ATIS-0300116

ATIS Standard on -

Interoperability Standards between Next Generation Networks (NGN) for Signature-Based Handling of Asserted information Using Tokens (SHAKEN)

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 and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Published by

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

ATIS-0300116

ATIS Standard on

Interoperability Standards between Next Generation Networks (NGN) for Signature-Based Handling of Asserted information Using Tokens (SHAKEN)

Alliance for Telecommunications Industry Solutions

Approved December 5, 2016

Abstract

This document is intended to provide Next Generation Network (NGN) telephone service providers (SPs) with a framework and guidance for interoperability as calls process through their networks implementing Signature-Based Handling of Asserted Information Using Tokens (SHAKEN) technologies to ensure the validation as well as the completion of legitimate calls and the mitigation of illegitimate spoofing of telephone identities.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Next Generation Interconnection Interoperability Forum (NGIIF) addresses next generation network interconnection and interoperability topics associated with emerging technologies. Specifically, it develops operational procedures that involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues that impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies.

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.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, NGIIF, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, NGIIF, which was responsible for its development, had the following leadership:

Amy Hindman, Co-Chair (Verizon Wireless)

Mary Retka, Co-Chair (CenturyLink)

Table of Contents

1 Scope and Purpose 1

1.1 Scope 1
1.2 Purpose 1

2 Normative References 1

3 Definitions, Acronyms, and Abbreviations 2

3.1 Definitions 2
3.2 Acronyms & Abbreviations 2

4 Overview 3

4.1 Operationalization Assumptions 4
4.2 STIR/SHAKEN Overview (from ATIS-1000074) 5
4.2.1 STIR Overview 5
4.2.2 Persona Assertion Token (PASSporT) Token 5
4.2.3 RFC 4474bis 5
4.3 SHAKEN Architecture 5
4.4 SHAKEN Call Flow 7
4.5 4474bis Verification Procedures 8
4.5.1 PASSporT and Identity Header Verification 8
4.5.2 Verification Error Conditions 8

5 Certificates 9

5.1 Certificate Assertion in Calls Processed Across Multiple Networks 9
5.2 Attestation Indicator (“attest”) 10
5.3 PASSporT and Identity Header Verification 10
5.4 Call Completion Reporting Related to Certification 11

6 Operational Considerations 12

6.1 Exception Processing 12
6.2 Error Handling 13
6.2.1 403 – Stale Date 13
6.2.2 428 – Use Identity Header 13
6.2.3 436 – Bad-Identity-Info 13
6.2.4 437 – Unsupported Credential 13
6.2.5 438 – Invalid Identity Header 14

Table of Figures

Figure 4.1 – SHAKEN Reference Architecture 6
Figure 4.2 – SHAKEN Reference Call Flow 7

ATIS Standard on –

Interoperability Standards between Next Generation Networks (NGN) for Signature-Based Handling of Asserted Information Using Tokens (SHAKEN)

1 Scope and Purpose

1.1 Scope

This document is intended to provide Next Generation Network (NGN) telephone service providers (SPs) with a framework and guidance for interoperability as calls process through their networks implementing Signature-Based Handling of Asserted Information Using Tokens (SHAKEN) technologies to ensure the validation as well as the completion of legitimate calls and the mitigation of illegitimate spoofing of telephone identities.

1.2 Purpose

This document will define the operationalization, between NGN telephone SPs, for the handling of signature-based and asserted information using the tokens (i.e., SHAKEN) framework.

2 Normative References

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

ATIS-1000074, *Signature-based Handling of Asserted information using Tokens (SHAKEN) framework document.*[1]

Report and Order (R&O) and *Further Notice of Proposed Rulemaking* (*FNPRM*) in FCC 13-135 and WC Docket No.13-39, adopted October 28, 2013 and released November 8, 2013.[2]

Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, WC Docket No. 07-135, *Declaratory Ruling and Order, FCC 15-72*, (released July 10, 2015).[3]

ATIS-0300106, *Intercarrier Call Completion/Call Termination Handbook.*[4]

draft-ietf-stir-rfc4474bis-09, *Authenticated Identity Management in the Session Initiation Protocol (SIP)*. This document is an active draft and subject to change.[5]

draft-ietf-stir-passport, *Persona Assertion Token*. This document is an active draft and subject to change.[6]

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/product.aspx?id=28297 >.

[2] This document is available from the Federal Communications Commission (FCC) at: < https://www.fcc.gov/ >.

[3] This document is available from the Federal Communications Commission (FCC) at < https://www.fcc.gov/ >.

[4] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/product.aspx?id=26780 >.

[5] This document is available from the Internet Engineering Task Force (IETF) at: < https://datatracker.ietf.org/doc/draft-ietf-stir-rfc4474bis/ >.

3 Definitions, Acronyms, and Abbreviations

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

3.1 Definitions

Trusted Network: A trusted network is a network that follows the 3GPP Trust Model[7]

Untrusted Network: An untrusted network is a network that does not follow the 3GPP Trust Model[8]

Local Policy: Factors that could influence "local policy" include state, national, international regulation, operator preferences (consistent with applicable regulation) and user preferences.

3.2 Acronyms & Abbreviations

ANI	Automatic Number Identity
AS	Authentication Service
ATIS	Alliance for Telecommunications Industry Solutions
CDR	Call Detail Record
CR	Call Record
CSCF	Call Session Control Function
CSR	Customer Service Record
CVT	Call Validation Treatment
FCC	Federal Communications Commission
FNPRM	Further Notice of Proposed Rule-Making
GETS	Government Emergency Telecommunications Service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAM	Initial Address Message
IBCF	Interconnection Border Control Functions
ID	Identification
IMS	IP-Multimedia Subsystem
IP	Internet Protocol
ISUP	Integrated Services Digital Network User Part

[6] This document is available from the Internet Engineering Task Force (IETF) at: < https://datatracker.ietf.org/doc/draft-ietf-stir-passport/ >.

[7] 3GPP TS 33.234 V023.0 (2002-11); 3GPP TS 29.165 V11.5.0 (2012-12).

[8] 3GPP TS 33.234 V023.0 (2002-11); 3GPP TS 29.165 V11.5.0 (2012-12).

JSON	JavaScript Object Notation
NGIIF	Next Generation Interconnection Interoperability Forum
NGN	Next Generation Network
NNI	Network-to-Network Interface
NS/EP	National Security and Emergency Preparedness
OCSP	Online Certificate Status Protocol
PASSporT	Persona Assertion Token
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
PKI	Public Key Infrastructure
R&O	Report and Order
RFC	Request for Comments
SHAKEN	Signature-Based Handling of Asserted Information Using Tokens
SIP	Session Initiation Protocol
SKS	Secure Private Key Store
SP	Service Provider
STI	Secure Telephone Identity
STIR	Secure Telephone Identity Revisited
3GPP	Third Generation Partnership Project
TDM	Time-Division Multiplexing
TN	Telephone Number
TrGW	Transition Gateway
UA	User Agent
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
VoIP	Voice over Internet Protocol
VS	Verification System

4 Overview

This interoperability standards document provides NGN telephone SPs with the information to interoperate while utilizing the SHAKEN session initiation protocol (SIP)-based framework for the authentication and assertion of a telephone identity on origination and the validation of the telephone identity of calls across networks.[9] This standard therefore relates to the interoperability among carriers as a result of the SHAKEN framework.

[9] It should be noted that SHAKEN has application to other potential critical service parameters in signaling messages.

4.1 Operationalization Assumptions

- All calls must attempt to complete to the end user.[10]
- SPs that sign authentication tokens will have the means to determine the legitimacy of the signaled parameters being attested to (such as the Caller ID to be displayed). This capability will include cases when the Caller ID to be displayed is different from the originating ANI or belongs to another SP.
- Today, assertion of telephone identity in VoIP networks between peering service providers, particularly in a 3GPP IP Multimedia Subsystem (IMS) environment, typically uses the P-Asserted-Identity as defined in RFC 3325 as a network self-asserted identity. This usage assumes an inherent trust model between peering providers. However, in many telephone calling scenarios where there are many indirect call path relationships between the originating and terminating providers, these trust relationships are often simply not verifiable and do not allow for identification of the true origination of the call. Currently, the P-Asserted-Identity header field can be populated by an enterprise Private Branch Exchange (PBX) and passed on without validation by the service provider.[11]
- Use of standardized cryptographic digital signatures to validate the originator of a signed identity can provide a verifiable mechanism to identify the authorized originator of a call into the VoIP network with non-repudiation. Further, the use of an assigned attestation indicator and a unique origination identifier depending on how and where the call is originated in the VoIP network represents the originating signer's ability to vouch for the accuracy of the source of origin of the call. For example, if the service provider has an authenticated direct relationship with the origination of the call, this attestation is categorized differently than calls that are originated from different networks or gateways that the service provider may have received from an unauthenticated network or that are unsigned. Verifiers of signatures will use these attestations as information to provide trace back mechanisms, as well as information to feed into any call spam identification solution enabled on behalf of their customer.[12]
- Authentication tokens signed by trusted SPs will be accepted by downstream providers even if the call is routed/handed off from an untrusted (by the terminating SP) intermediate provider.
- Common procedures will be established by the industry to deal with cases when an authentication token cannot be signed by the originating SP due to a network event or traffic congestion.
- Common procedures will be established by the industry to deal with cases when a received verification token cannot be validated by the terminating SP due to a network event or traffic congestion.
- Only the end user can choose to block the call or delegate that authority to block the call or use a call-blocking mitigation technique.[13] Calls that are sent to an intermediate provider and are "cranked back" (a term used to describe the means by which SPs routed around congestion) must continue processing to the next step in an attempt to complete the call to the end user of the dialed digits.[14]
- Terminating SPs shall complete the call to the end user, i.e., the called party, unless otherwise specified by the end user to block the call.
- Terminating SPs while processing calls signed by an untrusted network will follow a predetermined means to process the Caller ID.
- Terminating SPs while processing calls without signed tokens in their networks will follow a predetermined means for processing the Caller ID.
- Terminating SPs while processing calls with tokens signed by an SP other than the originating SP will follow a predetermined means for processing the Caller ID.
- Providers will follow a predetermined means to address errors in certificates.
- Providers will follow a predetermined means to address invalid certificates.

---

[10] Report and Order (R&O) and Further Notice of Proposed Rulemaking (FNPRM) in FCC 13-135 and WC Docket No.13-39, adopted October 28, 2013 and released November 8, 2013.

[11] ATIS-1000074, *Signature-based Handling of Asserted information using Tokens (SHAKEN)*

[12] ATIS-1000074, *Signature-based Handling of Asserted information using Tokens (SHAKEN)*

[13] Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, WC Docket No. 07-135, Declaratory Ruling and Order, FCC 15-72, (released July 10, 2015).

[14] ATIS-0300106, Intercarrier Call Completion/Call Termination Handbook, Section 6.

- Terminating SPs will follow a predetermined means to be able to determine if an originating SP's certificate has been revoked.
- Intermediate SPs are expected to pass all signaling without modifications. In cases where intermediate SPs legitimately (via contract or government mandate) make changes, they will apply their own signatures to the result, (such as via government contract for certain national security services).
- Terminating SPs will follow a predetermined means to address discrepancies between the attested Caller ID and the asserted Caller ID.

4.2 STIR/SHAKEN Overview (from ATIS-1000074)

4.2.1 STIR Overview

The documents draft-ietf-stir-rfc4474bis and draft-ietf-stir-passport define a set of protocol level tools that can be used in Session Initiation Protocol (SIP) for applying digital signatures to the Caller ID or telephone number of the calling party.[15]

4.2.2 Persona Assertion Token (PASSporT) Token

The document draft-ietf-stir-passport defines a token-based signature that combines the use of JavaScript Object Notation (JSON) Web Tokens, JSON Web Signatures, and X.509 certificate key pairs, or Public Key Infrastructure (PKI), to create a trusted signature. The authorized owner of the certificate used to generate the signature can be validated and traced back to the known trust anchor who signed the certificate. The Persona Assertion Token (PASSporT) token includes a number of claims the signer of the token is asserting. The associated public certificate is used to verify the digital signature and the claims included in the PASSporT token. The public certificate is also used to validate the entity that signed the token through a Service Provider Identifier (SPID), as defined in draft-ietf-stir-certificates. The validated claims and the validated identity of the entity signing the claims can both be used to determine the level of trust in the originating entity and their asserted calling party information. Call blocking applications or other mitigation techniques could use the information over time to determine "reputation" of the entity signing the token, which could provide further input to determine the level of trust for the calling party information. Note that PASSporT tokens and signatures themselves are agnostic to network signaling protocols but are used in draft-ietf-stir-rfc4474bis to define specific SIP usage as described in the next section.[16]

4.2.3 RFC 4474bis

The document draft-ietf-stir-rfc4474bis defines a SIP-based framework for an authentication service and verification service for using the PASSporT signature in a SIP INVITE. It defines a new Identity header field that delivers the PASSporT signature and other associated parameters. The authentication service adds the Identity header field and signature to the SIP INVITE generated by the originating provider. The INVITE is delivered to the destination provider which uses the verification service to verify the signature using the identity in the P-Asserted-Identity header field or From header field.[17]

4.3 SHAKEN Architecture

There are a number of architectural components required for an end-to-end STI framework.

The figure below shows the SHAKEN reference architecture. This is a logical view of the architecture and does not 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

[15] ATIS-1000074, *Signature-based Handling of Asserted information using Tokens (SHAKEN)*

[16] ibid.

[17] ibid.

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.[18]

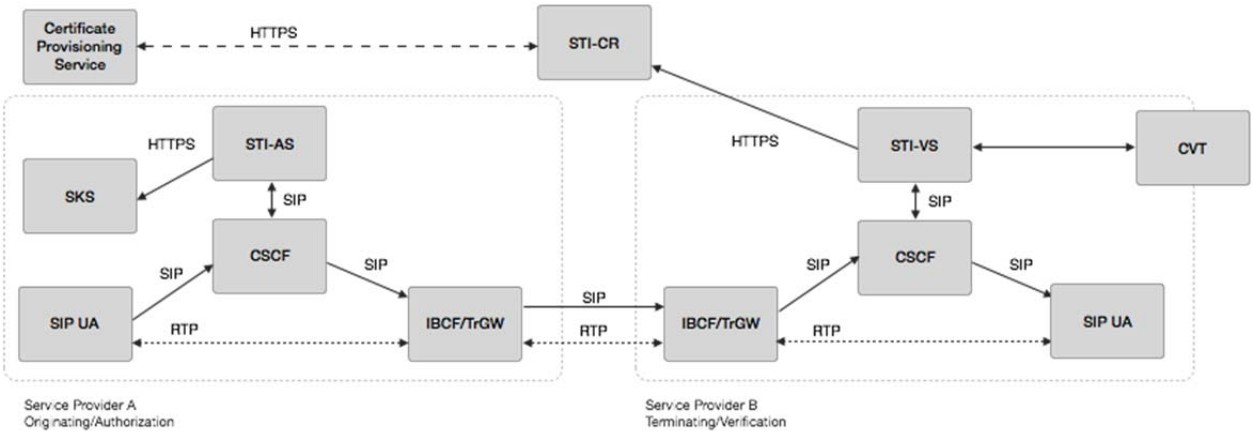

Figure 4.1 – SHAKEN Reference Architecture[19]

This SHAKEN reference architecture includes the following elements:

- SIP UA – The SIP User Agent authenticated by the service provider network. When the SIP UA is under direct management control of the telephone service provider, the service provider network can assert the calling party identity in originating SIP INVITE requests initiated by the SIP UA.
- IMS/Call Session Control Function (CSCF) – This component represents the SIP registrar and routing function. It also has a SIP application server interface.
- Interconnection Border Control Function (IBCF)/Transition Gateway (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 draft-ietf-stir-rfc4474bis. 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 that 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 draft-ietf-stir-rfc4474bis. It has an Hypertext Transfer Protocol Secure (HTTPS) interface to the Secure Telephone Identity 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. The CVT can also provide information in its response that indicates how the results of the verification should be displayed to the called 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.

[18] ibid.

[19] ibid.

- Secure Telephone Identity Certificate Repository (STI-CR) – This represents the publically 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.[20]

4.4 SHAKEN Call Flow

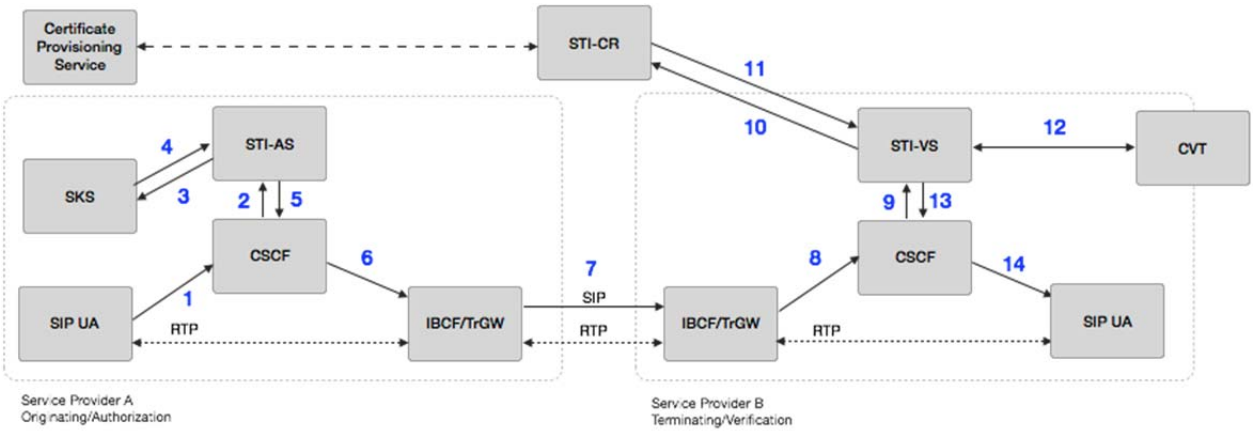

Figure 4.2 – SHAKEN Reference Call Flow[21]

1. The originating SIP UA, which first REGISTERs and is authenticated to the CSCF, creates a SIP INVITE with a telephone number identity.
2. The CSCF of the originating provider adds a P-Asserted-Identity header field asserting the Caller ID of the originating SIP UA. The CSCF then initiates an originating trigger to the STI-AS for the INVITE.
   NOTE: The STI-AS must be invoked after originating call processing.
3. The STI-AS in the originating SP (i.e., Service Provider A) first determines through service provider-specific means the legitimacy of the telephone number identity being used in the INVITE. The STI-AS then securely requests its private key from the SKS.
4. The SKS provides the private key in the response, and the STI-AS signs the INVITE and adds an Identity header field per draft-ietf-stir-rfc4474bis using the Caller ID in the P-Asserted-Identity header field.
5. The STI-AS passes the INVITE back to the SP A's CSCF.
6. The originating CSCF, through standard resolution, routes the call to the egress IBCF.
7. The INVITE is routed over the NNI through the standard inter-domain routing configuration.
8. The terminating SP's (Service Provider B) ingress IBCF receives the INVITE over the NNI.
9. The terminating CSCF initiates a terminating trigger to the STI-VS for the INVITE.
   NOTE: The STI-VS must be invoked before terminating call processing.
10. The terminating SP STI-VS uses the "info" parameter information in the Identity header field per draft-ietf-stir-rfc4474bis to determine the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR.
11. The STI-VS validates the certificate (see Section 5.3.1 [of ATIS-1000074] for details) and then extracts the public key. It constructs the draft-ietf-stir-rfc4474bis format and uses the public key to verify the signature in the Identity header field, which validates the Caller ID used when signing the INVITE on the originating service provider STI-AS.
12. The CVT is an optional function that can be invoked to perform call spam analytics or other mitigation techniques and return a response related to what should be signaled to the user for a legitimate or

[20] ibid.

[21] ibid.

illegitimate call. The CVT may be integrated in the service provider network or outside the service provider network by a third party.

13. Depending on the result of the STI validation, the STI-VS determines that the call is to be completed with any appropriate indicator (that may be defined outside of this document) and the INVITE is passed back to the terminating CSCF which continues to set up the call to the terminating SIP UA.

    NOTE: Error cases where verification fails are discussed in Section 6 [of ATIS-1000074 and Section 6.2 of this document].

14. The terminating SIP UA receives the INVITE and normal SIP processing of the call continues, returning "200 OK" or optionally setting up media end-to-end.[22]

4.5 4474bis Verification Procedures

Draft-ietf-stir-rfc4474bis defines the procedures for verification services including the methods used to verify the signature contained in the Identity header field.[23]

4.5.1 PASSporT and Identity Header Verification

The certificate referenced in the "info" parameter of the Identity header field shall be validated by performing the following:

- Check the certificate's validity using the Basic Path Validation algorithm defined in the X.509 certificate standard (RFC 5280).
- Check that the certificate is not revoked using CRLs and/or OCSP.

The verifier validates that the PASSporT token provided in the Identity header of the INVITE includes all of the baseline claims, as well as the SHAKEN extension claims. The verifier shall also follow the draft-ietf-stir-rfc4474bis-defined verification procedures to check the corresponding date, originating identity (i.e., the originating telephone number) and destination identities (i.e., the terminating telephone numbers).

The "orig" claim and "dest" claim shall be of type "tn".

The "orig" claim "tn" value validation shall be performed as follows:

- The P-Asserted-Identity header field value shall be checked as the telephone identity to be validated if present, otherwise the From header field value shall also be checked.
- If there are two P-Asserted-Identity values, the verification service shall check each of them until it finds one that is valid.

  NOTE: As discussed in draft-ietf-stir-rfc4474bis, call features such as call forwarding can cause calls to reach a destination different from the number in the To header field. The problem of determining whether or not these call features or other B2BUA functions have been used legitimately is out of scope of STIR. It is expected that future SHAKEN documents will address these use cases.[24]

4.5.2 Verification Error Conditions

If the authentication service functions correctly, and the certificate is valid and available to the verification service, the SIP message can be delivered successfully. However, if these conditions are not satisfied, errors can be generated as defined draft-ietf-stir-rfc4474bis. This section identifies important error conditions and specifies procedurally what should happen if they occur. Error handling procedures should consider how best to always deliver the call per current regulatory requirements[25] while providing diagnostic information back to the signer.

---

[22] ibid.

[23] ibid.

[24] ibid.

[25] Report and Order (R&O) and Further Notice of Proposed Rulemaking (FNPRM) in FCC 13-135 and WC Docket No. 13-39, adopted October 28, 2013 and released November 8, 2013 ("Rural Call Completion").

There are five main procedural errors defined in draft-ietf-stir-rfc4474bis that can identify issues with the validation of the Identity header field. The error conditions and their associated response codes and reason phrases are as follows:

403 – 'Stale Date' – Sent when the verification service receives a request with a Date header field value that is older than the local policy for freshness permits. The same response may be used when the "iat" has a value older than the local policy for freshness permits.

428 – 'Use Identity Header' is not recommended for SHAKEN until a point where all calls on the VoIP network are mandated to be signed either by local or global policy.

436 – 'Bad-Identity-Info' – The URI in the "info" parameter cannot be dereferenced (i.e., the request times out or receives a 4xx or 5xx error).

437 – 'Unsupported credential' – This error occurs when a credential is supplied by the "info" parameter but the verifier does not support it or it does not contain the proper certificate chain in order to trust the credentials.

438 – 'Invalid Identity Header' – This occurs if the signature verification fails.

If any of the above error conditions are detected, the terminating network shall convey the response code and reason phrase back to the originating network, indicating which one of the five error scenarios has occurred. How this error information is signaled to the originating network depends on the disposition of the call as a result of the error. If local policy dictates that the call should not proceed due to the error, then the terminating network shall include the error response code and reason phrase in the status line of a final 4xx error response sent to the originating network. On the other hand, if local policy dictates that the call should continue, then the terminating network shall include the error response code and reason phrase in a Reason header field (defined in [RFC 3326]) in the next provisional or final response sent to the originating network as a result of normal terminating call processing.

Example of Reason header field:

```
Reason: SIP ;cause=436 ;text="Bad Identity Info"
```

In addition, if any of the base claims or SHAKEN extension claims are missing from the PASSporT token claims, the verification service shall treat this as a 438 'Invalid Identity Header' error and proceed as defined above.[26]

5 Certificates

5.1 Certificate Assertion in Calls Processed Across Multiple Networks

With the implementation of SHAKEN, it is expected that there will be the addition of the identity header with the signature. ATIS-1000074 expects that for the majority of calls, the originator network will sign and authenticate the calling party TN where the originating SP holds the telephone number and has explicitly authenticated the origination of the telephone call from the device. There are however other scenarios to consider:

- The originating network provider signs and indirectly authenticates the calling party TN (where they have a third party – e.g., reseller – to whom they have provided their numbering resources.)
- The originating network provider signs the call but does not have any authority for calling party TN (e.g., roaming).
- Calls that originate on un-trusted networks (e.g., legacy TDM networks or networks where the provider is not certified).

[26] ATIS-1000074, *Signature-based Handling of Asserted information using Tokens (SHAKEN).*

5.2 Attestation Indicator ("attest")

This indicator allows for both identifying the service provider that is vouching for the call as well as clearly indicating what information the service provider is attesting to.

In the SHAKEN framework we define the following three levels of attestation:

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

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

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

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

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

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

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

NOTE: When partial attestation is used, each customer will have a unique origination identifier created and managed by the service provider, but the intention is that it will not be possible to reverse engineer the identity of the customer purely from the identifier or signature. As described in section 5.2.4, the unique origination identifier allows data analytics to establish a reputation profile and assess the reliability of information asserted by the customer assigned this unique identifier. The identifier also provides a reliable mechanism to determine the customer for forensic analysis or legal action where appropriate.

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

- Is the entry point of the call into its VoIP network.
- Has no relationship with the initiator of the call (e.g., international gateways).

NOTE: The token will provide a unique origination identifier of the node in the "origid" claim. (The signer is not asserting anything other than "this is the point where the call entered my network".)

For the PASSporT extension claim, the "attest" key value pair shall be set to uppercase characters "A", "B", or "C" corresponding to the appropriate attestation defined above.[27]

5.3 PASSporT and Identity Header Verification

ATIS-1000074 calls for the terminating end to provide the validation of the signature in the identity header and asserts that the following steps should be used:

[27] ibid.

- Check the certificate's validity using the Basic Path Validation algorithm defined in the X.509 certificate standard (RFC 5280).
- Check that the certificate is not revoked using CRLs and/or OCSP.[28]

In addition, the following step also needs to be completed:

- The asserted telephone number matches the signed Caller ID

However, SPs must attempt to complete the call to the terminating end. To accomplish this, SPs should follow these steps:

- The terminating end SP should allow the call to be completed, alerting the end user that the call cannot be validated using the normal method it employs to accomplish that alert.
- The terminating end SP should initiate the process to open a trouble ticket to the originating SP, indicating the call details, the validation issue encountered, and advising that the call was completed to the end user showing that it could not be validated.
- The originating SP should work to resolve the issue expeditiously, and to close the ticket with the terminating SP indicating that the issue was fixed.

5.4 Call Completion Reporting Related to Certification

To provide call completion reporting, with the addition of certification, the call detail record (CDR) will need to be augmented.

In the SHAKEN framework (ATIS-1000074), CDRs will need to capture information about calling number authentication information in SIP protocol call signaling. The following information is considered a starting point for inclusion in a SHAKEN-enabled CDR:

- A SHAKEN version number (which should be 0 if the element does not support SHAKEN processing).
- SHAKEN Identity header indication (e.g., 0/1, yes/no, true/false, exists/does-not-exist, found/not-found)
- The trunk group or other interface on which the call attempt arrived.
- The Certification Authority URL
  - PASSporT token protected header with the value BASE64URL(UTF(JWS Protected Header))
  - PASSporT token payload with the value BASE64URL(JWS Payload)
  - PASSporT token signature with the value BASE64URL(JWS Signature)
  - SHAKEN authentication attempt indicator:
    - Not Checked
    - SUCCESSFUL
    - FAILED – 403 'Stale Date'
    - FAILED- 428 'Use Identity Header'
    - FAILED – 436 'Bad-Identity-Info'
    - FAILED – 437 'Unsupported Credential'
    - FAILED – 438 'Invalid Identity Header'
    - FAILED – Unknown
  - The Level of Attestation
    - Full
    - Partial
    - Gateway
  - Origination Identifier UUID (RFC4122)

[28] ATIS-1000074, *Signature-based Handling of Asserted information using Tokens (SHAKEN)*

NOTE: Interworking SHAKEN with SS7 ISUP IAM “Screening Indicator” field at a SHAKEN-enabled PSTN gateway should also be captured in a CDR but is beyond the scope of this recommendation.

6 Operational Considerations

6.1 Exception Processing

The SHAKEN framework depends on the ability of the originating SP, after verifying the veracity of the signaled data, to sign the verification token using a private encryption key, obtained from the Certificate Repository. Similarly, the SHAKEN framework requires the terminating carrier to verify the signature using the corresponding public key, also obtained from the Certificate Repository.

Certificates in the Certificate Repository have expiration dates and may expire without being renewed. Additionally, under exceptional circumstances such as network outages, physical damage, disasters (natural or otherwise), or simple traffic congestion, it is possible that access to the encryption functionality will not be available to one or both carriers. The industry will need to develop common practices and procedures for dealing with these exception cases without either disrupting the flow of network traffic or compromising network integrity and security.

Following are guidelines for addressing exception cases:

NOTE: This list may not be all inclusive.

- Terminating SPs may indicate to the end user that the call was signed by an untrusted network, and therefore a risk exists that the Caller ID being shown is invalid.
- Terminating SPs may indicate to the end user that the call has not been signed, and therefore a risk exists that the Caller ID being shown is invalid.
- Terminating SPs shall check the originating SP’s current certificate issued by the Certificate Authority, and use the certificate to validate the call.
    - If the SP sending the signed token is a trusted source, the terminating SP may indicate to the end user that the call was signed by a trusted network.
    - If the SP sending the signed token is not a trusted source, the terminating SP may indicate to the end user that the call was signed by an untrusted network, and therefore a risk exists that the Caller ID being shown is invalid.
- Terminating SPs shall determine if the originating SP’s certificate is valid.
    - If the originating SP’s certificate is effective at the time of the call and the originating SP is a trusted network, the terminating SP may indicate to the end user that the call was signed by a trusted network.
    - If the originating SP’s certificate is not effective at the time of the call, the terminating SP may indicate to the end user that a risk exists that the Caller ID being shown is invalid.
- Under certain circumstances, an intermediate SP might legitimately (via contract or government mandate) alter the Caller ID and attest to the altered Caller ID with its own signature (e.g., for certain NS/EP GETS calls, it is the intermediate GETS SP who first authorizes the call, and then might legitimately change the Caller ID). In these cases, for the purposes of error processing, the intermediate SP that signed the token will be treated as the originating SP.
- Under certain circumstances or in abnormal situations (e.g., network damage or traffic congestion), it may not be possible for a SP to obtain or validate a certificate. In such cases call processing should continue to call completion. The terminating SP may indicate to the end user that the call was not signed or could not be verified, and therefore a risk exists that the Caller ID being shown is invalid. Terminating SPs may determine that the message header contents do not agree with the content signed by the token. The terminating SP call processing should continue to call completion. The Caller ID should be treated as an un-verified Caller ID. The terminating SP is expected to initiate off-line activity, such as opening a trouble ticket, to address the cause of this error.

6.2 Error Handling

The philosophy behind error handling is that, whenever possible and where not otherwise authorized by the terminating subscriber, call processing should continue to call completion regardless of the state of the Caller ID processing. Error handling procedures should consider how to deliver the call, whenever possible, per current regulatory requirements, while providing diagnostic information back to the originating SP.

The normative handling of the call set up where the SHAKEN framework is implemented will be for the originating end, having registered and been authenticated to the CSCF, to then process the call and send the call setup information, including the certificate information in the INVITE and the attestation indication. The terminating end receives the INVITE and validates the certificate, performs the termination functions, and returns the “200 OK” to the originating end.

When the terminating end determines that there is an issue with the INVITE or certificate, the error handling processes are implemented. Appropriate response codes, as listed below, should be sent to inform the originating SP of the anomaly. The following are the error messages and the means for handling those error messages.

6.2.1 403 – Stale Date

403 – ‘Stale Date’ – Sent when the verification service receives a request with a Date header field value that is older than the local policy for freshness permits. The same response may be used when the "iat" has a value older than the local policy for freshness permits.[29]

In the case of a ‘Stale Date’ error, call processing should continue to call completion. The Caller ID should be treated as an un-verified Caller ID.

Upon receiving this response code, the originating SP is expected to initiate off-line activity, such as opening a trouble ticket, to address the cause of this error.

6.2.2 428 – Use Identity Header

428 – ‘Use Identity Header’ is not recommended for SHAKEN until a point where all calls on the VoIP network are mandated to be signed either by local or global policy.[30]

6.2.3 436 – Bad-Identity-Info

436 – ‘Bad-Identity-Info’ – The URI in the “info” parameter cannot be dereferenced (i.e., the request times out or receives a 4xx or 5xx error). [31]

In the case of a ‘Bad-Identity-Info’ error, call processing should continue to call completion. The Caller ID should be treated as an un-verified Caller ID.

Upon receiving this response code, the originating SP is expected to initiate off-line activity, such as opening a trouble ticket, to address the cause of this error.

6.2.4 437 – Unsupported Credential

437 – ‘Unsupported credential’ – This error occurs when a credential is supplied by the “info” parameter but the verifier does not support it or it does not contain the proper certificate chain in order to trust the credentials.[32]

In the case of an ‘Unsupported Credential’ error, call processing should continue to call completion. The Caller ID should be treated either as an un-verified Caller ID or as ‘Unknown’.

---

[29] ibid.

[30] ibid.

[31] ibid.

[32] ibid.

Upon receiving this response code, the originating SP is expected to initiate off-line activity, such as opening a trouble ticket, to address the cause of this error.

6.2.5 438 – Invalid Identity Header

438 – 'Invalid Identity Header' – This occurs if the signature verification fails.[33]

In the case of an 'Invalid Identity Header' error, call processing should continue to call completion. The Caller ID should be treated as an invalid (spoofed) Caller ID.

Upon receiving this response code, the originating SP is expected to initiate off-line activity, such as opening a trouble ticket, to address the cause of this error.

[33] ibid.