iconectiv®

SHAKEN Policy Administrator

Secure Telephone Identity (STI) Certification Authority Methods and Procedures

STI-PA Release 1.0

iconectiv System Documentation
STI-PA-US-METHODPROCCA-001
Issue 1
October 2019

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

Executive Summary

This document provides the guidelines and procedures to be followed by Certification Authorities (CAs) in the Secure Handling of Authenticated Identify 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 Service Providers 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 ordered 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 collaboration in establishing the overall governance to ensure that only approved service providers 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 PA Service Desk Administrator:

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://www.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 PA Service Desk Admin following registration for an account on the PA website. The Service Desk 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 PA for review. Once the Certification Authority is approved, the CA is added to the PA list of Trusted STI-CAs.

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

The CA will receive instructions via email for logging into the 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 PA of any company name changes, including those related to sales. The CA must also notify the 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 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 PA so the account can be updated. A CA must notify the PA Service Desk Admin to have their PA account updated, but they must also separately provide any requested legal documents.
- If a business terminates, the CA must notify the PA per the CP and the account will be deactivated.

In all the above cases the PA will notify the Service Providers.

7 Account Management

7.1 Registering for a Certification Authority Account

Instructions to register on the PA website:

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

   https://www.authenticate.iconectiv.com

   Recommended browsers:

   - Google Chrome
   - Firefox

2. Click on the **Register** (Register) button on the upper right corner of the page to go to the registration page. See Figure 1 below.
3. Select the *Certification Authority* **Account Type** radio button.

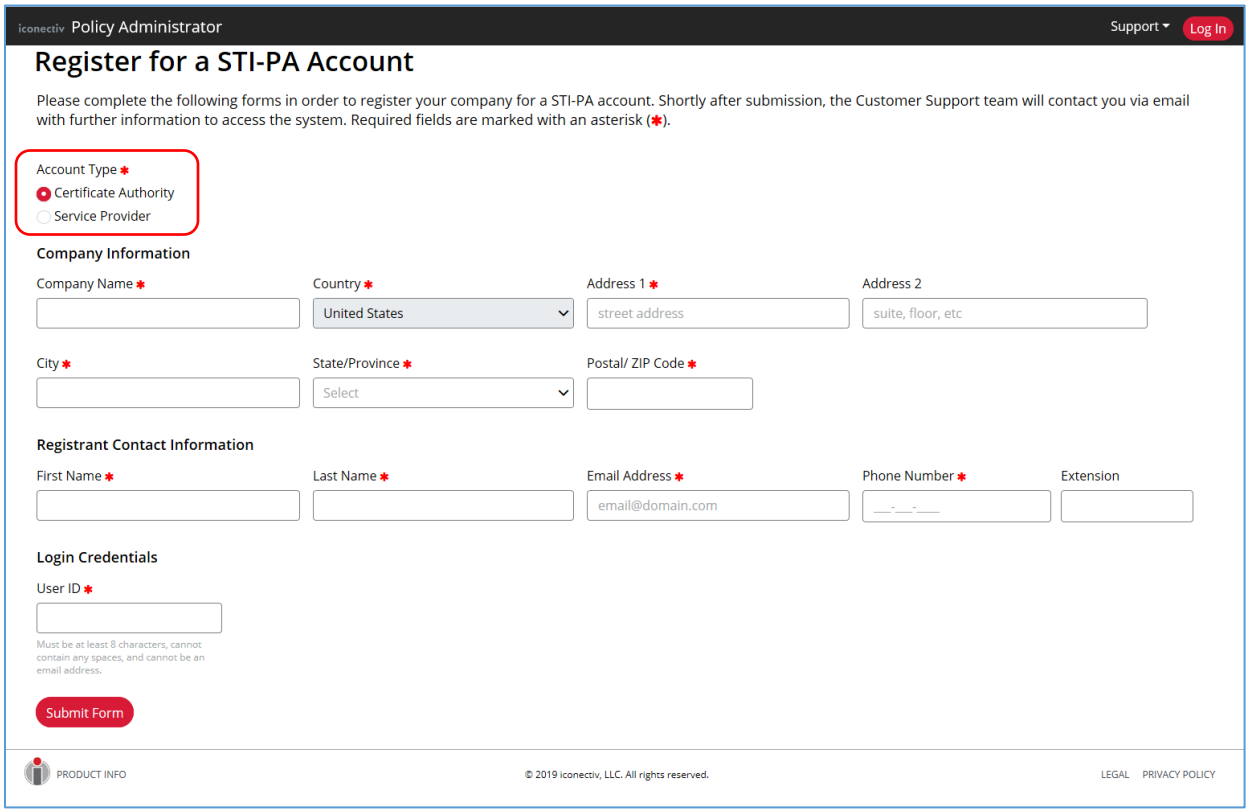
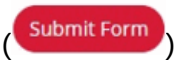


Figure 1 Registration Page – Select *Certification Authority* Account Type

4. 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 PA account.

5. Click the **Submit Form** (

) button.

> ❖ **IMPORTANT NOTE:** DO NOT CLOSE THE BROWSER until you have completed the Email Verication process in these procedure steps.

Upon successful validation, an **Email Verification dialog** will display onscreen with instructions to find the verification email in order to complete the registration.

6. Check the mailbox of the Email Address indicated for the email sent from ***STI-PA Do Not Reply*** containing the verification code and Code Expiry.
   - The email verification must be completed prior to the Code Expiry.
     - ❖ Note: You may need to search for the email in your ***Junk*** mailbox.
   - If you are unable to complete the verification prior to Code Expiry, or you cannot find the verification email, contact the PA Service Desk Admin as noted in section 2 of this document to send a new verification code.
7. Complete the Email Verification.
   a. ***Type*** the verification code exactly as shown in the email in the **Verification Code** textbox.
   b. Click the **Submit Form** button.

A ***Success*** message will display at top of the page if the verification code was submitted correctly. 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 PA Service Desk 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 PA Service Desk Admin will contact the CA to obtain the CA's root certificate.

2. Once the root certificate is received, the PA Service Desk Admin adds that CA to the PA list of Trusted STI-CAs in its website.
   - The PA Service Desk 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 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 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 and initial login the CA Admin user will be required to accept the **Account Level Agreement** in order to activate their account in the 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 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 PA with certificates that have been revoked. The timeframe in which a CA must notify the PA that as certificate has been revoked is specified in the CP.

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 PA reserves the right to deactivate the CA's account until updated contact information is provided.

8 Glossary

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