

Improper Authentication and Attestation

Purpose and Scope

This STI-GA document relies on the industry accepted STIR SHAKEN standard(s) including the definition of A, B, and C Attestation levels.

Because the STI-GA and its industry partners may need to investigate improper use of STI certificates as part of the token revocation process, agreed definitions of Improper Authentication and Improper Attestation are being published to support STI GA processes and policies. This document is not an STI-GA Policy, or a best practice. It constitutes general guidance to be used by the STI-GA Board and its industry partners in helping to determine if a party is improperly authenticating or attesting to calls. Any effort by the STI-GA Board to revoke an SPC token for any reason will follow the published Revocation Process.

Definitions

Improper Authentication - Using the STI certificate to authenticate any information contained within an STI-GA recognized SHAKEN extension that is known to be false.

Improper Authentications include, but are not limited to:

- The inclusion of an RCD extension signed with an STI certificate where the data in that RCD extension has been falsified.
- The inclusion of an RCD extension signed with an STI certificate where the SHAKEN Attestation for the call is set at Level-C.
- The inclusion of an RPH extension signed with an STI certificate where the call does not qualify for priority treatment.

Improper Attestation – Attestation is a process specifically defined within the SHAKEN standard. Any Attestation level set that does not conform with the industry standards set in ATIS 1000074 (see attachment A). An Improper Attestation includes any call where an originating service provider (OSP) signs a call with a level of Attestation inconsistent with the information it has, or is required to have, about the call.

- A-Level Attestations denote that the OSP has a direct authenticated relationship with the customer from which the call came and can verify the customer's right to use the Telephone Number (TN) in the caller ID field.
- B-Level Attestations denote that the originating SP has a direct authenticated relationship with the customer from which the call came but cannot verify the customer's right to use the TN in the caller ID field.
- C-Level Attestations denote only that the call signer has no relationship with the initiator of the call. In this case the call signer is making no claim whatsoever about the accuracy of the TN in the caller ID field or the customer that initiated the call.

Improper Attestations may include, but are not limited to:

- An A-Level Attestation on an illegally spoofed call. Indicators of an illegally spoofed TN are unallocated, invalid or on a reasonable Do Not Originate list. But a legitimate TN could also be illegally spoofed.
- A B-Level Attestation where the originating provider has not validated the customer.
- A C-Level Attestation on a call when the OSP provides the Attestation. (This does not apply to Gateway and Intermediate SPs, when they are required by the FCC to sign unsigned calls.)

B- & C-Level Attestations

B-Level Attestations denote that the OSP can validate the customer from which the call came, but not the TN in the caller ID field. As there is no way to objectively and easily determine whether the OSP is being truthful in its claim that it can identify the customer, the STI-GA is not considering enforcement against improper B-Level Attestations.

A call given B-Level Attestation, where the OSP does not *have a direct authenticated relationship with the customer or cannot identify the customer*, is a call for which the level of Attestation is inconsistent with the information the OSP has, or is required to have, about the call.

C-Level Attestations denote only that the call signer has no relationship with the initiator of the call. In this case the call signer is making no claim whatsoever about the accuracy of the number in the caller ID field or the customer that initiated the call. The STI-GA is not considering enforcement against improper C-Level Attestations.

A call given C-Level Attestation where the OSP is under an FCC know your customer requirement, is a call for which the level of Attestation is inconsistent with the information the OSP has, or is required to have, about the call.

Attachment A

A. Full Attestation: *The signing provider shall satisfy all of the following conditions:*

- *Is responsible for the origination of the call onto the IP-based service provider voice network.*
- *Has a direct authenticated relationship with the customer and can identify the customer.*
- *Has established a verified association with the telephone number used for the call.*

NOTE 1: The signing provider is asserting that their customer can “legitimately” use the telephone number that appears as the calling party (i.e., the Caller ID). The legitimacy of the telephone number(s) the originator of the call can use is subject to signer-specific policy, but could use mechanisms such as the following:

- *The TN was assigned to this customer by the signing service provider.*
- *This TN is one of a range of numbers assigned to an enterprise or wholesale customer.*
- *The signing service provider has ascertained that the customer is authorized to use a TN (e.g., by business agreement or evidence the customer has access to use the number). This includes TNs assigned by another service provider.*
- *The TN is not permanently assigned to an individual customer but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe.*

NOTE 2: Ultimately it is up to service provider policy to decide what constitutes “legitimate right to assert a telephone number” but the service provider’s reputation may be directly dependent on how rigorous they have been in making this assertion.

B. Partial Attestation: *The signing provider shall satisfy all of the following conditions:*

- *Is responsible for the origination of the call onto the IP-based service provider voice network.*
- *Has a direct authenticated relationship with the customer and can identify the customer.*
- *Has NOT established a verified association with the telephone number being used for the call.*

NOTE: By populating this value, the service provider attests that it can trace the source of the call to a customer for policy enforcement purposes.

C. Gateway Attestation: *The signing provider shall satisfy all of the following conditions:*

- *Has no relationship with the initiator of the call (e.g., international gateways).*

NOTE: The signer/originating service provider should be able to trace a call to an interconnecting service provider and/or peer node for traceback or policy enforcement purposes. Gateway attestation may also be used when the STI-AS does not have sufficient information for determining that an "A" or "B" attestation level applies even when the call was received at a customer interface.
