**ATIS-1000088**

# A Framework for SHAKEN Attestation and Origination Identifier

**TECHNICAL REPORT**

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

The SIP Forum is a leading IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations; interoperability testing events and special workshops, educational activities, and general promotion of IP communications standards, services, and technology for service provider, enterprise, and governmental applications. The SIP Forum is also the producer of the annual SIPNOC conferences (for SIP Network Operators Conference), focused on the technical requirements of the service provider community. One of the Forum's technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation that provides detailed guidelines for direct IP peering and interoperability between IP PBXs and SIP-based service provider networks, and the SIPconnect Certification Testing Program, a unique certification testing program that includes a certification test suite and test platform, and an associated "SIPconnect Certified" logo program that provides an official "seal of certification" for companies products and services that have officially achieved conformance with the SIPconnect specification. Other important Forum initiatives include work in security, SIP and IPv6, and IP-based Network-to-Network Interconnection (IP-NNI). For more information about all SIP Forum initiatives, please visit:

< http://www.sipforum.org/ >



# ATIS-1000088, A Framework for SHAKEN Attestation and Origination Identifier

Is an ATIS & SIP Forum Joint Standard developed by the **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **Technical Working Group (TWG)** under the **SIP Forum**.


*Published by*

**Alliance for Telecommunications Industry Solutions**
**1200 G Street, NW, Suite 500**
**Washington, DC 20005**

**SIP Forum LLC**
**733 Turnpike Street, Suite 192**
**North Andover, MA 01845**

## Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. International Telecommunication Union Telecommunication Sector (ITU-T) and U.S. ITU Radiocommunication Sector (ITU-R) Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The SIP Forum is an IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations, the SIPit, SIPconnect-IT, and RTCWeb-it interoperability testing events, special workshops, educational seminars, and general promotion of SIP in the industry. The SIP Forum is also the producer of the annual SIP Network Operators Conference (SIPNOC), focused on the technical requirements of the service provider community. One of the Forum's notable technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation for direct IP peering and interoperability between IP Private Branch Exchanges (PBXs) and SIP-based service provider networks. Other important Forum initiatives include work in Video Relay Service (VRS) interoperability, security, Network-to-Network Interoperability (NNI), and SIP and IPv6.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005, and/or to the SIP Forum, 733 Turnpike Street, Suite 192, North Andover, MA, 01845.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

The **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **SIP Forum Technical Working Group (TWG)** was responsible for the development of this document.

## Table of Contents



## Table of Figures



## Table of Tables

ATIS Technical Report on –

# A Framework for SHAKEN Attestation and Origination Identifier

## 1 Scope, Purpose, & Application

### *1.1 Scope*

This technical report provides a framework for SHAKEN (ATIS-1000074-E, [Ref. 1]) attestation and granularity of the Origination Identifier.

### *1.2 Purpose*

The population of attestation indicator and origination identifier in the SHAKEN Identity header relies on decisions the originating service provider (originating SP) makes based on the type of interface at the ingress to its network, knowledge of the customer or SP entity it has received the call from, and knowledge or agreements as to the calling party telephone numbers (calling TNs) used on the interface. These determinations are made both through administrative and security management procedures as well as security services applied at call processing time. The resulting values are provided to the SHAKEN Secure Telephone Identity Authentication Service (STI-AS) function to be passed with the protected call data. This report documents the characteristics of the security services applied at the User-to-Network Interface or Network-to-Network Interface of an originating SP, and some guidelines for the population of SHAKEN attestation indicator and origination identifier based on these services.

The material and guidelines presented here should be considered informative, as practice and norms can be expected to evolve with deployment and industry experience.

## 2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Technical Report. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Technical Report are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] ATIS-1000074-E, Errata to Signature-based Handling of Asserted Information using toKENs (SHAKEN)

[Ref 2] ATIS-1000080-E, Errata to Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management

[Ref 3] ITU-T Recommendation X.811 (04/1995) | ISO/IEC 10181-2:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework

[Ref 4] ITU-T Recommendation X.815 (11/1995) | ISO/IEC 10181-6:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework

[Ref 5] ITU-T Recommendation X.812 (11/1995) | ISO/IEC 10181-3:1996, Information technology – Open Systems Interconnection – Security Frameworks For Open Systems: Access Control Framework

[Ref 6] CCITT Recommendation X.800 (1991), Security architecture for Open Systems Interconnection for CCITT applications.

[Ref 7] ATIS-1000030.2008(S2018) - Authentication and Authorization Requirements for Next Generation Network (NGN)

[Ref 8] NIST SP 800-63-3 - NIST Special Publication 800-63-3 Digital Identity Guidelines

[Ref 9] CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates Version 1.6.8

[Ref 10] IETF RFC 8224 – Authenticated Identity Management in the Session Initiation Protocol.

# 3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < https://glossary.atis.org >.

## *3.1 Definitions*

**Customer**: Typically a service provider's subscriber, which may or not be the ultimate end-user of the telecommunications service. A customer, for example, may be a person, enterprise, reseller, or value-added service provider. See description in Clause 5.2.

**End user**: The entity ultimately consuming the VoIP-based telecommunications service. For the purposes of this report, an end user may directly be the customer of a service provider or may indirectly use the VoIP-based telecommunications service through another entity such as a reseller or value-added service provider. See description in Clause 5.2.

**Identity**: Unless otherwise qualified, an identifier that unambiguously distinguishes an entity for authentication and other security and policy application purposes (compare to "distinguished identifier" as used in X.811 [Ref 3]). For the purposes of this report, an identity may or may not be a "TN-based caller identity" depending on the context.

**Principal**: An entity whose identity can be authenticated (X.811 [Ref 3]). For the purposes of this report the principal will typically be a service provider, customer, end user, or devices and systems under their control, depending on the context.

**Real-world identity**: Identifiers and identifying characteristics of a principal outside of the telecommunications services domain, including but not limited to personal or business name, physical location or postal address, government-issued identifiers, credit information, etc. Compare to the use of "real-life identity" and "real-world identity" in NIST SP 800-63-3 [Ref 8].

**Responsible Organization (RespOrg):** Entity designated as the agent for the Toll-Free subscriber to obtain, manage and administer Toll-Free Numbers and provide routing reference information in the SMS/800 Toll-Free Number Registry.

**TN-based caller identity:** The originating phone number included in call signaling used to identify the caller for call screening purposes. In some cases this may be the Calling Line Identification or Public User Identity. For the purposes of this study, the caller identity may be set to an identity other than the caller's Calling Line Identification or Public User Identity.

## *3.2 Acronyms & Abbreviations*

| | |
|---|---|
| ATIS | Alliance for Telecommunications Industry Solutions |

| | |
|---|---|
| CSCF | Call session control function |
| FQDN | Fully qualified domain name |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| NNI | Network-to-network interface |
| MGCF | Media gateway control function |
| SBC | Session border controller |
| SGW | Signaling gateway |
| SP | Service provider |
| STI-AS | Secure Telephone Identity Authentication Service |
| STI-CA | Secure Telephone Identity Certification Authority |
| STI-VS | Secure Telephone Identity Verification Service |
| TLS | Transport Layer Security |
| TN | Telephone number |
| UA | User agent |
| UNI | User-to-network interface |
| VASP | Value-added service provider |
| VoIP | Voice over IP |

# 4 Architecture

## *4.1 SHAKEN Reference Architecture*

The figure below shows the SHAKEN reference architecture. This is a logical view of the architecture and doesn't mandate any particular deployment and/or implementation. For reference, this architecture is specifically based on the 3GPP IMS architecture with an IMS application server, and is only provided as an example to set the context for the functionality described in this document. The diagram shows the two IMS instances that comprise the IMS half-call model; an originating IMS network hosted by Service Provider A, and a terminating IMS network hosted by Service Provider B.

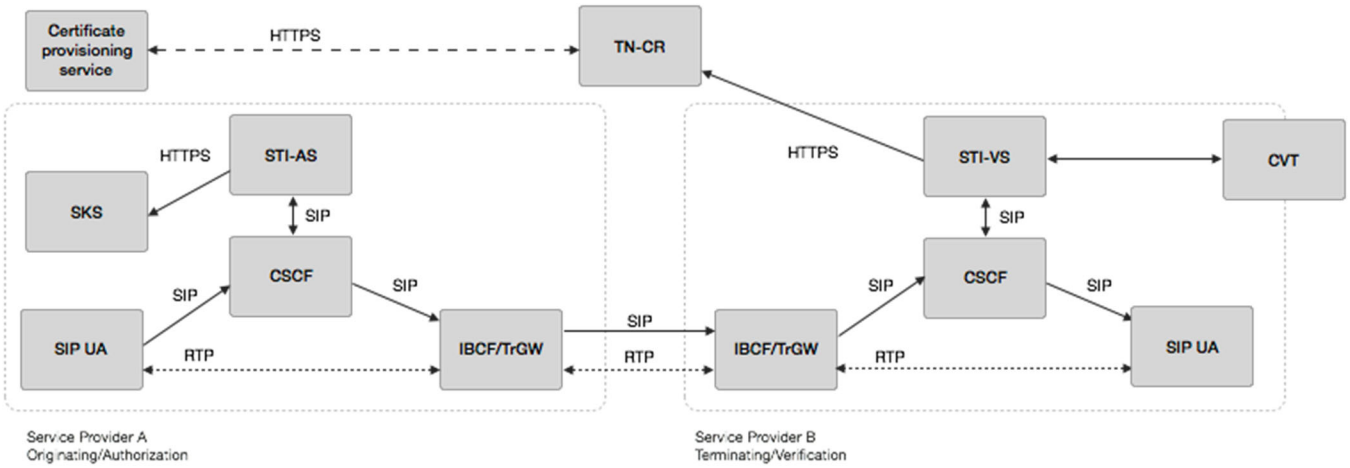


**Figure 4-1: SHAKEN Reference Architecture**

This SHAKEN reference architecture includes the following elements:

- SIP UA – The SIP User Agent that is authenticated by the service provider network and the calling party identity is known since it is under direct management by the telephone service provider. It initiates the SIP INVITE as the calling party.
- IMS/CSCF - This component represents the SIP registrar and routing function. It also has a SIP application server interface.
- IBCF/TrGW - This function is at the edge of the service provider network and represents the Network-to-Network Interface (NNI) or peering interconnection point between telephone service providers. It is the ingress and egress point for SIP calls between providers.
- Authentication Service (STI-AS) - The SIP application server that performs the function of the authentication service defined in RFC 8224 [Ref 10]. It should either itself be highly secured and contain the Secure Key Store (SKS) of secret private key(s) or have an authenticated, Transport Layer Security (TLS)-encrypted interface to the SKS which stores the secret private key(s) used to create PASSporT signatures.
- Verification Service (STI-VS) - The SIP application server that performs the function of the verification service defined in RFC 8224 [Ref 10]. It has an HTTPS interface to the Telephone Number Certificate Repository that is referenced in the Identity header field to retrieve the provider public key certificate
- Call Validation Treatment (CVT) - This is a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified and then providing a response to signal the display response for the end user.
- SKS – The Secure Key Store is a logical highly secure element that stores secret private key(s) for the authentication service (STI-AS) to access.
- Certificate Provisioning Service – A logical service used to provision certificate(s) used for STI.
- Telephone Number Certificate Repository (TN-CR): This represents the publicly accessible store for public key certificates. This should be an HTTPS web service that can be validated back to the owner of the public key certificate.

# 5 SHAKEN Security Services and Attestation

The SHAKEN Identity header provides certain security services for call signaling information between an originating service provider (originating SP) and a terminating service provider (terminating SP) in the VoIP-based service provider network. It authenticates the originating service provider identity to the terminating service provider and it protects the integrity of call parameters populated by the originating SP. These

services correspond to the authentication and integrity security dimensions as described in X.811 [Ref 3] and X.815 [Ref 4]. It is intended that the Identity header is populated via an STI-AS function by the first SP to receive the call in the VoIP-enabled SP network, a point in the VoIP-based SP network as close as possible to the ultimate source of the call, and is transmitted unchanged across any NNI and intermediate SP networks so that it can be verified by the terminating SP in its STI-VS function. The originating/signing SP identity, in the form of a Service Provider Code (SPC) is contained in the PKI certificate associated with the public/private key pair the SP uses to create the cryptographic signature in the Identity header (the originating SP is the "principal" as that term is defined in X.811 [Ref 3] for the SHAKEN signing/verification transaction). The certificate can be validated against root STI-CA certificates shared within a common governance and trust domain per ATIS-1000080 [Ref 2]. The signature also protects the integrity of the call parameters, including calling and called number, timestamp, "attestation indicator," and "origination identifier." The SP-level identity and authentication and call parameter integrity services support other security dimensions such as non-repudiation as defined in X.800 [Ref 6]. In the SHAKEN model, the Identity header protects this information across the NNIs through the SP networks but assuring the correctness of the parameters relies on other mechanisms and procedures the originating SP typically applies at the user-to-network interface (UNI) as described below.

## *5.1 Attestation Indicator*

The SHAKEN Identity header does not convey a customer identity or end-user identity other than calling TN which may or may not uniquely identify the customer or end-user, nor does it convey authentication credentials for the customer entity that originated the call into the VoIP-based SP network. Instead, it contains an "attestation indicator" (the "attest" claim) which encodes the extent to which the originating SP has itself identified and authenticated its customer and determined the customer's "association" to the calling party telephone number. The initial set of attestation values are "A," "B," or "C" defined as follows (as excerpted from ATIS-1000074-E [Ref 1], Clause 5.2.3):

**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.

…

**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.

…

**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).

…

In terms of security services, the process of determining an attestation level equates to the application of UNI "identity," "authentication," and "access control" security services. The primary UNI "identity" is a user identity indicating the customer and not necessarily tied to the calling TN. The UNI "authentication" service refers to authenticating the customer/user, again potentially irrespective of calling TN. Note that this UNI service is different from the SHAKEN "authentication" service (STI-AS) which generates the Identity header for propagation across the NNI. "Access control" in this instance pertains to determining whether the customer, once identified and authenticated, is authorized to utilize the calling TN (that is, the customer has a "verified association" to the TN as described in the attestation level definitions). A call that passes all three of these security services may be marked with the highest level of attestation ("A"), and a call that does not pass one or more of these should be passed with a reduced attestation level. Once the terminating SP's "verification" function (STI-VS) has verified the integrity of the Identity header through the received signature, the terminating SP network can use the received attestation indicator to make decisions about the validity of the calling TN for further analytics, call processing decisions, and conveying information to terminating user agents.

## *5.2 UNI Model*

In the VoIP-based service provider network, calls are placed to originating SPs and received from terminating SPs over a signaling and media path that constitutes a UNI. The reference model (Clause 4.1, above) covers one use case where the UA initiating the call at the UNI is under "direct management" of the originating SP. More generally, the initiating UA that signals the call to the originating SP is typically in the possession of or under the control of a "customer," which is typically an entity that has a direct commercial relationship with the originating SP and may or may not be the ultimate source of the call (the end-user entity). In addition to individuals or enterprises that can be considered both customers and direct end users of the originating SP's service, other types of customers include communications resellers and value-added service providers (VASPs) that bundle communications capabilities with other services and provide those services to other entities. Resellers accept calls sourced from other parties (indirect end users) and relay them into the VoIP-based SP network via their own UNI. A VASP may relay calls similar to a reseller or may itself originate calls from a call center or automated function on behalf of one or more of the VASP's own clients who in that specific use case are not direct customers of the originating SP. For the purposes of this report, the "UNI" will refer to the interface between the customer networks or devices and the originating SP network and not any upstream interfaces between the customer and any indirect end users that may be the ultimate source of calls received by the originating SP. This is a further disaggregation of the UNI security model presented; for example, in ATIS-1000030 [Ref 7] that considers the end user as synonymous with the subscriber or customer entity. Note that there is a separate class of call flows where the "originating SP" for the purposes of SHAKEN Identity header population receives a call over an NNI from another service provider. This is discussed in Clause 5.3.

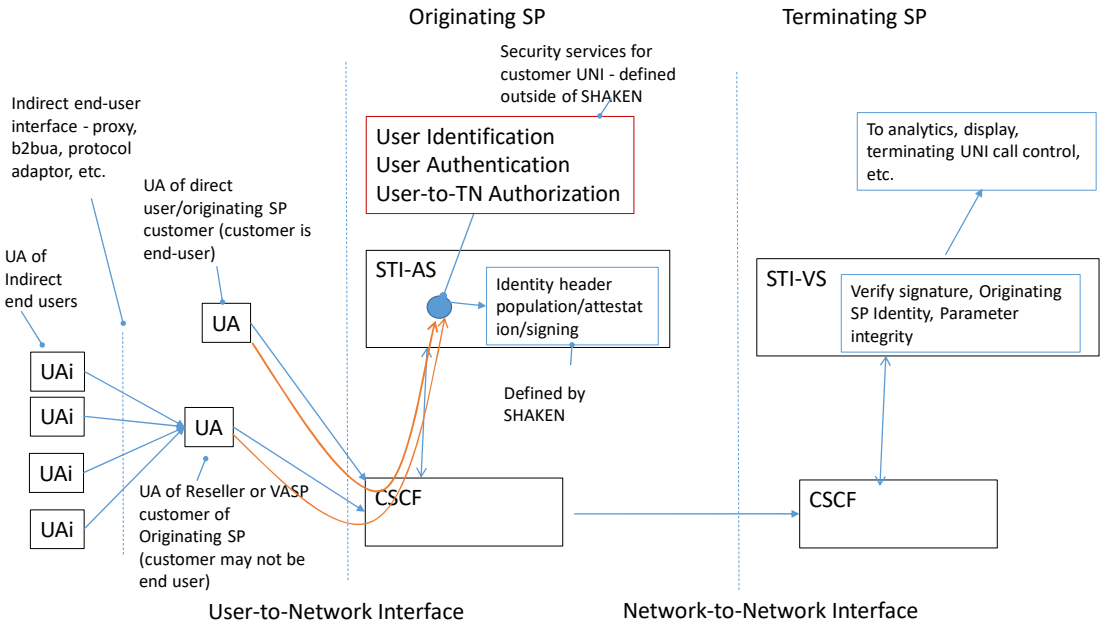


**Figure 5-1: User-to-Network Interface in context of SHAKEN**

### 5.2.1 Customer Identity

The primary user identity associated with a UNI is a "customer identity" used to determine the commercially responsible party for consumption of the service (the customer is the "principal" for UNI authentication and other security policy application as that term is defined in X.811 [Ref 3]). In limited cases an originating SP may rely on a TN-based identity for this purpose. In many cases a TN does not unambiguously identity the customer, making it an insufficient identifier for UNI authentication and authorization procedures. Other forms of user identity include account names or IDs, equipment identifiers (e.g., mobile IMSI, Private User Identity or IMEI), physical connections or IP network addresses. One or more forms of user identity are inputs to an authentication process to verify the customer and in some cases to an authorization process to determine what services the customer is entitled to.

In the ideal case the originating SP establishes the real-world identity of the customer by personal name, business name, e-mail and physical home or business address, tax ID or other government-conferred identifiers, payment accounts and credit history, etc. This allows the SP to track the responsible party for placing or receiving calls for commercial purposes, policy enforcement and other legal purposes. The real-world customer identity is typically associated with user names, customer equipment IDs, and/or other identifiers used in protocols and procedures at the UNI. There are some use cases (e.g., see A.1.2, below) where the originating SP may not strongly determine the real-world identity of the customer. That reduces the value of a customer identity for assigning policy characteristics and tracking responsibility for service usage to particular entities.

As noted in Clause 5.2 and in some of the use cases described in Annex A, in a number of cases the end user is not the same entity as the "customer," so the customer identity is not directly tied to the end user. In these cases an end user identity is not needed for UNI authentication procedures (only the originating SP's customer needs to be identified as the principal gaining access to the SP's resources). As might be required in certain attestation scenarios, there may be a need for the SP to establish (directly or indirectly

through the customer) that the customer UNI is servicing a particular end user entity for TN authorization purposes.

### 5.2.2 TN-based Caller Identity

The caller identity used across the NNI in general and in the SHAKEN Identity header specifically is a calling party TN in the form of a national or international E.164 number. While customer IDs other than TN may be used for authentication and authorization decisions at the UNI, non-TN identities are not typically delivered across the NNI or used directly in transit or terminating network processing (a "calling name" may be added by the terminating network using a database lookup against the calling TN received via the NNI). An origid claim sent in the Identity header may or may not be associated with individual customers (see discussion in Clause 6, below), but the parameter is also intended to be an opaque value not specifically conveying identity.

A TN-based identity may be tied to other types of user identities that an originating SP utilizes to determine the source of the call for commercial purposes (customer identity information). In the simplest cases there is a one-to-one correspondence between a TN-based identity and a customer account ID so that either may be used by the originating SP for authentication, identification, and authorization purposes. In many cases there is not a one-to-one correspondence and the service provider will likely use an identity other than the TN to identify the customer at the UNI. This is particularly true where the customer and end user are different entities and/or where the customer UNI presents calls from multiple calling TNs. A few possible scenarios for the use of TN-based caller identity at the UNI are included in Annex A, below.

### 5.2.3 User Authentication

Once a VoIP communications service customer has been identified, authentication is the means of verifying that they are the authorized entity to be using UNI resources and that the entity is responsible for the commercial and policy terms of placing or receiving calls to and from the SP network. User authentication can take a number of forms including transactions via equipment-resident or user-provided credentials, network location, and/or protected network paths. Some of these are described in Annex A, below.

### 5.2.4 TN Authorization and Screening

For the purposes of SHAKEN attestation, once an originating SP has identified and authenticated the customer, the originating SP network determines whether a customer is authorized to utilize a calling TN (described in SHAKEN as the customer's "association" with the TN). Authorizing and determining the authorization of a customer to utilize a TN resource are parts of the "access control" security dimension as described in X.812 [Ref 5] along with other authorizations to use the VoIP service itself. Authorizing the use of a TN with a service is largely an administrative process before the handling of the call, for instance by populating a subscriber record or populating a database for affirmative control of TNs, or by recording customer agreement to terms of use. If the originating SP network can determine that the customer is authorized to use a customer-asserted TN then it would presumably mark an "A" attestation in the Identity payload. Where it cannot determine the authorization it would mark a "B" attestation. One possible implementation would be for the originating SP and customer to agree that calling TNs will be "screened," and any calls with TNs not explicitly authorized will be rejected. Only authorized calling TNs would be passed, including an "A" marking. Some possible means of determining authorization under different usage scenarios are described in Annex A, below.

## *5.3 Identity Header Population and Attestation for Calls Received at a Network-to-Network Interface*

Within a common governance and trust domain (e.g., U.S. service providers), the end goal of SHAKEN mechanism deployment is for all calls transiting the VoIP-based service provider network to be marked with

an Identity header containing call parameters (SHAKEN claims) populated based on information determined directly at the customer's UNI where they first enter the trust domain. Once the Identity header is created by the originating SP, it is to be passed across any downstream NNIs without modification. Calls may still arrive at an NNI without an Identity header for a number of reasons, and therefore the receiving gateway or intermediate SP might assume the role of "originating SP" for the purposes of SHAKEN call processing. This would result in the gateway/intermediate SP populating an Identity header using information they can determine across the NNI and signing it with its own credentials. The main use case for SHAKEN "authentication" for calls received at an NNI is an international gateway provider, where calls are received from entities outside the trust and governance domain, and therefore the source's identity and adherence to the receiving SP's country or regional policies may not be determined. Likewise, the SP populating the Identity header is not expected to have any knowledge of the identity, authenticity or authorization to use calling TNs of any customers homed on the interconnecting gateway SP's network or other interconnecting parties behind that SP's network. Any Identity header received at a gateway may not be verifiable (in the future, inter-governance-authority agreements and administration mechanisms may make this possible). A signature with the gateway provider's credentials allows for traceability to a call's entry point into the trust domain. The gateway provider should not populate attestation values (A or B) that rely on UNI security services that cannot be applied at the NNI.

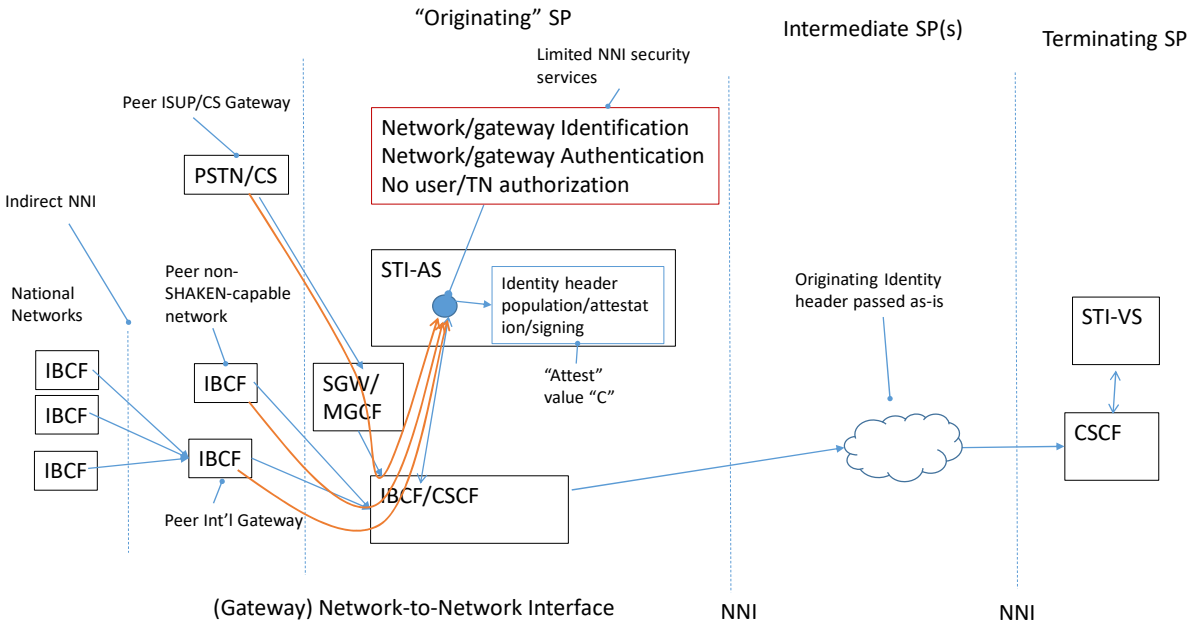


**Figure 5-2: Network-to-Network Interface in context of SHAKEN**

Another reason that a call might arrive at an NNI without an Identity header is that the NNI uses a non-SIP protocol (e.g., TDM/ISUP), so that capability is not available even if the carrier originating the TDM call leg is or could be covered under the governance and trust domain. The first SP that transits the call across a VoIP NNI may populate an Identity header using its own credentials, and as with the international gateway scenario it should not populate attestation values A or B that rely on UNI security services.

Especially during a transition phase where SHAKEN functions are not deployed in a substantial percentage of SP networks, it may be of some limited value for an intermediate SP to add an Identity header using its own credentials, to provide traceability to itself where it can provide information regarding an upstream SP. There is probably limited additional value for an intermediate provider to add an Identity header if one is present (created within the trust domain), and doing so may make it harder to determine at the verification

function which header has the more authoritative information about the call parameters. As with the other NNI-origination use cases, the intermediate provider should not itself mark A or B attestation values.

## *5.4 Guidelines*

### 5.4.1 Full Attestation

In order to mark a call with an Identity header containing the "full attestation" attest claim value ("A"), all the previously discussed UNI security services should be applied and passed. As a result, the following conditions should apply:

- The originating SP administrative functions should determine the real-world identity of the customer.
- The originating SP network should receive the call through an interface constituting a UNI.
- The customer should present its identity across the UNI interface as necessary for authentication purposes.
- The originating SP UNI security function should authenticate the customer's identity through an authentication transaction, protected network path, or other means.
- The originating SP UNI security function should apply an access control procedure and determine that the customer is authorized to utilize the calling TN, or the originating SP should itself populate a known authorized calling TN.

Per SIP procedures, any calling TN populated by the originating SP should be passed in the SIP P-Asserted-Identity header, and that value will also be populated as the "orig" claim value of the SHAKEN PASSPorT token of the Identity header.

Note that the "customer" refers to the direct customer of the originating SP. Where the originating SP has assigned the calling TN or the customer has provided evidence that it has authorization to use the calling TN itself, the originating SP can mark an "A" attestation without reference to authorizations of any indirect end users (e.g., in a reseller or VASP scenario). In some other scenarios the TN assignments and/or authorizations apply to the indirect end user or call-initiation functions executed on behalf of the reseller's or VASP's own customer. In those cases the SP's customer should provide assurances that they can trace the identity of an indirect end user and that user's authorization to utilize a calling TN. The customer should be able to certify that only the authorized party (or calls originated on their behalf) will use the particular set of authorized TNs, and any traceback to the ultimate source will rely on the cooperation of the SP's customer.

### 5.4.2 Partial Attestation

In order to mark a call with an Identity header containing the "partial attestation" attest claim value ("B"), at a minimum the customer identity and authentication services should have been applied to the call. As a result, the following conditions should apply:

- The originating SP administrative functions should determine the real-world identity of the customer.
- The originating SP network should receive the call through an interface constituting a UNI.
- The customer should present its identity across the UNI interface as necessary for authentication purposes.
- The originating SP UNI security function should authenticate the customer's identity through an authentication transaction, protected network path or other means.
- The originating SP UNI security function has not determined the customers authorization to utilize a calling TN, or it has applied an access control procedure and could not determine the customer's authorization to use the presented calling TN.

### 5.4.3 Gateway Attestation

An “originating SP” for the purposes of SHAKEN “authentication” processing should mark a call with an Identity header containing the “gateway attestation” attest claim value (“C”) under the following circumstances:

- An SP (international gateway SP, intermediate SP) populating an Identity header for a call received through an NNI should mark the call with “gateway attestation.” Presumably this will be done only when an Identity header has not been received at the NNI and/or the interconnecting SP or other entity is outside the trust domain.
- An originating SP populating an Identity header for a call received through a UNI interface should populate “gateway attestation” when it is unable to identify and authenticate the customer initiating the call. Note that in most cases there should be an identifiable customer utilizing a UNI interface. The gateway marking may be used, for instance, if the real-world identity of the customer is not sufficiently determined.

### 5.4.4 Other Attestation Values

In the future, additional attestation indicator values may be defined to take into account different security dimensions or levels of granularity.

# 6 Origination Identifier

Per ATIS-1000074-E [Ref 1] Clause 5.4.2, the SHAKEN PASSporT contains a unique origination identifier (“origid”) consisting of a globally unique string corresponding to a UUID (RFC 4122).

The purpose of the unique origination identifier is to assign 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 trace back identification of customers or gateways.

## *6.1 Origid Granularity*

As an opaque identifier, the origid claim does not convey any SP or customer information in and of itself barring the sharing of origid decoding lists among SPs (not currently envisioned). It may be used in the originating SP network logging and call detail records to aid local traceback searches, and a terminating SP may include the value in traceback requests to support originating SP tracing of calls to a portion of the originating network, to a customer, and/or to a UNI or NNI. The origid may also be used to signal traffic that can be correlated by terminating SP analytics, and therefore the value should be a persistent and/or permanent value to allow such remote correlation over time to expose common sources of traffic.

For the originating SP’s own purposes, the aggregation of calls by origid at any granularity (e.g., access or core network instance, region, customer, peer node, etc.) could be sufficient to support location of the origination source within its own network, for instance in response to a traceback request. However, for the terminating SP it may be useful to receive origids populated at one of the finer levels of granularity (customer/SP or peer node) for reputation scoring and traffic-source disambiguation purposes. This is particularly the case where there is not a one-to-one correspondence between the individual calling TNs and the traffic source and/or the originating SP does not exercise control over the TN marking so that the TN itself is not a unique and unambiguous indication of the source of the call. Therefore, the calling scenarios where it might be appropriate to mark calls with a network- or network-component-level of granularity are those where the access and/or core network exercise control over the customer UAs and/or the TNs marked on the call, and particularly when a given UA is associated with only one or a small number of TNs so that an origid at the customer granularity does not add information (assuming the terminating SP has some way of recognizing this is the case). For calling sources where the originating SP network itself

does not exercise control over the calling TNs and a given customer or SP interface presents many calling TNs, then origid at the customer or peer SP granularity or finer is important for the terminating SP to recognize calls attributable to a given source, despite being marked with different TNs. This is likely the case for calls received at an NNI and also for calls received at a UNI from a reseller, VASP, or any enterprise calling source serving more than a few individuals.

Where a particular part of the originating SP's network handles traffic from both kinds of sources (controlled UAs with limited TNs and non-SP-controlled UAs with larger numbers of calling TNs), an originating SP may choose to use the finer granularity for all types of traffic. Over time, origid values populated at the granularity of individual customers for personal or small business service, when combined with calling patterns, could reveal information to other SPs and parties in the SHAKEN ecosystem regarding customer identity, personal relationships and/or business relationships that may not be obvious from calling/called numbers alone. The industry should consider whether or not this may raise privacy issues. One possible solution to this might be to use a persistent, but not permanently assigned origid value.

There are possibly no such privacy issues for resellers, VASPs, and possibly larger enterprise customers with more diverse calling patterns and service usage. Private information leakage regarding individual customers should also not be an issue with international gateway or other NNI-originated calls marked at a peer or interconnecting SP level of granularity. Where a given SP marks calls with origids assigned at different levels of granularity (e.g., customer, peer, gateway, region, etc.) and for different purposes, it is unclear how these purposes would be sorted out by analytics in the terminating SP network to know the appropriate handling of calls correlated to a given origid. The terminating SP may need to determine this autonomously or obtain guidance from each originating SP.

## *6.2 Guidelines*

### 6.2.1 Origid for calls received via an NNI

The following guideline applies for population of origid for calls received at an NNI:

- An SP populating an Identity header for calls received across an NNI should populate a persistent and/or permanently assigned origid claim value at the granularity of per peer SP or per peer NNI.

### 6.2.2 Origid for calls received via a UNI

The following guidelines apply for calls received at a UNI:

- For customers or customer groups where an originating SP directly assigns, populates, or otherwise exercises control over the calling TNs associated with calls received across the customers' UNIs, the originating SP may populate the Identity header origid value at a granularity other than on a per-customer or per-UNI basis, as may be useful for traceback purposes within the SP's own network.

Note: SP "control" of calling TNs may be via policy/terms of use, administrative, or per-call authorization checks and is not limited to TNs directly assigned by the SP.

- For customers or customer groups where an originating SP does not exercise control over the calling TNs populated at the UNI, the originating SP should populate the Identity header origid value at a per-customer or per-UNI granularity.

Note: The SP may be expected to mark a call with "B" attestation or lower if it does not exercise control over the population of calling TNs on a given customer UNI.

- The origid value should be a persistent and/or permanently assigned value at the selected source granularity. Where origid is populated at the granularity of a customer or UNI that may be associated with an individual person, such as for a residential or small business service, the originating SP should consider the use of an origid value that is not permanently associated with the customer or UNI in case a permanent value may expose additional private information.

# 7 Conclusions

The SHAKEN standard protects information exchanged between an originating and terminating SP over one or more direct or intermediate NNIs. The attestation claim encodes the originating SP's knowledge of the SP's customer or other SP traffic source. The validity of these markings relies on security services and security administration procedures applied by the originating SP and in some cases the SP's customer if the customer is not the same entity as the end user. The origid claim for each call should be populated at a granularity that both supports traffic source identification and traceback within the originating SP's network and to aid the terminating/verifying SP in correlating traffic from common sources when that correlation might be of use for analytical purposes. Best practices for the application of UNI security services in support of SHAKEN attestation are expected to evolve as the industry gains experience with the use of the SHAKEN framework.

# 8 Annex A: Use case examples for UNI Identity, Authentication, and Authorization in relation to SP use of SHAKEN (Informative)

There are many possible use cases of UNI security services as inputs to SHAKEN processing. These should be thought of both in the management plane and in the transport and call processing planes. The process begins with establishing the customer real-world identity at on-boarding time and negotiating terms of use, establishing UNI authentication credentials and securing network paths, and establishing and maintaining TN authorization. In the service plane, it consists of authentication of the customer and determining TN authorization for each call to the extent that is part of the calling scenario. The process continues with monitoring of customer/TN usage patterns to enforce policy.

The scenarios are different, among other dimensions, based on whether the customer is the direct end user or the end user is behind a customer proxy/b2bua, which entity is assigned a TN, and whether or not the originating SP assigned the TN, and some of the scenarios present challenges to the SP being able to apply one or more of the necessary security services to achieve a higher level of attestation. The following is a discussion of some possible use cases for UNI security services in relation to determining an attestation value.

## *A.1 Customer and TN identity use cases:*

### *A.1.1 Direct Individual Assignment*

As part of establishing a new account, such as a landline VoIP or mobile account, an SP may directly assign a TN to the account for the customer's use in placing and receiving calls. A TN can also be ported from another service provider and likewise be used to identify the individual user account. With typical post-paid service to individuals the account is more tightly associated to a particular real-world user (e.g., by postal address and credit checks) to assure payment after consumption of the service. In many of these cases a TN-based identity can be used interchangeably with other forms of user identity.

### *A.1.2 Prepaid Account*

In a prepaid mobile account, a TN is tied to an account and a prepaid mobile phone or SIM. The account is associated to the customer entity, who might be assumed to be an individual end user of the service, through a registration process. While the TN and prepaid account are strongly associated, the association to individually identified real-world users may be looser than for post-paid accounts since the associated charges are collected in advance.

### *A.1.3 Enterprise*

An SP may directly assign or port TNs to an enterprise as they would for an individual account, and the TNs are used with the SP's service. Enterprise customers may utilize multiple SPs to originate calls, and they may mark calls with a TN (such as a main business number) across all their providers regardless of which SP assigned the TN. An enterprise may mark calls with a Toll-Free number acquired from a Toll-Free RespOrg (Responsible Organization), which may or may not be the originating SP. In cases where an enterprise customer utilizes multiple calling TNs possibly from different SP or RespOrg TN providers, an originating SP may choose to utilize other customer identifiers to determine the source of the call instead of relying on TNs that they did not assign. In many cases, any SP accepting calls originated from the enterprise will have business contact, location, and credit information for the enterprise so they can strongly identify the real-world user entity. One possible way to determine the real-world identity of an enterprise or other organization entity is to apply methods similar to certification authority "extended validation" as used in the process for issuing web server X.509 certificates [Ref 9]. The EV process is a methodology to "identify the legal entity that controls a Web site" [Ref 9, Clause 2.1.1] and to use that information to establish web server credentials. In some cases enterprise services may be offered on a prepaid basis with lesser

customer identity and credit verification requirements, and as such a weaker link to a real-world business or organization identity.

### *A.1.4 Communications Reseller*

A communications reseller may interact with TN-based identities in various ways. The reseller may receive direct TN assignments from an SP, port previously assigned TNs to an SP, or acquire Toll-Free TNs from an SP (acting as a RespOrg), and then they may resell use of these TNs to individual or enterprise end-user entities in association with the communications services originated through the assigning SP. They may also provide service on a "bring-your-own-number" basis where the end user has received assignments from other SPs or RespOrgs. The reseller may originate either of these types of numbers through multiple service providers, not just one who made an original TN assignment. In most reseller use cases, an originating SP does not know the identity of the ultimate end users and only identifies and authenticates the reseller customer. Identification of end users relies on the communications reseller to make any such determination, and further layers of indirection might obscure the ultimate source. The originating SP may determine the real-world identity of the reseller itself using extended validation methods as mentioned in A.1.3 or other means of determining real-world business information.

### *A.1.5 Value-Added Service Provider (VASP)*

Some entities provide communications services ancillary to other services; for example a doctor's office patient management platform with voice contact features. As with communications resellers, a value-added provider may arrange for TN assignments from an SP or Toll-Free RespOrg for use by a particular VASP customer or for use by the VASP's platform generally irrespective of customer, or customers may bring their own TN assignments and delegate their use to the VASP to originate calls on the end customer's behalf. An end customer may utilize the same calling TN through their own direct services and for calls a VASP originates on their behalf. TNs assigned to either the VASP or the end-user entity may be used through different originating SPs. As with reseller scenarios, the originating SP typically knows the VASP customer and does not have direct knowledge of users of VASP call centers or platforms. Any determination of the identity of end-users and their TN authorizations would need to be traced through the VASP. The originating SP can determine the real-world identity of the VASP via extended validation-type methods or other means.

## *A.2 User/Customer Authentication*

### *A.2.1 Device*

In device-based authentication, the user identity and permanent cryptographic credentials are stored on the device and used in an authentication transaction with the network. For instance, in 3G/4G mobile networks an IMSI identity and authentication keys are stored on a SIM card, and these may be tied through registration to the mobile phone's hardcoded ID (IMEI) and an associated TN (MSISDN). Access to the credentials for use in an authentication transaction may require further unlocking codes or other factors.

### *A.2.2 Account*

Devices and software that do not have permanent credential storage often use an account ID and credentials (e.g., passwords, pre-shared keys, private keys/certificates) that are manually entered by a user or populated through administrative procedures. For instance, a communications app may require an e-mail-address-based identity and user-entered or cached password credentials. A customer softswitch or SBC may authenticate at the transport layer (e.g., TLS), for instance using a customer FQDN or wildcard domain name in a PKI client certificate and stored private key. Barring other factors applied to the authentication process the account credentials may be moved between physical devices or software instances or re-entered in different apps or browser windows to gain access to the service.

### *A.2.3 Network*

Where the originating SP controls the customer connection point such as in a broadband access network or where customer equipment such as an enterprise PBX or reseller platform has a fixed network IP

address, the originating SP may rely on physical interface or IP address to authenticate the customer over the UNI. The customer and originating SP may also set up protected network-layer tunnels (e.g., IPsec) between their networks to exclude traffic received outside the tunnels. These physical or network location characteristics may be a sole factor for authenticating a customer or it may be a second factor combined with device-stored credentials or other primary forms of authentication.

## *A.3 Calling TN Authorization and Screening*

### *A.3.1 SP Marking*

An originating SP can determine the account ID and authenticate the customer and then mark or re-mark the call with a specific calling TN it has assigned to the customer. This is possible when there is a one-to-one correspondence between customer account and TN.

### *A.3.2 Direct Assignment*

The originating SP may directly assign TNs to a customer and allow the customer to mark calls at the UNI with those TNs and receive an “A” marking. Any other TNs would receive a “B” marking unless authorization was determined through some other means.

### *A.3.3 Toll-free TN Assignment*

Toll-free TNs are acquired by a RespOrg from a central database and assigned to terminating users, or to TN or service resellers that may delegate their use to end users. The RespOrg also configures how the TNs are to route from originating access networks when called as a destination TN. While the primary purpose of a toll-free TN is for use as a destination number, the toll-free TN user may also mark outgoing calls with the toll-free TN as the calling TN. The RespOrg, which may be an SP, the TN user or a third-party entity, is the authoritative source of toll-free TN assignment information and therefore the RespOrg serves an equivalent role to an SP that assigns a geographic TN for the purpose of determining the authorized assignee or user of the toll-free TN. An originating SP that is not also the RespOrg for the (toll-free) calling TN may use means similar to those used for geographic TNs to determine the RespOrg has authorized a toll-free TN’s use by the originating SP’s customer.

### *A.3.4 Contract Relationship*

The customer and originating SP may have contract terms that state the customer will only mark calls with authorized TNs. In this case there may be no explicit per-TN authorization step in the originating SP but misuse would be enforced under contract terms of use.

### *A.3.5 Letter of Authorization (LOA)*

A possible way to establish authorization would be for an SP that assigns TNs to provide some form of a “letter of authorization” (LOA) to the customer (e.g., an enterprise customer, reseller or value-added service provider) that the customer can present to other SPs it uses to originate calls. The LOA will presumably contain the assigning SP identity, customer identity that can be verified by the receiving SP (e.g., company name, address, and other verifiable characteristics) and a list of TNs the authorizing SP assigned or in-ported to its network. The receiving SP can, for example, add these TNs to an authorization database and use the list to drive an “A” marking for calls containing TNs in the list. Any such LOA would need to be periodically verified to determine that the TNs are still validly associated to the customer from the assigning SP, and if such a process is implemented with any volume of TNs there should be automated mechanisms to exchange LOA documents and re-verify TN assignments.

### *A.3.6 Independent Authorization Check*

A possible method for an originating service provider to independently verify the customer’s authorization to use a TN is by proving that the customer requesting authorization can use the TN, such as by calling the TN and giving a verbal code that the customer will be challenged to replay to the originating SP, or by sending a code in an SMS message. These methods would be most applicable in cases where the TN is used for a person-to-person service, terminating to an individual user.

### *A.3.7 Indirect Authorization*

In a number of reseller/VASP scenarios the TN assignee will not be the customer with a direct relationship to the originating SP. The reseller/VASP may come up with a means to determine the TNs the end-user customer is assigned and then relay a request for originating SPs to accept those TNs from its UNI to receive "A" marking. The originating SP will likely not know the identity of the end user and would need to rely on enforcement of contract terms with the reseller or VASP.

### *A.3.8 No Validation*

An originating SP may not have a process to determine authorization for customers to use TNs through a UNI. Presumably such an originating SP will always mark calls with a "B" attestation if the customer is known and authenticated or possibly "C" if the real-world identity of a customer is ambiguous. SPs may find, however, that customers will request that their traffic receives "full attestation" whether the customer is an individual, enterprise, reseller, etc. and under many legitimate use cases for calling number TN marking. The service quality need may drive SPs to initiate an authorization process where they are not currently doing so today.

## *A.4 Example Use Case Matrix*

A way to represent the scenarios is a matrix of the customer and end-user type, UNI or NNI security services applied, and a possible SHAKEN attestation result. Table A-1 provides some examples.

**Table A-1: Example use cases for application of UNI/NNI security services and attestation**

| End user | Customer/ Inter-connecting entity | TN assigned to | TN assigned by | Identity established by | Authentication type | Authorization established by | Attestation result |
|---|---|---|---|---|---|---|---|
| Mobile subscriber | Same as end user | Subscriber | Originating SP | Customer name/address/credit checks | Device | Direct assignment | A |
| Enterprise PBX | Same as end user | Enterprise customer | Other SP | Customer name/address/credit checks | Customer ID/pre-shared key, IP network ACL | Letter of Authorization | A |
| Individual or enterprise | VASP | VASP | Originating SP | Customer name/address/credit checks, end-user traced through customer | Customer ID/IP network ACL | Direct assignment, terms of use (customer responsible for end user's use of TNs) | A |
| Non-domestic entity | Gateway provider | End user | Non-domestic provider/not determined | Not determined (gateway provider not the originating SP) | Network interconnection | Not determined | C |
| Individual or enterprise | Reseller | End user | Other SP | Customer name/address/credit checks, end-user traced through customer | Network interconnection | Terms of use | A or B based on terms enforcement |