**Contribution**

**TITLE:** Contribution: Proposed updates to IPNNI-2019-00021R003, draft TR on “Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Delegate Certificates”

**SOURCE:** Doug Bellows, Inteliquent, Inc.

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

**ABSTRACT**

This contribution contains a proposed update to the description of the use of TNAuthlist for SHAKEN signing in IPNNI-2019-00021R003

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

**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.

#

# Overview

SHAKEN uses the protocols and mechanisms defined by the IETF Secure Telephone Identity Revisited (STIR) Working Group. The STIR document [RFC8226] describes a credential system in the form of STI certificates that enables telephone service providers to cryptographically assert authority over telephone numbers. The scope of an STI certificate is expressed by the certificate’s TNAuthList object. As defined in [RFC8226], a TNAuthList can identify the set (or a subset) of TNs assigned to the certificate holder. Alternatively, the TNAuthList may contain an SPC value assigned to the telephone service provider holding the certificate, with the implication that it identifies all of the telephone numbers associated with that identifier for the service provider.

To avoid unnecessary complexity, the SHAKEN specifications profile the STI certificate scoping mechanism provided by [RFC8226]. [ATIS-1000080-E] restricts the contents of a SHAKEN certificate TNAuthList object to a single SPC value assigned to the SHAKEN SP holding the certificate. Furthermore, [ATIS-1000074-E] utilizes the SPC value in the TNAuthList solely as an identifier of the signing SP independent of the calling TNs used on individual calls for which the SP performs the STI-AS function. This enables a SHAKEN-compliant SP to provide full attestation for a customer originating a call from a calling TN assigned by a different TN service provider. These simplifications are justified given that a SHAKEN SP must pass a very rigorous STI-PA vetting process in order to obtain a SHAKEN certificate.