STI-PA of any company name changes, including those related to sales. The CA must also notify the STI-PA if the company terminates business or the CA chooses to no longer be a part of the SHAKEN ecosystem.

- ◆ In the case of a sale, the STI-PA reserves the right to require the new company to re-register to serve as an STI-CA and provide an updated CPS.
- ◆ In the case of a company name change, whether it be due to a sale or other legal or marketing reasons, the CA must notify the STI-PA so the account can be updated. A CA must notify the STI-PA Admin to have their STI-PA account updated, but they must also separately provide any requested legal documents.
- ◆ If a business terminates, the CA must notify the STI-PA per the CP and the account will be deactivated.

In all the above cases the STI-PA will notify the STI Participants.

## 7 Account Management

### 7.1 Registering for a Certification Authority Account

#### Instructions to register on the STI-PA website:

1. Open a browser window and go to the Policy Administrator website:

<https://authenticate.iconectiv.com>

*Recommended browser:*

- Google® Chrome
2. Click the **CERTIFICATION AUTHORITY** → **GET STARTED** link on the page header, or the **GET STARTED** (**GET STARTED**) button below Certification Authority Registration section of the same page to go to the Certification Authority Registration page.
  3. Click on the **BEGIN REGISTRATION** (**BEGIN REGISTRATION**) button at bottom of the page to go to the registration page. See [Figure 1](#) below.
  4. Select the *Certification Authority* **Account Type** radio button.

The screenshot shows the 'Register for a STI-PA Account' page in the iconectiv Policy Administrator. The page title is 'Register for a STI-PA Account'. Below the title, there is a paragraph: 'Please complete the following forms in order to register your company for a STI-PA account. Shortly after submission, the Customer Support team will contact you via email with further information to access the system. Required fields are marked with an asterisk (\*).'

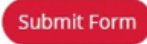
The 'Account Type' section is highlighted with a red box. It contains three radio buttons: 'Certificate Authority' (selected), 'Service Provider', and 'RespOrg'. Below this, there are sections for 'Company Information', 'Registrant Contact Information', and 'Login Credentials'. The 'Company Information' section includes fields for Company Name, Country (United States), Address 1 (street address), Address 2 (suite, floor, etc), City, State/Province (Select), and Postal/ ZIP Code. The 'Registrant Contact Information' section includes fields for First Name, Last Name, Email Address (email@domain.com), Phone Number, and Extension. The 'Login Credentials' section includes a User ID field and a Verification section with an 'I'm not a robot' checkbox and a reCAPTCHA widget. A 'Submit Form' button is located at the bottom of the form. The footer of the page contains 'PRODUCT INFO', '© 2021 iconectiv, LLC. All rights reserved.', and 'LEGAL PRIVACY'.

**Figure 1** Registration Page – Select *Certification Authority* Account Type



5. Complete all required (\*) fields, using correct formats as per noted.

❖ **IMPORTANT NOTE:** Write down the **User ID** separately as you will need this ID to log into the STI-PA web application. **This will be the CA Admin User ID for your company's STI-PA account.**

6. Click the **I'm not a robot** checkbox next to the User ID field (and any additional prompt(s) that may display), then click the **Submit Form** (  ) button.

Upon successful form validation, a success message will display with information on the next step to completing the registration process.

7. Verify **Registrant Contact Email Address**.

Check the mailbox of the Email Address indicated in the success message for the email sent from **STI-PA Do Not Reply** containing the email verification link.

❖ Note: You may need to search for the email in your **Junk** mailbox.

- You must click on the link in the email prior to its expiry.
- If you are unable to complete the verification prior to expiry, contact the STI-PA Admin as noted in section 2 [[Contact Information](#)] of this document to send a new verification email.

8. Complete the Email Verification by clicking the link in the email.

A **Success** message will display if you complete the verification prior to link expiry. You will receive an email explaining the next steps in the registration process.

## 7.2 Submitting Certificate Practice Statement

Once an account is created, the STI-PA Admin will contact the CA to obtain their CPS for review by PMA Director.

## 7.3 Activating the Certification Authority Account

1. Once the account is approved, the STI-PA Admin will contact the CA to obtain the CA's root certificate.
2. Once the root certificate is received, the STI-PA Admin adds that CA to the STI-PA list of Trusted STI-CAs in its website.
  - The STI-PA Admin also **approves** the account registration at this time.

3. Once registration is approved, the CA will receive an email containing the temporary password and link to the STI-PA login page.
4. Using the **CA Admin User ID** created on the registration form as login ID and the temporary password from the email, fill in the login fields on the STI-PA Login page and click the Log In button.
  - The CA Admin user will be prompted to change the password before they can log in for the first time.
  - Password Guidelines:
    - Must be length of 8-99 characters
    - Must have at least one number 0-9
    - Must have one lower case letter a-z
    - Must have one upper case letter A-Z
    - Must include one of the following special characters: ^\$\*.[]{}()? -"!@#%&^, ><'";|\_~`
5. Following password change the CA Admin user will be required to accept the **Account Level Agreement** in order to activate their account in the STI-PA.

Once the account is activated, the account portal allows a CA to update any contact information, add users, as well as to notify the STI-PA of any revoked certificates per the following section. Online Help Pages will be available to guide you in your tasks.

## 7.4 Adding Revoked Certificates to the CRL

Once a CA has an active account, they are able to use the account to provide the STI-PA with certificates that have been revoked. The timeframe in which a CA must notify the STI-PA that as certificate has been revoked is specified in the CP. This does not apply to delegate certificates. Delegate certificates will not be included on the CRL.

## 7.5 Account Maintenance

It is the responsibility of the CA to keep their accounts updated, in particular contact information. If a CA fails to do so, the STI-PA reserves the right to deactivate the CA's account until updated contact information is provided.

## 8 Glossary

<b><u>ACRONYM</u></b>	<b><u>MEANING</u></b>
ATIS	Alliance for Telecommunications Industry Solutions
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
OCN	Operating Carrier Number
SP	Service Provider
RespOrg	ResponsibleOrganization
STI-CA	Secure Telephone Identity Certification Authority
STI-GA	Secure Telephone Identity Governance Authority
STI-PA	Secure Telephone Identity Policy Administrator

## 9 References

- ◆ *ATIS-1000074* - Signature-based Handling of Asserted Information using Tokens (SHAKEN)
- ◆ *ATIS-1000080* - Signature-based Handling of Asserted Information using Tokens (SHAKEN): Governance Model and Certificate Management
- ◆ *ATIS-1000084* - Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators