CST-GA Canadian Secure Token Governance Authority

Policy Guide
Date: November 25, 2021
Version: 1.3

Table of Contents

Overview 3
Definitions 4
Policies 5
Service Provider Token Access Policy 5
Canadian SHAKEN Certificate – Restrictions on Use 9
Solution Vendor Testing Policy 10

Overview

The Canadian Secure Token Governance Authority ("CST-GA") has been directed by the Canadian Radio-television and Telecommunications Commission ("CRTC") Compliance and Enforcement Sector Decision 2019-403 to fulfill the following responsibilities in accordance with ATIS 1000080.v003 and its successors:

1. define policies and procedures governing which entities can acquire STI certificates and,
2. establish policies governing which entities can manage the PKI and issue STI certificates.

This Guide is a repository of policy decisions made by the CST-GA Shareholders' Board from time to time and provides a single source reference for all such policies.

All policies may be reviewed and amended from time to time by the CST-GA Shareholders' Board.

Revision Control

Revision #	Reason
1.0	Initial guide
1.1	Policy 001 v. 1.1
1.2	Policy 001 v 2.0
1.3	Policy 003 v 1.0

Definitions

"Authorized User" means those entities who meet the criteria to receive a Service Provider Code Token as described in CST-GA *Policy 001 Service Provide Code Token Access Policy.*

"Canadian Telephone Number" means telephone numbers derived from the assignment of central office codes by the Canadian Numbering Administrator to qualified Canadian telecommunications service providers.

All other capitalized terms have the meaning set forth in the relevant ATIS documents, i.e. ATIS 1000074 and 1000080 v003, 1000084v002 and their successors.

Policies

Service Provider Token Access Policy

Policy Decision: 001 Version: 2.0

Date: October 14, 2021

Service Provider Code (SPC) Tokens are obtained from the Canadian STI-PA and will permit access to Secure Telephone Identity (STI) certificates from an approved STI Certificate Authority (CA). STI Certificates are used to sign calls (i.e. to authenticate Caller ID) in the Canadian SHAKEN ecosystem.

Shareholders of the Canadian Secure Token Governance Authority ("CST-GA") are eligible to obtain SPC Tokens. Eligibility criteria to become a Shareholder in the CST-GA is as follows:

Canadian Incumbent Local Exchange Carrier ("ILEC"), Small Incumbent Local Exchange Carrier("SiLEC"), Competitive Local Exchange Carrier ("CLEC"), facilities based Wireless Service Provider ("WSP"), registered and in good standing with the Canadian Radio-television and Telecommunications Commission ("CRTC").

ILEC, SiLEC, CLEC or WSP has direct access to Canadian numbering resources from the Canadian Numbering Administrator.

In addition to the foregoing eligibility requirements, CST-GA Shareholders are required to submit a statutory declaration in a form determined by CST-GA from time to time ("Statutory Declaration") reporting the total combined number of Network Access Services and Mobile Subscribers (collectively, "NAS", as further defined in the Statutory Declaration) in its network. For CST-GA Shareholders that participate in the annual Statistics Canada Data Collection Survey ("DCS"), NAS shall be as reported in their most recent DCS filing. CST-GA Shareholders who are not required to participate in the DCS, or who become operational following the annual DCS filing deadline (and therefore have not yet filed a DCS report) will be required to report the actual NAS in its network at the time of its application to become an Authorized User.

Telecommunications Services Providers ("TSPs"), registered with the CRTC in a category which permits the provision of voice services in Canada and who are not eligible to become CST-GA Shareholders may obtain SPC Tokens by establishing with CST-GA their: (a) identity, (b) reputation and (c) STIR/SHAKEN technical compliance, through the form of application in Appendix A of this Policy.

Appendix A

Application to be Authorized by CST-GA to Receive an SPC Token in Canada

Identity

Name
(Name must match CRTC registration)
Primary contact
Name Title
e-mail Telephone Number

List any secondary contacts here:

Registered with the CRTC in the following categories to provide voice services in Canada:

(check all that apply)
BITS License Non-Dominant Carrier Reseller

Number of years of operation under this name in Canada:
Operating Company Number (OCN) registered for this entity:
Related Company *if applicable*:

Note *if OCN is registered to a related company, provide the name of the related company and acknowledge by checking here* ☐ *that the SPC Token assigned to this OCN may only be used for STI Certificates associated with Canadian calling numbers.*

List names of all related entities providing voice services in Canada

List the countries in which the applicant operates telecommunications services

Reputation

The following questions are intended to provide additional information that may be useful for assessing the trustworthiness of the applicant organization, and for ongoing compliance monitoring by the CST-GA.

When has the applicant last filed a STIR/SHAKEN readiness report per CRTC Decision 2021-123 appendix 1 or 2?

Please answer only Yes or No to the following:

a. Has the applicant or any related party ever had CST-GA issued SPC token suspended or revoked?

b. Has the applicant or any related party within the last two years, been subject to any CRTC enforcement actions relating to matters that could affect the integrity of the STIR/SHAKEN framework?

c. Has the applicant or any related party within the past 2 years, received a "Cease and Desist-type" letter from any Canadian government agency (e.g., CRTC) that could affect the integrity of the STIR/SHAKEN framework?

d. Has the applicant participated or is participating in CISC NTWG meetings regarding SHAKEN/STIR (e.g., Task Identification Forms (TIFs) 38, 40)?

e. Does the applicant intend to participate with other Canadian Service Providers in the investigation of spoofing, robo-calling, or other nuisance calling incidents?

f. Does the applicant participate in the Commissioner for Complaints for Telecom-television Services (CCTS)?

g. Is the applicant considered by CCTS to be a non-compliant provider?

h. Is the applicant or any related party an originating and/or terminating service provider in the US?

i. Is the applicant or any related party a current or previous holder of a Service Provider Code token (SPC) in the US?

   If yes, has this US SPC token ever been revoked or suspended?

j. Has the applicant or any related party received in the last 2 years, a "Cease and Desist-type" letter from any US government agency (e.g., FCC, FTC, DoJ)?

k. Is the applicant or any related party registered in the US Robocall Mitigation Database? If yes, please indicate status.

l. Has the applicant in the last 2 years been removed from the US Robocall Mitigation Database by the FCC?

m. Does the applicant or any related party participate in US Industry Traceback Group (ITG) Traceback requests?

Technical Compliance

Attach statement describing how the applicant determines that a caller has the right to use the calling party number including in the following scenarios:

1. **Individual user lines** (e.g., landline, mobile or VoIP client) where the calling number is inserted by the network. If the user has the ability to change the number that will be displayed, describe the mechanism used to determine that the user has the right to use the number. Describe how this information will be verified on a regular basis to ensure it is still accurate.

2. **Enterprise lines:** If the user has the ability to insert the calling party number, describe the mechanism to determine the user has the right to assert the number. If the mechanisms used is described in ATIS-1000089 (*ATIS Technical Report on Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements*) provide details of the implementation – for example, if a central telephone number database is used, identify the database and how it is populated and maintained. If a different mechanism other than those described in ATIS-1000089 is used, describe how this works, and why it provides a similar level of confidence.

By checking the box below, the undersigned hereby acknowledges and agrees that:

1. all information provided in this Application Form is true, complete and correct;
2. such information will be:
    a. relied upon, and used by CST-GA to determine if authorization to acquire an SPC Token will be granted;
    b. in the event that authorization is granted, incorporated by reference into the form of agreement that the undersigned will be required to execute and deliver to be authorized to acquire an SPC Token.

_____

Sign

_____

Print Name

Revision Control

Revision #	Reason
1.0	Initial definition of SPC token access policy
1.1	Amendment to reflect collection of NAS data as a requirement and not as criteria
2.0	Addition of alternate eligibility criteria for TSPs not eligible to become CST-GA Shareholders

Canadian SHAKEN Certificate – Restrictions on Use

Policy Decision: 002 Version: 1.0

Date: August 5, 2020

Authorized Users of STI certificates obtained from approved Certification Authorities in Canada must only use these STI certificates for the authentication of Canadian Telephone Numbers and toll-free telephone numbers assigned to Canadian Authorized Users.

Revision Control

Revision #	Description
1.0	Initial Policy

Solution Vendor Testing Policy

Policy Decision: 003 Version: 1.0

Date: November 25, 2021

Summary

CST-GA has recognized that establishing a process to gain some efficiencies in individual TSP testing of the STIR/SHAKEN policy and certificate management solution in Canada would be of general benefit to TSPs and solution vendors. This process will allow a solution vendor, once successfully performing and submitting User Readiness Test Plan results with their first TSP customer in Canada, to forgo submitting results to the PA for specified test cases/steps with other TSP customers. Subsequent TSP customers, using the same solution vendor and release (as further defined below), are still required to complete the User Readiness Test Plan, but with designated status information for specified test cases/steps.

Process

1. Solution vendor and first Canadian TSP customer (who is an authorized user) initiate the testing process and submit User Readiness Test Plan results to the PA.
2. Once User Readiness Test Plan results are approved by the PA, subsequent Canadian TSP customers using the same vendor solution and release will not be required to include results for the following test cases/steps:
    a. Test_PA_08 (Step 2)
    b. Test_PA_09 (Steps 2 and 3)
    c. Test_PA_10 (Steps 2 and 3)
    d. Test_PA_11 (Steps 2 and 3)
    e. Test_PA_13
    f. Test_PA_14
    g. Test_CA_API_01 (Step 2)
    h. Test_CA_API_02 (Steps 2 and 3)
    i. Test_CA_API_03 (Steps 2 through 5)
    j. Test_CA_API_04 (Steps 2 and 3)
    k. Test_CA_API_05 (Steps 2 and 3)
    l. Test_CR_02
3. For each of the above test cases/steps, the TSP can instead indicate: "**Solution vendor [*Vendor Name*] with release [*Vendor Release Number*] completed as part of the User Readiness Test Plan results approved for TSP [*TSP Name*]**" in the "**Status**" column.
4. For ongoing compliance with this process, each solution vendor will be required to:
    a. Complete any required acceptance testing on subsequent CST-GA STIR/SHAKEN policy and certificate management solution releases with at least one TSP customer, and
    b. Complete the User Readiness Test Plan on any subsequent release of the vendor solution that potentially impacts any of the above specified test cases/steps.
5. CST-GA retains the exclusive right to withdraw or modify this process at any time.

Revision Control

Revision Number	Reason
1.0	Initial Policy