**Contribution**

**TITLE:** Proposed update to Section 7.1 of “Signature-based Handling of Asserted Information Using Tokens” (Draft - IPNNI-2016-00003R010) regarding TN Attestations

**SOURCE\*:** Doug Bellows, Senior Engineer – Inteliquent, Inc.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ABSTRACT**

In applying the SHAKEN attestation procedure, there will be a number of scenarios where a service provider will attest to TNs that they cannot authenticate directly and/or TNs that are not tied to an individual user or enterprise customer. This document proposes updates to the wording of section 7.1 - “Certificate Attestation Policy Indication” to provide a more general description of these scenarios.

**NOTICE**

This is a draft document and thus, is dynamic in nature. It does not reflect a consensus of the ATIS-SIP Forum IP-NNI Task Force and it may be changed or modified. Neither ATIS nor the SIP Forum makes any representation or warranty, express or implied, with respect to the sufficiency, accuracy or utility of the information or opinion contained or reflected in the material utilized. ATIS and the SIP Forum further expressly advise that any use of or reliance upon the material in question is at your risk and neither ATIS nor the SIP Forum shall be liable for any damage or injury, of whatever nature, incurred by any person arising out of any utilization of the material. It is possible that this material will at some future date be included in a copyrighted work by ATIS or the SIP Forum.

\* CONTACT: Doug Bellows; email: dbellows@inteliquent.com; Tel: +1-312-380-4509

# STI Certificate Creation

…

## Certificate Attestation Policy Indication

As detailed in draft-ietf-stir-certificates, level of assurance (LOA) indicators can be included as Object Identifiers (OIDs) in the certificate’s “certificate policy extension” as defined in RFC5280 and used as a mechanism to represent the type of attestation the signature is representing at the time of signing. This indication allows for both identifying the service provider that is vouching for the call as well as a clear indication of what information the service provider is attesting.

In the SHAKEN framework we will use this certificate policy indication for attestation in the following scenarios:

A.  **Full Attestation:** The signing provider:

* 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: The signing provider is asserting that their customer can “legitimately” insert the 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 number was assigned to this customer by the signing provider.
* This number is one of a range of numbers assigned to an enterprise or wholesale customer.
* The signing provider has ascertained that the customer is authorized to use a number assigned by another service provider (e.g. by business agreement or proof the customer has access to use the number).
* The number 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: ultimately it is up to service provider policy to decide what constitutes “legitimate right to assert a number” but the service provider’s reputation in various data analytics may be directly dependent on how rigorous they have been.

B. **Partial Attestation:** The signing provider:

* is responsible for the origination of the call onto the telephone 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: Each customer will have a unique identifier, but it will not be possible to reverse engineer the identity of the customer purely from the identifier, certificate, or signature. The unique identifier provides a consistent identifier to allow data analytics to establish a reputation profile and assess the reliability of information asserted by this customer. The unique identifier also provides a reliable mechanism to identify the customer for forensic analysis or legal action where appropriate.

C. **Gateway Attestation:** The signing provider:

* is the entry point of the call onto the telephone network
* has no relationship to the initiator of the call (e.g., international gateways).

Note: The signature will provide a unique identifier of the node. (The signer is not asserting anything other than “this is the point where the call entered my network”.)

There will be three SHAKEN assigned OIDs in an IANA registry that will be used globally in all certificate creation for these three scenarios. They will be of the form ‘0.0.0.0’ and will be included specifically in this document when created and available.