CRTC INTERCONNECTION STEERING COMMITTEE

NETWORK WORKING GROUP

STIR/SHAKEN Guidelines
Version 2.0

File ID:
NTGLSTSH20

Issue Date:
June, 2023

Issue History

Issue	Editor	Date	Reason for release
0.0	Gerry Thompson, Thomas Rumball	February 11, 2021	Draft of STIR/SHAKEN guideline initiated.
0.1	Gerry Thompson, Thomas Rumball, Ken Politz, Ofir Smadja, Alain Bouvier, Brian Fitzgerald, John MacKenzie	March 11, 2021	Draft of STIR/SHAKEN guideline for NTWG TIF 40 review.
1.0	NTWG TIF 40	May 20, 2021	Draft provided to NTWG for review then forwarding to CISC Steering Committee for consideration. Draft approved and guideline published.
1.1	Gerry Thompson, Thomas Rumball, Ken Politz, Alain Bouvier, Brian Fitzgerald, John MacKenzie	May 4, 2023	Updated draft of STIR/SHAKEN guideline for NTWG TIF 40 review.
2.0	NTWG TIF 40	June 6, 2023	Draft provided to NTWG for review then forwarding to CISC Steering Committee for consideration.

Table of Contents

Introduction

These guidelines are the product of Network Task Identification Form 40 ("TIF 40") and developed through collaborative efforts by the members of the CRTC Interconnection Steering Committee ("CISC") Network Working Group ("NTWG").

TIF 40 was initiated in February 2020 and approved by the CISC Steering Committee in April 2020. TIF 40 was initiated by the industry to investigate technical considerations and make recommendations associated with the implementation of STIR/SHAKEN technology in the Canadian environment. This implementation was initiated by the Canadian Radio-television and Telecommunications Commission (CRTC) in Decisions 2018-32, 2019-402, 2019-403, and 2019-404, and 2021-123. STIR (Secure Telephone ID Revisited) is a group of standards developed by the IETF. SHAKEN (Signature-based Handling of Asserted information using toKENs) is a group of standards developed by ATIS.

In Compliance and Enforcement and Telecom Decision CRTC 2021-123, the Commission directed TSPs to, "*implement STIR/SHAKEN to authenticate and verify caller identification (ID) information for Internet Protocol (IP)-based voice calls as a condition of offering and providing telecommunications services, effective 30 November 2021.*"[1]

These guidelines are developed to distill the findings from TIF 40 into STIR/SHAKEN network deployment recommendations for the Canadian industry. These guidelines take existing standards and add vetted TIF 40 contributions to form network deployment recommendations which may serve as a default or baseline for the industry. Note that the recommendations may be modified by intercarrier operational agreements.

For clarity, TIF 40 describes the STIR/SHAKEN technical landscape. These guidelines extract findings from TIF 40 to recommend baseline STIR/SHAKEN functionality and to identify where a common approach is expected to yield better results for the public. These guidelines are intended to bridge available industry standards with targeted intercarrier implementations.

Purpose

TIF 40 was initiated to address:

- List of current CRTC directives
- List of available standards

[1] Compliance and Enforcement and Telecom Decision CRTC 2021-123 | CRTC

- Applicability to TSP types: ILEC, SILEC, WSP, Types 1 & 2 CLECs, Types 3 & 4 CLECs, IP voice provider reselling PSTN access
- Applicability to call types
    - domestic IP voice calls
    - Canada-US
    - other international
- Terminology: signing, authentication, verification, etc. (for common understanding)
- Support for signing “A”, “B”, “C” attestation: Identify what is required.
    - Calling Name versus known caller
- Treatment of private number/presentation restricted
- Explanation of “verstat” parameter and what it means to service providers of various types
- Presentation rules/recommendations to end users: “A”/“B”/“C”/nothing, verified/not verified
- Call Diversion
- Delegated authority/Entity identity
- Additional items as they are discovered.

Principles

Technological and Competitive Neutrality: Network interconnection services are under the regulatory oversight of the CRTC. In Telecom Decision CRTC 2008-17, issued on 3 March 2008, the Commission states:

> “The Commission notes that pursuant to the Policy Direction, to the extent that it is regulating network interconnection arrangements, the Commission must ensure the technological and competitive neutrality of those arrangements, to the greatest extent possible, to enable competition from new technologies and not to artificially favour either Canadian carriers or resellers.”

The principle of technological and competitive neutrality is maintained throughout these guidelines.

Assumptions and Constraints

In the areas of standards, the CISC NTWG is not a Standards Development Organization (“SDO”). Instead, it reviews standards and specifications developed by SDOs, and where appropriate makes recommendations to the CRTC and Canadian telecom service providers (TSPs) for such standards and specifications to be adopted as Canadian guidelines.

Update Mechanism

These STIR/SHAKEN Guidelines are a “living document.” New standards are being developed and adopted through balloting, and new TSP implementation practices are being developed from implementation experience. New additions to this document will assume that the applicable standards have been approved, infrastructure vendors have adopted such standards, and TSPs have tested the functionality. NTWG members wanting to modify these Guidelines may do so by presenting a contribution at the NTWG. The contribution may then be adopted and incorporated into these Guidelines as the NTWG sees fit, under the guidance of the CISC Administrative Guidelines available on the CRTC web site.

Preamble to Technical Sections

The following technical sections are the result of incorporating contributions from several NTWG members during TIF 40 discussions. Each contribution was discussed thoroughly by the WG to establish relevancy of the topic to the scope of these STIR/SHAKEN guidelines.

In developing these guidelines, NTWG leveraged standard development efforts of IETF, ITU-T, 3GPP and ATIS. Specific references are contained within where applicable. If one of these guidelines conflict with existing or revised CST-GA policies, then the CST-GA policies should prevail.

1.0 Base STIR/SHAKEN

This section provides guidelines and updates for basic STIR/SHAKEN which TSPs deployed to meet the 30 June 2021 target launch date per Decision 2019-402-2, subsequently revised to 30 November 2021 per Decision 2021-123. This section will focus primarily on PASSporTs (Personal ASSertion Token; RFC 8588) which support Caller ID attestation.

As the STIR/SHAKEN governance in Canada has evolved to allow broader TSP participation, Caller ID attestation is now expected as early as possible in the call flow, ideally by the originating TSP.

If a call arrives at a TSP without Caller ID attestation, then "C" level attestation is the highest level of attestation that should be assigned to the call (see section 1.2).

1.1 Origination Identifier (OrigID)

ATIS-1000074 defines the Origination ID. The OrigID is generated and managed by the originating service provider but is primarily intended to assist in traceback when necessary.

As recommended in ATIS-1000074, Canadian TSPs should use the Universally Unique ID (UUID) version 4 as defined in RFC 4122 for OrigIDs. This approach does not provide an absolute guarantee that the OrigID will be globally unique, but the length of the UUID, use of random numbers, along with the inclusion of a time value and the specified algorithm ensures that the OrigID can be considered globally unique (statistically) for all practical purposes.

In addition, even if the OrigID generated by one service provider overlaps with another service provider (theoretically possible, but statistically "impossible"), the SHAKEN PASSporT, through the referenced public STI certificate, identifies the originating service provider, and the combination becomes globally unique.

The OrigID assigns an opaque identifier corresponding to all or part of the originating service provider's network (data centers, IBCF nodes, access networks, IMS core complexes, etc.), customers, customer or interconnecting service provider nodes, classes of customer devices, or other groupings that a service provider might want to use to indicate common call sources for determining things such as reputation or traceback identification of customers or gateways.

1.2 Attestation Levels

Attestation levels (indicators) are defined in ATIS-1000074 as "A", "B", or "C". They are passed from TSP to TSP as STIR/SHAKEN is defined initially as a Network-to-Network Interface (NNI).

A (Full): The signing TSP shall satisfy all the following conditions:

- The signing TSP is responsible for the origination of the call onto the IP-based service provider voice network.
- The signing TSP has a direct authenticated relationship (i.e., commercial agreement) with the calling customer and can identify the calling customer. (This is sometimes called "Know Your Customer" or "KYC".)
- The signing TSP has established a verified association with the telephone number used for the call.

Call Examples where a Calling TN meets "A" Level Attestation:

- A SIP-Switched call from an identified calling customer receives an "A" level attestation if any of the following is true:
    - The Telephone Number (TN), or number, is registered and confirmed;
    - The calling customer uses a spoofed number, and that spoofed number is overridden by the TSP with a number assigned to the calling customer;
    - The calling customer can not originate a call with another number;
    - The calling customer uses a number which the originating TSP verifies that the calling customer is assigned. (In cases where this number is not assigned by the originating TSP (e.g., such assignment is the premise of a delegate certificate[2].)
- A Non-SIP Switched call from an identified calling customer (where the non-SIP switch has an outgoing SIP trunk) receives an "A" level attestation if the number cannot be changed or overridden by the customer per the following examples:
    - A basic POTS or PacketCable customer with Tip/Ring access;
    - A PRI line that is restricted to numbers assigned by the Switch;
    - The customer is unable to use a number assigned by another Telephone Number Service Provider (TNSP), or any other number for that matter.

B (Partial): The signing TSP shall satisfy all the following conditions:

- The signing TSP is responsible for the origination of the call onto its IP-based voice network.

[2] A delegate certificate, as specified in ATIS-1000092, is a method for an originating SP to determine that its customer's call is entitled to full attestation for certain enterprise or legitimate call spoofing scenarios where the originating SP does not have a direct authenticated relationship with the calling customer and does not have a verified association with the calling TN.

- The signing TSP has a direct authenticated relationship (i.e., commercial agreement) with the calling customer and can identify the calling customer (i.e., “Know Your Customer”.)
- The signing TSP has not established a verified association with the TN, or number being used for the call.

Call Examples where a Calling TN meets “B” Level Attestation:

- A SIP-Based identified calling customer – the call receives a “B” level attestation when:
    - the calling customer can place a call with a number that has not been assigned by the Originating TSP but has a direct authenticated relationship with the Originating TSP; or
    - the calling customer can originate a call with the “From” as a toll free or other number provided by another RespOrg (Responsible Organization; an organization that controls the use of a toll-free number, i.e., 1-8XX-NXX-XXXX), but the customer has a direct authenticated relationship with the Originating TSP.
- A non-SIP Switched identified customer (non-SIP switch with outgoing SIP trunk) receives a “B” level attestation when:
    - the calling customer can place a call with any number but has a direct authenticated relationship with the Originating TSP; or
    - the calling customer has a PRI line with or without an assigned block of numbers and calls from this PRI line are not restricted to this list of telephone numbers, but has a direct authenticated relationship with the Originating TSP.

C (Gateway): “C” is assigned by a TSP when the conditions for “A” and “B” are not met. When assigning “C” (Gateway) attestation, the attesting TSP shall satisfy all the following conditions:

- The call entered the TSP’s IP-based network without attestation.
- The attesting TSP has no relationship with the initiator of the call.

Call Examples where a Calling TN meets “C” Level Attestation:

- An unsigned call is received from another TSP (e.g., a domestic or international gateway).

- An unsigned call is received from a non-SIP switch and no information about the identity of the calling customer, or the number can be confirmed.

"C" is assigned to primarily facilitate Traceback by providing the OrigID which can identify the point of interface.

Mixed Traffic Situations: When outgoing calls are signed at the edge of a network, the attestation level must match the lowest level of attestation within the mixed traffic. For example, if there is a known mix of calls that should receive "A" and "B" level attestation, then all these calls must receive a "B" level attestation. It is for this reason that attestation levels should be assigned as close to the origination point as possible.

Example: a legacy switch has a TDM trunk with a combination of "A" and "B" attestation traffic, but the TSP cannot be 100% accurate that each "From" number is from an "A" attestation source on the switch. Therefore, all calls in this group must be assigned "B" level attestation.

1.3 Intra and Inter TSP Calls

There are two groups of calls, those within a TSP's network (intra TSP calls) and those between TSPs (inter TSP calls).

1.3.1 Intra TSP Calls

All SIP INVITES for intra TSP calls do not require a SHAKEN PASSporT. Instead, TSPs may "tag" intra network calls with industry-defined tags, as SIP headers, in either of two formats:

- "P-Attestation-Indicator" and "P-Origination-Id" (based on an ATIS IP-NNI contribution)
- "Attestation-Info" and "Origination-Id" (3GPP TS 24.229 post-version 16.6.0)

"Tagging" is the act of adding assertion information to the above SIP headers at the originating TSP's network. Tagging an intra TSP call satisfies the same objectives as including a PASSporT. The use of tagging SHAKEN attributes for intra TSP calls is at the discretion of the TSP.

1.3.2 Inter TSP Calls

For Inter TSP calls, all SIP INVITES are expected to have a SHAKEN PASSporT based on ATIS-1000074. STIR/SHAKEN introduces three new attributes which

must be considered: Attestation Indicator, Origination Identifier, and “verstat” (a SIP signaling parameter).

- Attestation Indicator (“attest”) is a value that expresses the assertion level of the Caller ID by the originating TSP as discussed in section 1.2. This attestation or claim is substantiated and preserved by an originating TSP’s digital STI certificate (public key cryptography)
- The Origination Identifier (“origid”), as discussed in section 1.1, is opaque information uniquely generated by the originating TSP and describes where the call is originated. It is based upon ATIS-1000074 and 3GPP IMS recommendations. OrigIDs should be constructed such that:
    - If an investigation is required, such as during a Traceback, the terminating TSP will provide the originating TSP with the OrigID to assist in determining who originated the call
    - TSPs should be aware that the OrigID may also be used by a terminating TSP for analytics

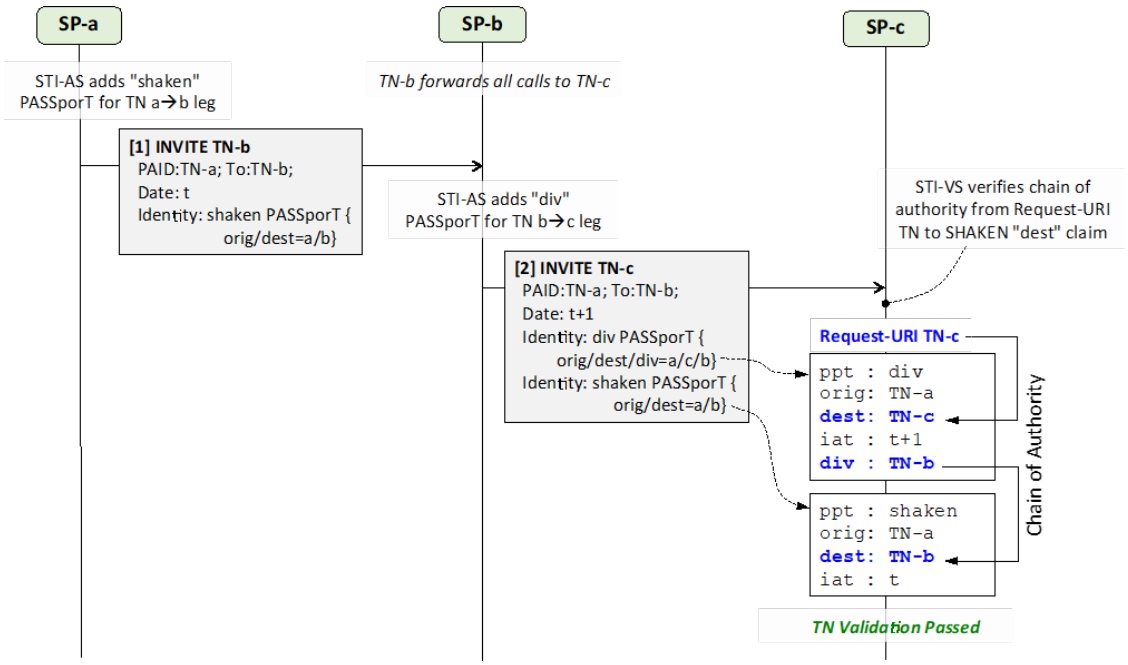
Inter TSP INVITE messages are not expected to contain tags. If tags are detected, they should be removed by the receiving TSP. Otherwise agreed to as part of a bilateral agreement, inclusion of tags could cause a call to fail or be mishandled. This is because tag information is defined to be used within a TSP’s network and not across a Network-to-Network Interface (NNI).

1.4 Call Forwarding (or Diversion)

As of today, the industry is not generally ready to support the Diversion (or “div”) PASSporT, and specifically, achieve interoperability across TSPs. For example, the current ATIS REST API (ATIS-1000082) reference implementation does not include Diversion support. However, there is an effort to promote and adopt a 3GPP-based successor to ATIS-1000082 that minimally supports “shaken”, “div” and “rph” PASSporTs. These proposed changes are now reflected in 3GPP TS 24.229 post-version 17.9.0 (Annex V).

Since Canadian TSPs cannot stop call forwarding (one example of Diversion) from occurring, expected behavior needs to be defined. Diversion includes but is not limited to call forwarding and call transfer.

The following example is for call forwarding, a common form of Diversion [note that this example references a figure in ATIS-1000085 and the normative approach for supporting Diversion]:



It is common to see call forwarding within the SHAKEN ecosystem implemented in one of two ways. Both may be observed. The implementation method is a consequence of different standards bodies and different equipment vendor implementations. Signing and verification guidelines are provided for both ways of implementing call diversions.

- Example:
  - Caller on SP-a, with TN-a, calls Caller on SP-b, with TN-b, who has their call forwarded to SP-c and TN-c
  - Leg One: TN-a calls TN-b
  - Leg Two: Call sent to TN-c

- **The first way, as defined by IMS and 3GPP:**
  - Leg One:
    - From: TN-a
    - PAI: TN-a
    - To: TN-b
    - Request-URI: TN-b
    - Originating Number: From, PAI
    - SHAKEN PASSporT (TN-a, TN-b, iat, attest, origid)
  - Leg Two
    - From: TN-a
    - PAI: TN-a
    - To: TN-b

316 - Request-URI: TN-c
317 - SHAKEN PASSporT (TN-a, TN-b, iat, attest, origid)
318 - Diversion: TN-b
319
320 - The following are guidelines (assuming partial support of "div") for
321 this first way:
322 - If "div" PASSporT is not supported, then just sign
323 (authenticate) with a SHAKEN PASSporT, if none received;
324 else, forward the received SHAKEN PASSporT
325 - During verification, if "div" is supported, validate the "div"
326 chain:
327 - if "div" chain and "shaken" PASSporT validate, then
328 set "verstat" to "TN-Validation-Passed"
329 - else if just the "div" chain does not validate, set
330 "verstat" to "No-TN-Validation"
331 - else validation will fail (i.e., either one or more "div"
332 PASSporTs, other than chain validation, and/or the
333 "shaken" PASSporT fail validation). However, for
334 now, based on NTWG contribution NTCO0699, set
335 "verstat" to "No-TN-Validation" until the industry
336 resolves issues associated with diversion and
337 widespread support for the "div" PASSporT.
338 - During verification, if "div" is not supported, then validate the
339 received "shaken" PASSporT:
340 - if the "shaken" PASSporT is valid then:
341 - if it can be determined that the "shaken"
342 PASSporT "dest" claim and the Request-URI
343 identify the same destination, then set "verstat"
344 to "TN-Validation-Passed" (e.g., the "dest"
345 claim and SIP To header contain a toll-free
346 number, and the Request-URI contains the
347 routing TN for that toll-free number and the
348 verifier knows the routing TN for this number)
349 - else (i.e., the "dest" claim and Request-URI
350 identify different destinations), then set
351 "verstat" to "No-TN-Validation"
352 - if the "shaken" PASSporT is not valid, then validation
353 will fail. However, for now, based on NTWG
354 contribution NTCO0699, set "verstat" to "No-TN-
355 Validation" until the industry resolves issues
356 associated with diversion and widespread support for
357 the "div" PASSporT.
358 - See section 1.5 below for the recommended display for
359 these "div" call scenarios
360
361

- **The second way, as done operationally today by several SIP stacks:**
  - Leg One:
    - From: TN-a
    - PAI: TN-a
    - To: TN-b
    - Request-URI: TN-b
    - Originating Number: From, PAI
    - SHAKEN PASSporT (TN-a, TN-b, iat, attest, origid)
  - Leg Two
    - From: TN-a
    - PAI: TN-a
    - To: TN-c
    - Request-URI: TN-c
    - SHAKEN PASSporT (TN-a, TN-b, iat, attest, origid)
    - Diversion: TN-b
    - NOTE: SIP stack forces the To and Request-URI header TNs to be the same
  - The following guidelines (assuming partial support of “div”) for this second way are the same as above with the following note:
    - If “div” is supported or not, the “shaken” PASSporT will fail validation. The SIP To header TN is TN-c, but the “shaken” PASSporT was signed with a “dest” claim containing TN-b; In this case, if supported by local policy, the recommendation is to treat these calls as “No-TN-Validation” as opposed to “TN-Validation-Failed.”

Since Canadian TSPs cannot stop call forwarding during the deployment of STIR/SHAKEN and it will continue to exist, there are conditions, without Diversion PASSporT support, where verification of an associated SHAKEN PASSporT may fail. The above guidelines best ensure initial support and delivery of these types of calls.

1.4.1 Note on End-user Device Call Diversion

Certain types of end-user devices such as SIP-PBXs can divert incoming calls received from the host SP to a new destination in the global network. The end-user device diverts the call either by redirecting the incoming INVITE request with a 302 Moved Temporarily response, or by retargeting the incoming INVITE request to establish the divert-to call leg. It is up to the host service provider to establish policies to enable the end-user device to divert calls using either of these mechanisms.

If host SP policies allow the end-user device to divert calls via redirection, then the host SP shall consume the “302 response” and retarget the INVITE request on behalf of the end-user device. The SP STI-AS shall perform "div" authentication for the retargeting event before sending the INVITE to the new destination.

If host SP policies allow the end-user device to divert calls via retargeting, things get somewhat more complex since variations in SIP-PBX implementations mean that the STI-AS must support a wider range of use cases in terms of the varying levels of information made available to the authentication (signing) service in the retargeted INVITE request. Furthermore, allowing end-user devices to divert calls via retargeting opens a security breach that must be dealt with.

Since these more complex use cases are not actively being addressed in industry standards, support of end-user devices to divert calls via retargeting is discouraged.

1.5 Display Mechanisms

Currently, the only potential display mechanism for STIR/SHAKEN (apart from modifying Calling Name or CNAM) is the 3GPP “verstat” parameter. The following table recommends TSP settings for the treatment of the “verstat” parameter. Note that it is anticipated that in the current stage of STIR/SHAKEN deployment, calls with legitimate numbers will fail verification for a number of reasons, and a failure indication could be disruptive. As the quantity of these false positives decreases, consideration should be given to replacing the recommended “Normal” displays below with an indication of legitimate verification failure.

Attestation (MO)	Verification (MT)	Analytics Availability	Recommended Display
A - Full	Passed	No	"Calling Number Verified"[3]
		Yes	Analytics results
	Failed	No	Normal
		Yes	Analytics results
	No verification performed	No	Normal
		Yes	Analytics results
B - Partial	Passed	No	Normal
		Yes	Analytics results
	Failed	No	Normal
		Yes	Analytics results
	No verification performed	No	Normal
		Yes	Analytics results
C - Gateway	Passed	No	Normal
		Yes	Analytics results
	Failed	No	Normal
		Yes	Analytics results
	No verification performed	No	Normal
		Yes	Analytics results
No Attestation performed	N/A	No	Normal
		Yes	Analytics results

Recommended Mapping of Verification Results to End User Device (NTCO0699)

During this current stage of STIR/SHAKEN deployment, user experience will vary across the telecommunications ecosystem. TSPs do not directly control if or what ultimately gets displayed on a UE. For example, wireless handset vendors are already representing "Calling Number Verified" with a green check mark. PBXs and POTS home phones have no known way of displaying STIR/SHAKEN results.

The above table does not dictate what method should be employed to guarantee "Normal" behavior. In any event, to avoid false negatives, it is recommended that a "Normal" display is provided that is consistent with the absence of STIR/SHAKEN and Analytics. Specifically, the UE would act normally (pre-

[3] A terminating SP that supports and also successfully validates a SHAKEN PASSporT name claim as defined in section 1.6 should consider both the calling number and name as verified.

445 STIR/SHAKEN environment) when verification results in No-TN-Validation or TN-
446 Validation-Failed.

447 Analytics, if used, can incorporate STIR/SHAKEN results. Analytics could flag
448 "possible fraud" while STIR/SHAKEN by itself would validate the Caller ID.
449 Analytics relies on multiple inputs (including the STIR/SHAKEN verification
450 service result) to execute an algorithm to advise the called party of the integrity of
451 the Calling Line ID. Examples of inputs include a Call Validation Treatment (CVT)
452 application or an in-network approach using switching and called party subscriber
453 records. Special care should be taken when both STIR/SHAKEN and Analytics
454 are implemented. They could present confusing messages to the end user.

455 Although any level of attestation may result in a successful verification, the
456 recommendation in the above table (NTCO0699) is to display "Calling Number
457 Verified" as indicated. Otherwise, the recommendation is to maintain a "Normal"
458 display. To achieve a "Normal" display, no "verstat" is sent to the UE in certain
459 cases. Specifically, the terminating TSP does not send "verstat" when its value is
460 TN-Validation-Failed or No-TN-Validation. The UE should also not act on any
461 TN-Validation-Failed and No-TN-Validation "verstat" values received.

462 ## 1.6 Calling Name (SHAKEN PASSporT Name Claim)

463 The stated objective of this best practice is to restore the confidence in delivery
464 of the calling customer identity, which includes name. Base STIR/SHAKEN
465 provides confidence in the number. The goal is to also restore confidence in the
466 name.

467 Companies should be able to start supporting additional claims (post-version
468 draft-ietf-stir-passport-rcd-24, ATIS-1000094) in a "shaken" PASSporT. If there is
469 a claim that is not supported by a verification service, then such claim should be
470 ignored by the terminating SP. This is proposed as a quick way for the signing
471 SP to also "attest" to the calling name of the originating party.

472 The typical "shaken" PASSporT includes:

473 • Originating Number
474 • Terminating Number
475 • IAT
476 • Origination ID
477 • Attestation Level

478 An enhanced "shaken" PASSporT with a calling name claim includes:

479 • Originating Number
480 • Terminating Number
481 • IAT

- Origination ID
- Attestation Level
- Calling Name (an RCD claim such as “rcd”:{“nam”:“<name_length15>”})

Best practices on how to use the calling name claim include:

- Originating Number “A” attestation – Name can be claimed. Trusted and can be used with confidence.

- Originating Number “B” attestation – A high degree of confidence that the name is correct. The calling name that can be claimed is a name assigned by the originating TSP.

- Originating Number “C” attestation – Name is not attested to. In fact, a signing SP shall not make name claims on “C” attestation.

The terminating SP in Canada has no method of knowing who or when calling name was inserted. The name could have been manipulated during transport, and the TSP could have labelled the call during transport. The “rcd” “nam” key value allows the calling name to be claimed, and regardless of the number of hops, or if labeling is done in transit, the terminating SP can see the name attested to by the originating SP.

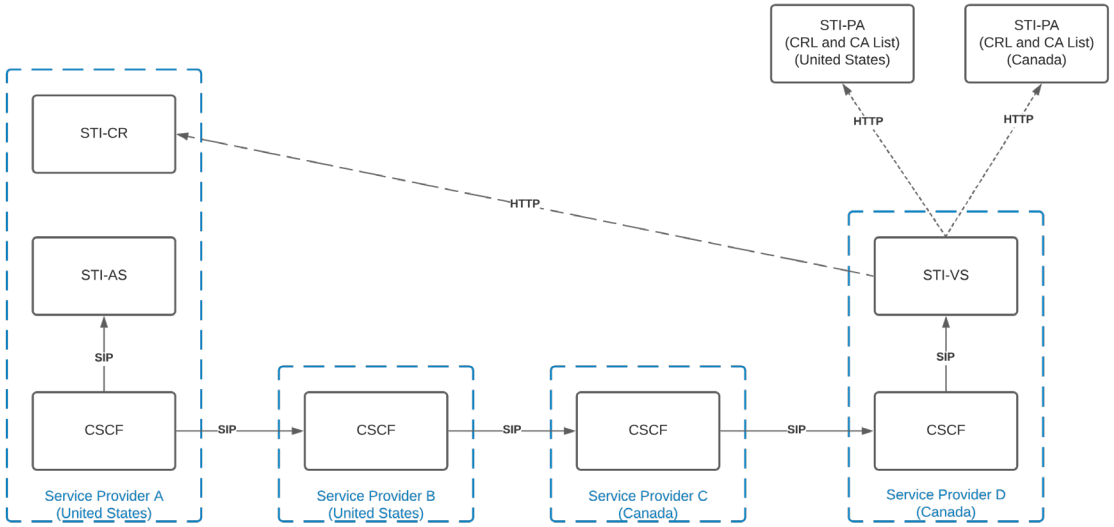
The terminating SP can then decide how to use the additional claim. The terminating SP controls the propagation of name to the end customer, not the originating SP. The additional calling name claim is used to give the terminating SP confidence in the received and verified name.

Terminating SPs that support the SHAKEN PASSporT “nam” claim should consider “Calling Number and Name Verified” as the recommended display per the table in section 1.5 when verification passes, the Attestation Level is “A” and there are no analytics available.

1.7 Cross-Border Traffic to/from U.S.

On July 26, 2022, the STI-GA and the CST-GA signed a Memorandum of Understanding (MoU) to collaborate in the fight to mitigate illegal robocalling. The MoU includes interconnection of STIR/SHAKEN systems in both Canada and the U.S. so that providers can more easily sign calls in one country and have the signature accepted in the other.

ATIS-1000087 and ATIS-1000091, respectively, present short- and longer-term frameworks for supporting both international (+1 country code), as well as other international country codes or regulatory domains. The following figure illustrates a cross-border call example from the U.S. to Canada consistent with ATIS-1000087:



Cross-Border STIR/SHAKEN (U.S. and Canada)

There are four key technical requirements for facilitating cross-border calls with STIR/SHAKEN:

1. A terminating service provider's STI-VS needs access to the certificate used to sign the originating call from the other country,

2. A terminating service provider's STI-VS needs access to the approved list of STI-CAs in the other country, as maintained by their policy administrator,

3. A terminating service provider's STI-VS needs access to the indirect Certificate Revocation List (CRL) in the other country, as referenced in the certificate used to sign the originating call, and

4. A terminating service provider's STI-VS needs access to the root certificate(s) used by a country's policy administrator to sign the approved list of STI-CAs and indirect CRL (this allows the STI-VS to validate authenticity).

Given that the above can all be satisfactorily met, TSPs can technically establish bilateral agreements with individual U.S. entities (who are authorized by the U.S. STI-GA) to send and receive authenticated cross-border calls. However, at this time, there are no related CST-GA policies that enable broad cross-border authentication of calls resulting from joint MoU discussions with the U.S. STI-GA.

1.8 Periodic Reporting

In Compliance and Enforcement and Telecom Decision CRTC 2021-123[1], amongst the directions to TSPs, the Commission directed TSPs to file STIR/SHAKEN status reports per the following table. The required content of the

543 STIR/SHAKEN status reports are provided by and updated from time to time by
544 Commission staff.
545
546

Report due to CRTC	Period From	Period To
every 31 May	1 September	28 February (or 29 February in leap years)
every 30 November	1 March	30 August

547

2.0 Future Guideline Updates for STIR/SHAKEN Enhancements

STIR/SHAKEN enhancements continue to be developed and their standards are emerging or evolving. As these standards mature and related contributions are presented to and adopted by the NTWG, these Guidelines will be updated accordingly. Enhancements could include but are not limited to:

Toll Free

Toll Free, as defined in ATIS-1000093, is a particular and candidate use case for delegate certificates (e.g., for non-facilities-based RespOrgs or Responsible Organizations). To date, there has been little expressed need amongst TSPs in Canada for delegate certificates to support this use case.

Call Diversion and interoperability

Diversion ("div") support and implementation, as specified in IETF RFC 8946 and ATIS-1000085, is discussed in section 1.4. As highlighted, broad, interoperable support of diversion will first require, for example, a richer, preferably industry standard, REST API than the reference implementation originally defined in ATIS-1000082 for just SHAKEN PASSporTs.

Rich Call Data (RCD)

RCD support and implementation, as specified in post-version draft-ietf-stir-passport-rcd-24 and ATIS-1000094 is at an early stage. Section 1.6 introduces optional support for the SHAKEN PASSporT name claim as an initial step towards broader originating SP validated claims and implementation support.

Display evolution

To the extent possible, display should be consistent across TSPs. When Analytics play a more significant role in determining display data, the guidelines in section 1.5 should be updated. No industry standards are anticipated in this area beyond early work documented in ATIS Technical Report (ATIS-1000081)

Resource Priority Header (RPH)

The Emergency Services Working Group (ESWG) continues to file status reports to the CRTC regarding the application of the STIR/SHAKEN framework for processing NG9-1-1 emergency calls and emergency callbacks. Although ATIS-1000078 defines the separate SIP Identity header using the "rph" PASSporT, other required standards have not yet been published. These other key standards are expected in 2023 and it has been the experience of the EWSG that vendors and TSPs then require up to 24 months prior to the introduction of such functionality.

Appendix: Glossary

(adapted from NTTF40 interim report, NTRE070)

3GPP	3rd Generation Partner Project (consortium of 7 mobile SDOs)
A	Attestation Level A (ATIS-1000074)
API	Application Programming Interface
AS	Authentication Service
ATIS	Alliance for Telecommunications Industry Solutions
B	Attestation Level B (ATIS-1000074)
C	Attestation Level C (ATIS-1000074)
Caller ID	Calling Line Identification (the telephone number of the calling party)
CA	Certification Authority
CISC	CRTC Interconnect Steering Committee
CLEC	Competitive Local Exchange Carrier
CNAM	Calling NAMe (name of account holder, associated with Caller ID)
CST-GA	Canadian Secure Token Governance Authority
CRTC	Canadian Radio-television and Telecommunications Commission
Customer	Refers to the retail end-user making or receiving a call (a Customer may be an individual or an enterprise, but a TSP carrying the call is not a Customer)
CVT	Call Validation Treatment

GA	Governance Authority
IETF	Internet Engineering Task Force
ILEC	Incumbent Local Exchange Carrier
INVITE	The initial call setup message in SIP
IP	Internet Protocol
IP-NNI	Internet Protocol Network-to-Network Interface task force
KYC	Know Your Customer
MVNO	Mobile Virtual Network Operator
NNI	Network-to-Network Interface
NTWG	CISC Network Working Group
PA	Policy Administrator
PacketCable	IP Telephony over cable television (DOCSIS standard)
PBX	Private Branch Exchange
PASSporT	Personal ASSertion Token (RFC 8588)
POTS	Plain Ordinary Telephone Service (usually refers to home phone)
REST	REpresentational State Transfer
RFC	Request for Comments (IETF)
RPH	Resource-Priority Header

SDO	Standards Development Organization
SHAKEN	Signature-based Handling of Asserted information using toKENs (ATIS)
SIP	Session Initiation Protocol
SS7	Signaling System number 7, the signaling system in the legacy TDM network
STI	Secure Telephone Identity
STIR	Secure Telephone Identity Revisited (IETF)
TDM	Time-Domain Multiplex
TN	Telephone Number
tn-a	originating TN
tn-b	called TN
tn-c	alternate TN that the call is diverted or forwarded to
TNAuthList	Telephone Number Authorization List
TNSP	Telephone Number Service Provider
TS	Technical Specification (3GPP)
TSP	Telecommunications Service Provider
VS	Verification Service

587

588 ** End of Document **