



CST-GA

Canadian Secure Token
Governance Authority

Policy Guide

Date: June 23, 2022

Version: 3.0

Table of Contents

Overview	3
Definitions.....	4
Policies	5
Policy 001 - Service Provider Token Access Policy	5
Policy 002 - RESCINDED Canadian SHAKEN Certificate—Restrictions on Use	9
Policy 003 - Solution Vendor Testing Policy.....	10
Policy 004 - Revocation of STI Service Provider Code (SPC) Token	12
Policy 005 - Reinstatement of STI Service Provider Code (SPC) Token.....	18

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
2.0	Policy 002 Rescinded Policy 001 v.2.1 – Appendix A was revised for consistency with the changes arising from rescinding Policy 002.
3.0	Policy 004 v.1.0 Policy 005 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: 2.1

Date: March 09, 2022

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, the related company must be registered with the CRTC to provide voice services in Canada and listed on the application.

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 Telecommunication 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
2.1	Revision to Appendix A for clarification and consistency with rescinding Policy 002.

Canadian SHAKEN Certificate – Restrictions on Use

Policy Decision: 002 Version: **RESCINDED**

Date: March 09, 2022

Revision Control

Revision #	Reason
1.0	Initial Policy
March 2022	Rescinded

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 #	Reason
1.0	Initial Policy

Revocation of STI Service Provider Code (SPC) Token

Policy Decision: 004

Version: 1.0

Date: June 23, 2022

This policy describes the circumstances for which an STI Service Provider Code (SPC) Token may be revoked, and the process leading to a revocation.

I. Background

The STIR/SHAKEN framework is designed to help mitigate illegal and unwanted caller ID spoofing and robocalling. The role of the Canadian Secure Token Governance Authority (CST-GA) is to oversee the ongoing operations of the framework in Canada and implement policies to ensure the overall integrity and security of the framework.

Service Provider Code (SPC) Tokens are exclusively for eligible entities as defined by the CRTC and outlined in CST-GA Policy 001. An eligible service provider (SP) applies to the CST-GA for a SPC Token, and once assigned, the SPC Token enables the SP to apply to an approved Secure Telephone Identity Certification Authority (STI-CA) for the SHAKEN certificate the SP needs to “sign”¹ calls with the proper level of attestation. Essentially, the SPC Token allows the SP to obtain a Certificate to sign calls within the STIR/SHAKEN ecosystem.

The eligible SPC Token holder must also execute a User Agreement defining the terms under which the SPC Token may be used. Misuse of the SPC Token, or failure to comply with applicable policies and other safeguards, could jeopardize the integrity of the STIR/SHAKEN ecosystem. For this reason, the User Agreement requires compliance with these policies and safeguards:

SPC tokens may only be used for the intended purposes as set forth in the User Agreement and the ATIS SHAKEN Specifications and in compliance with all requirements of such specifications. Entity agrees not to sign any telephone calls that do not meet the levels of attestation in the relevant ATIS SHAKEN Specifications.

II. Authority to Revoke Tokens

Revocation is to be performed by the STI-PA at its own discretion in some well-defined instances, or as directed by the CST-GA.

The STI-PA is primarily responsible for revoking SPC Tokens in the case of compromised credentials (see section III. Reasons for Revocation A), or when an entity is exiting the ecosystem (see section III. Reasons for Revocation B). In either of these instances, there is no question as to whether an SPC Token should be revoked. The STI-PA will also revoke SPC Tokens as directed by the CST-GA.

The CST-GA oversees all revocations other than those for compromised credentials or for when an entity is exiting the ecosystem. The CST-GA retains the right to review all STI-PA revocations.

¹ The term “sign” means the process whereby the originating provider appends a digital signature to attest to the level of trust that it has in the calling number.

There is no refund of annual fees, nor credit brought forward, if an SPC Token is suspended or revoked.

III. Reasons for Revocation

SPC Tokens may be revoked in the following circumstances:

- A. Compromised credentials. If the SPC Token's private key has been lost or stolen, or is or has been misused or otherwise compromised, or the Certification Authority has been compromised.
- B. The SP exits the ecosystem and closes their account with the STI-PA.
- C. Failure to pay any fees owing to CST-GA for more than 60 days past due.
- D. Failure to comply with other CST-GA Policies contained in this Guide, including but not limited to the [SPC Token Access Policy 001](#).
- E. At the direction of the CRTC or another body with relevant federal authority due to a violation of federal law and regulations related to caller ID authentication.
- F. Knowingly and/or repeatedly appending A or B level attestation to a telephone number in the following circumstances:
 - 1. NPA unassigned
 - 2. NXX unassigned
 - 3. NANP non-conforming
 - 4. Do not Originate associated with TN
 - 5. Certificate does not match country of origin
- G. Any breach of the terms and conditions of the User Agreement.
- H. Revocation of an SPC Token (or equivalent) in another jurisdiction.

IV. Complaints

Circumstances which could lead to revocation may only be identified by the CST-GA, STI-PA, SPs, or a regulatory authority (a "complainant"). CST-GA will not respond to complaints from subscribers of telecommunications services or from parties who are outside of the Canadian STIR/SHAKEN ecosystem.

All complaints must be submitted using the standard SPC Token Complaint Submission Form provided in Appendix A of this Policy. Complaints which do not conform to the processes described in this Policy will not be reviewed. Further, complainants must demonstrate that good faith efforts have been made to resolve the complaint directly with the SP.

The CST-GA may inform the CRTC's Chief Compliance and Enforcement Officer of the Complaint and Review process.

V. Complaint Process

1. On receipt of an STI SPC Token Complaint Submission Form, CST-GA will evaluate if it discloses sufficient, accurate information, and if the complaint is related to an established Reason for Revocation under this Policy. Furthermore, the complainant must demonstrate that reasonable effort has been made to resolve the issue directly with the SP.
2. In the event that CST-GA finds that the requirements in paragraph 1 above have been met, CST-GA will notify the complainant and deliver a Notice of Complaint to the respondent. The Notice of Complaint will include:
 - Confidentiality requirements
 - Identification of the complainant and the party against whom the complaint has been made
 - Summary of the complaint and relevant facts
 - Statement of CST-GA decision to investigate further
3. The respondent will have 5 days to respond in writing to the Notice of Complaint.
4. Following receipt of the response from the respondent, the CST-GA will have 10 business days to make a determination that:
 - no further action is required
 - further action or additional information is required
 - A Corrective Action Plan (CAP) is required by respondent. The CAP refers to a specific plan the SP must fulfil and is bound to follow, in order to avoid the revocation of its SPC Token
 - The SPC Token should be revoked without further investigation
5. CST-GA will prepare a Notice of Determination, which will include:
 - Confidentiality requirements
 - Summary of findings
 - Determination
 - Review Process
6. The Notice of Determination will be delivered to the complainant and the respondent.
7. Upon receipt of the Notice of Determination the respondent must communicate in writing within 5 business days of its intention to (1) provide a Corrective Action Plan (if permitted or required to do so under the determination); or (2) seek a review of the determination.
8. If the respondent does not respond in writing within 5 business days, CST-GA will direct the STI-PA to deactivate the SP account and notify all STI-CAs of the revocation of the SPC Token.
9. In the event that the respondent notifies CST-GA of its intention to seek a review of the determination or to implement a CAP (where permitted), CST-GA will direct the STI-PA to notify

the STI-CA not to issue any new or additional certificates to the respondent until the complaint is finally determined under this Policy.

VI. Review Process

The respondent may submit its request for a review using the Request for Review template provided in Appendix B to be delivered to CST-GA, within 5 days of receipt of the CST-GA Notice of Determination.

On receipt of a Request for Review, CST-GA will engage a third-party mediator, selected by the respondent from a list of mediators maintained by CST-GA. The mediator will have 5 business days to review the file and provide its determination to the parties as to whether the original determination should be modified or should stand. Such determination shall be binding on all parties. The entire cost of the mediator and review will borne by the unsuccessful party.

Appendix A

STI SPC Token Complaint Submission Template

At a minimum, the following data must be provided about a complaint:

- Name and affiliation of complainant, including contact information
- Name of party against which claim is submitted, including contact information
- Nature of complaint and supporting information, including reference to the accepted Reasons for Revocation described in the Policy
- Demonstration that reasonable effort has been made to resolve the issue directly
- Acknowledgment that any information provided may be shared with an appropriate regulatory authority such as the CRTC.

The STI SPC Token Complaint is to be submitted directly to CST-GA info@cstga.ca

Appendix B

Request for Review Template

A Request for Review can only be submitted once the CST-GA has provided the respondent with a Notice of Determination. The Request for Review must include the following information:

- Name and affiliation of respondent including contact information
- The determination
- Detailed reason(s) why the determination (and/or Corrective Action Plan if permissible by the determination) is not accepted by the respondent
- Acknowledgment that data may be shared with an appropriate regulatory authority such as the CRTC

Revision Control

Revision #	Reason
1.0	Initial Policy

Reinstatement of STI Service Provider Code (SPC) Token

Policy Decision: 005

Version: 1.0

Date: June 23, 2022

This policy outlines the procedures to reinstate a revoked SPC Token. This policy is intended for Service Providers (SP) whose token access has been revoked and want to reinstate.

Reinstatement

The Service Provider will be considered for SPC Token reinstatement upon re-application to CST-GA. All re-applications are subject to vetting and verification. As part of the re-application process, the SP must include with its application:

A written description of the issues that led to the SPC Token revocation, together with a letter, on SP letterhead, detailing the steps SP has taken to address such issues, signed by a corporate officer. SP must also include a copy of the Corrective Action Plan, if any, issued pursuant to the Revocation Policy.

Further, conditions of reinstatement include payment in full of each of the following:

- Standard application fees
- If applicable, outstanding annual fees
- Any other outstanding fees or other amounts, including fees or other amounts payable by the SP pursuant to the revocation process

Furthermore, there is no refund of annual fees, nor credit brought forward, if an SPC Token is suspended or revoked.

Probationary Period

To ensure the continued security and integrity of the STIR/SHAKEN ecosystem, following reinstatement there will be a six (6) month probationary period. If it is demonstrated, to the satisfaction of CST-GA, that a violation or non-observance of the CST-GA Revocation Policy has occurred, the SP's SPC Token will be immediately revoked, and a further investigation initiated.

Revision Control

Revision #	Reason
1.0	Initial Policy