**Contribution**

**TITLE:** Whitepaper on the Relationship of User-to-Network-Interface (UNI) Identity, Authentication, and Authorization to the STIR/SHAKEN Environment

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

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

**ABSTRACT**

To implement SHAKEN procedures in the VoIP-based service provider network, and in particular to implement an “attestation” procedure, service providers must rely on security services implemented at the user-to-network interface to identify valid customers and confirm their authority to utilize calling TNs. This whitepaper offers a possible framework for considering security services for various usage scenarios at the user-to-network interface and how they will interact with SHAKEN procedures.

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

**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.

# Introduction

The SHAKEN framework (ATIS-1000074) is designed to provide certain security services between an originating service provider and a terminating service provider in a VoIP-based service provider network to cryptographically protect call information sent between these two entities. Outside the SHAKEN mechanisms themselves, it is implied that for some set of calls there will be a related procedure at the user-to-network interface (UNI) to identify and authenticate the originating service provider’s customer and to determine whether or not that customer has authorization to originate calls using a particular calling party telephone number (TN). The SHAKEN reference model presents a simple case of a user agent under direct administrative control of the originating service provider, which represents only one such use case. Service providers will typically identify and authenticate their customers to some degree. There are a number of cases where explicit TN authorization is not part of current processes for accepting calls into its network. Layers of indirection, use of calling TNs across multiple service providers, and “legitimate spoofing” scenarios add complexity to this process. It can be assumed that many if not most customers of VoIP-based service provider networks will wish for their calls to be passed with the highest quality and therefore the highest level of assurance as to the validity of the calling information sent through the VoIP-based service provider network. This whitepaper describes the use of the UNI security services of “identity,” “authentication,” and “authorization” as inputs to the SHAKEN “authentication” process, and a framework that service providers might use to evaluate their use of UNI security services.

# SHAKEN services

## SHAKEN “authentication”

SHAKEN defines signaling elements and procedures to protect call information being sent between service providers. The end-to-end reference model is based on in RFC 8224 Section 5 that defines an “authentication service” implemented in a “proxy” that performs both a user agent (UA) authentication and authorization procedure and an inter-proxy signaling procedure to forward cryptographically signed parameter further on in the network. An end-to-end UA-to-UA model also mentioned in RFC 8224 is not applicable to SIP Identity/SHAKEN use in service provider networks. In SHAKEN, the “proxy” function is embodied in the originating SP’s CSCF and STI-AS functions. RFC 8224 also presents the identity in any user authentication as being TN or SIP URI based using the calling number identity of an individual call. SHAKEN concerns itself with the “inter-proxy” signaling from the RFC 8224 model and does not address the UA identity, authentication and authorization portion of the procedure except for a simple use case presented in the reference model.

## Authentication of the originating service provider

The SHAKEN procedure provides a method for the terminating service provider (terminating SP) network to authenticate the identity of the originating service provider (originating SP). In the network-to-network interface (NNI) call signaling with SHAKEN, the originating SP network adds a header to the SIP INVITE known as the “Identity header” that contains protected call parameters and a public-key-cryptography signature. The Identity header is forwarded to the terminating SP directly or through intermediate network NNIs that preserve the header. The identity of the originating SP is not itself conveyed in each call. Instead, the header contains a URL pointer to a public key certificate, which in turn contains the identity of the signing provider in the form of a “service provider code.” The PKI root certificates that protect the signing certificate are distributed through a trusted framework and thus the terminating service provider can authenticate and identify the originating service provider by pulling (or caching) its signing certificate and validating the Identity header signature against the certificate public key (see RFC 8226, ATIS-1000080 for certificate format and management process). The originating service provider identity in the certificate and verification of the signature allows the terminating SP to trace the call back to its origin in the SP network.

## Integrity of calling party number and other call parameters from originating SP

Along with providing a means to authenticate the originating SP, the cryptographic signature in the identity header provides an integrity service to a set of protected parameters to assure that they have been received unchanged from the originating SP. The parameters include the calling party number, an “attestation indicator” (described below), the destination TN, a timestamp to protect against replay attacks, and an opaque “origination identifier” which may be used by the originating service provider to denote different types or sources of traffic. By providing integrity to the parameters, the terminating SP can be assured that the parameters were the same as those the originating SP either marked the call with itself or that it received from the upstream source (a customer or a service provider outside the particular SHAKEN governance and policy realm). The correctness of the parameters are the responsibility of the originating SP, and any issues with the call can be traced back to that SP based on the SP-level identity and authentication.

## Attestation indicator

The SHAKEN Identity header does not convey a customer identity (other than calling TN which may or may not uniquely identify the customer) or authentication credentials for the customer entity that originated the call into the VoIP-based SP network. Instead, it contains an indicator as to 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 indicators from “A” to “C” represent, roughly speaking, that both the customer and its association to the telephone number have been verified (“A” marking or “full attestation”), the customer has been verified but the association with the telephone number have not (“B” marking or partial attestation), or neither the customer nor an association with the telephone number have been verified (“C” marking or “gateway attestation”). Once the terminating SP’s “verification” function (STI-VS) has verified the integrity of the identity header through the received signature, it can make decisions about the validity of the calling TN for further analytics, call processing decisions, and conveying information to the terminating user agents.

# SHAKEN and UNI security services

## User-to-Network interface

In the VoIP-based service provider network, calls are place to originating SPs and received from terminating SPs over a signaling and media path that constitutes a “user-to-network interface” or UNI. The “customer” that signals the call to the originating service provider is typically the entity that has a direct commercial relationship with the originating SP and may or may not be the ultimate source of the call. In addition to individuals or enterprises that can be considered direct end users, other types of customers include communications resellers and value-added service providers that bundle communications capabilities with other services. These entities accept calls sourced from other parties and relay them into the VoIP-based telecommunications network via their own UNI, or they place calls as directed by the end user or through automated functions executed on their behalf.

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

## UNI identity, authentication, and authorization as the basis of “attestation”

For the purposes determining attestation in SHAKEN, the originating SP must determine the identity of the customer, authenticate the customer, and determine the customer’s association to the calling telephone number (that is, the customer’s “authorization” to utilize the telephone number). If the originating network cannot execute one or more of these steps or if it fails to make one or more of these determinations, then the attestation level on the call is expected to be reduced appropriately.

### User identity

The primary use of a “user identity” at the UNI is to determine the commercially responsible party for consumption of the service. In some cases an originating SP may rely on a TN-based identity for this purpose. In many cases a TN does not uniquely 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 or IMEI), physical connections or IP network addresses, and also real-world personal or business names, addresses and other non-service-related identifiers. One or more forms of user identity are inputs to an authentication process to verify the user and in some cases to an authorization process to determine what services the user is entitled to.

Customer 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 on the calling TN). SHAKEN defines an opaque “origination identifier” (origid) that is populated in the signing certificate and delivered as an Identity header parameter with each call for the purpose of supporting traceback and reputation determination for different traffic sources (device classes, nodes, gateways, etc.). Due to the overhead associated with creating and distributing different certificates for different origids it is expected that origid will be used for purposes of segregating traffic at a granularity other than individual customers.

### TN identity

The caller identity used across the NNI is a telephone number (TN) in the form of a national or international E.164 number. A TN-based identity may be tied to other types of user identities that an originating SP uses to determine the source of the call for commercial purposes. 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 on the UNI. A few possible scenarios for the use of TN-based identity at the UNI are as follows:

#### 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 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.

#### 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 users may be looser than for post-paid accounts since the associated charges are collected in advance.

#### 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 SPs 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. In such cases, 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 user entity. In some cases enterprise services may be offered on a prepaid basis with lesser user and credit verification requirements.

#### Communications reseller

A communications reseller may interact with TN-based identities in various ways. The reseller may receive direct TN assignments from an SP or port assigned numbers to a particular SP, 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. 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.

#### 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 for use of a particular VASP customer or for the platform generally irrespective of customer, or customers may bring their own TN assignments to the platform. TNs assigned to the VASP or the end-user entity may be used across originating SPs.

### User authentication

Once a VoIP communications service customer has been identified, authentication is the means of verifying that they are the correct entity to be using the service.

#### 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.

#### Account

Devices and software that do not have permanent credential storage often use an account ID and credentials (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.

#### 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.

### 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). The process of authorizing the use of a TN with a service can be thought of as an administrative process before the handling of the call, for instance to populate a database for affirmative control of TNs or to record 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 include the following:

#### 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.

#### 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.

#### 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.

#### Letter of Authorization (LOA)

A possible way to establish authorization would be for an SP that assigns TNs to give some form of a “letter of authorization” (LOA) to the customer (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 (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.

#### Independent authorization check

A possible method for an originating service provider to independently verify the customers 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.

#### 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.

#### No validation

An originating SP may not have a process to determine authorization for customers to use TNs. Presumably such an originating SP will always mark calls with a “B” attestation if the customer is known and authenticated or “C” if incoming traffic is intermingled from various sources, for example international gateway service to carriers in other countries. It is likely, however, that customers will request that their traffic receives “full attestation” whether the customer is an individual, enterprise, reseller, etc. and under all possible 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.

## UNI Identity, Authentication, and Authorization Challenges and Threats

Under any UNI security regime, there are challenges to assuring that the security mechanisms are sufficient to protect the use of the interface, and threats that need to be recognized and mitigated at some level, such as by strengthening the mechanisms, monitoring, and coordinating with other network parties. Some threats to UNI identity, authentication and authorization are as follows:

### Identity

**Spoofing** – Spoofing is the marking of a calling TN on individual calls other than ones associated with the customer’s service. Illegitimate spoofing may be done to either avoid identification or to take on the identity of another specific party. Affirmative controls on TNs used to originate calls should be able to stop spoofed calls or to down-mark the SHAKEN attestation. However, there are legitimate uses for spoofing, and any affirmative controls may stop or reduce the quality of allowable calls.

**Re-origination** – End-user entities may open their user equipment to access by other parties, hiding the ultimate source of the traffic.

**Identity ambiguity** – In certain reseller or VASP arrangements, TNs assigned by the originating SP may be used by the customer on a pooled basis or may otherwise not be traceable to individual end users. Service providers, resellers, or VASPs may not have sufficient information about their customers to verify their authorization or to hold them accountable for misuse.

### Authentication

**Account hijacking** –account credentials can be stolen and used to impersonate a customer or reseller/VASP end user.

**Device hijacking/credentials cloning** – devices may be stolen or hijacked by malware, or the credentials on a device may be cloned and used elsewhere by unauthorized parties.

**IP address spoofing/network-layer attacks** – Entities that can take control of network routing or execute man-in-the-middle attacks to inject traffic into the network may bypass network access lists to gain access to service.

### Authorization

**Weak authorization process** – Service providers or their reseller/VASP customers making authorization claims may not fully determine the customer or end-user authorization to utilize a TN.

**Unsupported claims/exceeding authorization** – Another aspect of spoofing, customers may assert authorization to TNs they are not entitled to use, or they may use TNs outside their authorization.

**No enforcement** – Service providers may not enforce the use of only authorized TNs by a customer.

## Use case examples for UNI Identity, Authentication, and Authorization in relation to SP use of SHAKEN

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. A way to represent the scenarios is a matrix of the service usage, security services applied, and expected SHAKEN attestation result. Below are some examples:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **End user** | **Customer** | **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 | LOA | 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 use) | 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 |
| … |  |  |  |  |  |  |  |

# Acronyms and abbreviations

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

SBC Session border controller

SP Service provider

STI-AS Secure Telephone Identity – Authentication Service

STI-VS Secure Telephone Identity – Verification Service

TN Telephone number

UA User agent

UNI User-to-network interface

VASP Value-added service provider

VoIP Voice over IP

# References

IETF RFC 8224, Authenticated Identity Management in the Session Initiation Protocol (SIP)

IETF RFC 8226, Secure Telephone Identity Credentials: Certificates

ATIS-1000074, Signature-based Handling of Asserted Information using Tokens (SHAKEN)

ATIS-1000080, Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management