ATIS-1000074-E
SIP Forum TWG-10-E

Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)

JOINT STANDARD

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/ >

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000074-E, Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)

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

Copyright © 2019 by Alliance for Telecommunications Industry Solutions and by SIP Forum LLC.
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380 or the SIP Forum at 203.829.6307. ATIS is online at < http://www.atis.org > and the SIP Forum is online at < http://www.sipforum.org >.

ATIS-1000074-E

SIP Forum TWG-10-E

ATIS Standard on

Signature-based Handling of Asserted information using toKENs (SHAKEN)

Alliance for Telecommunications Industry Solutions

Approved February 27, 2019

Abstract

Signature-based Handling of Asserted information using toKENs (SHAKEN) is an industry framework for managing the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and verification of the telephone identity and other information in an Internet Protocol (IP)-based service provider voice network. This specification defines the framework for telephone service providers to create signatures in Session Initiation Protocol (SIP) and validate initiators of signatures. It defines the various classes of signers and how the verification of a signature can be used toward the mitigation and identification of illegitimate use of national telecommunications infrastructure and to protect its users.

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

1 Scope & Purpose 1
1.1 Scope 1
1.2 Purpose 1
2 Normative References 1
3 Definitions, Acronyms, & Abbreviations 2
3.1 Definitions 2
3.2 Acronyms & Abbreviations 2
4 Overview 3
4.1 STIR Overview 4
4.1.1 Personal Assertion Token (PASSporT) *4*
4.1.2 RFC 8224 ..... *4*
4.2 SHAKEN Architecture 4
4.3 SHAKEN Call Flow 6
5 STI SIP Procedures 7
5.1 PASSporT Overview 7
5.2 RFC 8224 Authentication procedures 7
5.2.1 PASSporT & Identity Header Construction *7*
5.2.2 PASSporT Extension "shaken" *8*
5.2.3 Attestation Indicator ("attest") *9*
5.2.4 Origination Identifier ("origid") *10*
5.3 RFC 8224 Verification Procedures 11
5.3.1 PASSporT & Identity Header Verification *11*
5.3.2 Verification Error Conditions *12*
5.3.3 Use of the Full Form of PASSporT *13*
5.3.4 Handing of Calls with Signed SIP Resource Priority Header Field *13*
5.4 SIP Identity Header Example for SHAKEN 13

Table of Figures

Figure 4.1 – SHAKEN Reference Architecture 5
Figure 4.2 – SHAKEN Reference Call Flow 6

ATIS Standard on –

Signature-based Handling of Asserted information using toKENs (SHAKEN)

1 Scope & Purpose

1.1 Scope

This document is intended to provide telephone service providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies toward the validation of legitimate calls and the mitigation of illegitimate spoofing of telephone identities on IP-based service provider voice networks (also to be referred to as Voice over Internet Protocol [VoIP] networks). The primary focus of this document is on the format of STI claims, the mapping of these claims to SIP (RFC 3261), and the authentication and verification functions.

1.2 Purpose

Using the protocols defined in ~~draft-ietf-stir-rfc4474bis~~RFC 8224 and ~~draft-ietf-stir-passport~~RFC 8225, this document defines the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework. This framework is targeted at telephone service providers delivering phone calls over VoIP, and addresses the implementation and usage of the IETF STIR Working Group protocols and the architecture and use of STI-related X.509-based certificates (RFC 5280). It also discusses the general architecture of service provider authentication and verification services. Finally, it provides high level guidance on the use of positive or negative verification of the signature to mitigate illegitimate telephone identity in general.

Illegitimate Caller ID spoofing is a growing concern for North American telephone service providers and their customers. There are many Caller ID spoofing mechanisms, and illegitimate spoofing can evolve to evade mitigation techniques. Service provider solutions must therefore be flexible to respond to evolving threats in much the same way as cybersecurity solutions. In addition, the integration of new technologies into established VoIP networks imposes many interoperability and interworking challenges. As a result, this document is a baseline document on the implementation of the protocol-related requirements for STI. The objective is to provide a baseline that can evolve over time, incorporating more comprehensive functionality and a broader scope in a backward compatible and forward looking manner.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this ATIS 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.

IETF RFC 8225~~draft-ietf-stir-passport~~, *Personal Assertion Token.*[1]

IETF RFC 8224~~draft-ietf-stir-rfc4474bis~~, *Authenticated Identity Management in the Session Initiation Protocol.*[1]

IETF RFC 8226~~draft-ietf-stir-certificates~~, *Secure Telephone Identity Credentials: Certificates.*[1]

draft-ietf-stir-passport-shaken, *PASSporT SHAKEN Extension*.[1]

IETF RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks.*[1]

IETF RFC 3261, *SIP: Session Initiation Protocol.*[1]

[1] Available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org/ >.

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*[1]

IETF RFC 3326, *The Reason Header Field for the Session Initiation Protocol (SIP).*[1]

ATIS-1000080, *SHAKEN: Governance Model and Certificate Management*[2]

ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*[2]

3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).*[3]

3 Definitions, Acronyms, & 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

Caller ID: The originating or calling party telephone number used to identify the caller carried either in the P-Asserted Identity or From header.

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
ATIS	Alliance for Telecommunications Industry Solutions
B2BUA	Back-to-Back User Agent
CRL	Certificate Revocation List
CSCF	Call Session Control Function
CVT	Call Validation Treatment
HTTPS	Hypertext Transfer Protocol Secure
IBCF	Interconnection Border Control Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
JSON	JavaScript Object Notation
JWS	JSON Web Signature
NNI	Network-to-Network Interface
OCSP	Online Certificate Status Protocol
PASSporT	Personal Assertion Token

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < www.atis.org >.

[3] Available from 3rd Generation Partnership Project (3GPP) at: < https://www.3gpp.org >

PBX	Private Branch Exchange
PKI	Public Key Infrastructure
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SKS	Secure Key Store
SP	Service Provider
SPID	Service Provider Identifier
STI	Secure Telephone Identity
STI-AS	Secure Telephone Identity Authentication Service
STI-CA	Secure Telephone Identity Certification Authority
STI-CR	Secure Telephone Identity Certificate Repository
STI-VS	Secure Telephone Identity Verification Service
STIR	Secure Telephone Identity Revisited
TLS	Transport Layer Security
TN	Telephone Number
TrGW	Transition Gateway
UA	User Agent
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
VoIP	Voice over Internet Protocol

4 Overview

This document presents the SHAKEN framework. SHAKEN is defined as a framework that utilizes protocols defined in the IETF Secure Telephone Identity Revisited (STIR) Working Group that work together in an end-to-end architecture for the authentication and assertion of a telephone identity by an originating service provider and the verification of the telephone identity by a terminating service provider.

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.

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.

4.1 STIR Overview

The documents ~~-ietf-stir-rfc4474bis~~RFC 8224 and ~~ietf-stir-passport~~RFC 8225 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.

4.1.1 Personal Assertion Token (PASSporT) ~~Token~~

The document ~~-ietf-stir-passport~~RFC 8225 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 Personal 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 ~~ietf-stir-certificates~~RFC 8226. 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 PASSporTs ~~tokens~~ and signatures themselves are agnostic to network signaling protocols but are used in ~~draft-ietf-stir-rfc4474bis~~RFC 8224 to define specific SIP usage as described in the next section.

4.1.2 RFC ~~4474bis~~8224

The document ~~draft-ietf-stir-rfc4474bis~~RFC 8224 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.

4.2 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 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.

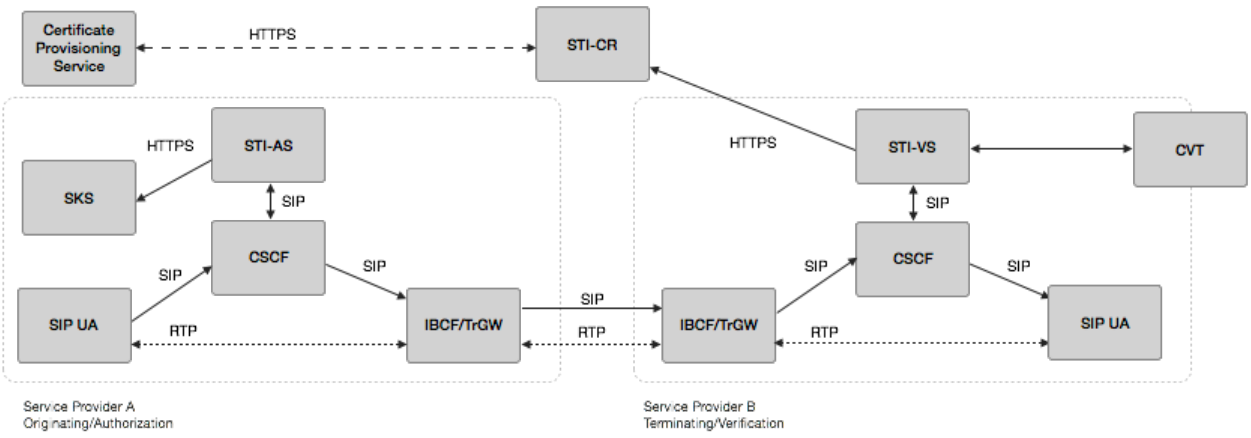

Figure 4.1 – SHAKEN Reference Architecture

This SHAKEN reference architecture includes the following elements:

- SIP UA – The SIP User Agent 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~~RFC 8224. 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~~RFC 8224. It has a~~n~~ 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.
- 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.

The focus of this document is on the STI-AS and STI-VS functionality and the relevant SIP signaling and interfaces. Detailed functionality for the Certificate Provisioning Service, the STI-CR, the SKS and the CVT will be provided in separate document(s).

4.3 SHAKEN Call Flow

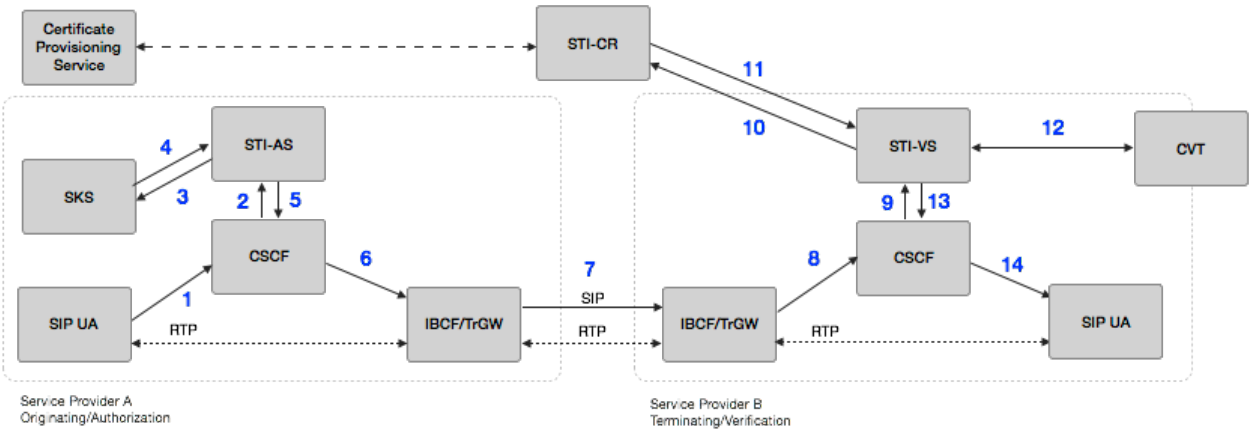

Figure 4.2 – SHAKEN Reference Call Flow

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~~RFC 8224 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 "x5u~~info~~" ~~parameter~~ field ~~information~~ in the PASSporT Protected Header~~Identity header field~~ per ~~draft-ietf-stir-rfc4474bis~~RFC 8225 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 for details) and then extracts the public key. It constructs the ~~draft-ietf-stir-rfc4474bis~~RFC 8224 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 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.
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.

5 STI SIP Procedures

Both RFC 8224draft-ietf-stir-4474bis and draft-ietf-stir-passportRFC 8225 define a base set of procedures for how STI fits into the SIP call flow. Draft-ietf-stir-rfc4474bisRFC 8224 defines an authentication service, corresponding to STI-AS in the SHAKEN reference architecture, as well as a verification service or STI-VS. This section will detail the procedures required for the STI-AS to create the required identity header.

5.1 PASSporT Token Overview

STI as defined in draft-ietf-stir-passportRFC 8225 specifies the process of the PASSporT token.

PASSporTs tokens have the following form:

- A protected header with the value BASE64URL(UTF(JWS Protected Header)).
- A payload with the value BASE64URL(JWS Payload).
- A signature with the value BASE64URL(JWS Signature).

An example of each is as follows:

Protected Header

```
{
      "typ":"passport",
      "alg":"ES256",
      "x5u":"https://cert.example.org/passport.crtcer"
}
```

Payload

```
{
       "iat":"1471375418"1443208345",
       "orig":{“tn”:"12155551212"},
       "dest":{“tn”:["12155551213"]}
}
```

draft-ietf-stir-passportRFC 8225 has specific examples of a PASSporT token.

5.2 4474bis RFC 8224 Authentication procedures

5.2.1 PASSporT & Identity Header Construction

For the SHAKEN framework, standard PASSporT base claims shall be used as defined in both PASSporT and draft-ietf-stir-rfc4474bis[RFC 8224] and [RFC 8225] documents, with the restrictions defined in this section.

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

The "orig" claim "tn" value shall be derived using the following rules:

- The P-Asserted-Identity header field value shall be used as the telephone identity, if present, otherwise the From header field value shall be used.
- If there are two P-Asserted-Identity header field values, the authentication service shall have logic to choose the most appropriate one based on local service provider policy.
- The action taken under the following conditions is outside the scope of this document:
    - There are P-Asserted-Identity header(s) present, but not one that contains a tel URI identity with a valid telephone number, or

- There are no P-Asserted-Identity header(s) present, and the From header does not contain a tel URI identity with a valid telephone number.

~~when neither the P-Asserted-Identity header field value nor the From header contain tel URI identities is outside the scope of the SHAKEN framework.~~

The "dest" claim "tn" value shall be derived using the following rules:

- The canonicalized value of the TN in the~~The~~ To header field value shall be used as the telephone identity.
- The action taken when the To header field does not contain a tel URI identity with a valid telephone number is outside the scope of the SHAKEN framework.

In the above context, the term "valid telephone number" refers to a telephone number that is a nationally specific service number (e.g., 611, 911), or a telephone number that can be converted into a globally routable E.164 number, as specified in section 8.3 of [RFC 8224].

~~Draft-ietf-stir-rfc4474bis~~RFC 8224 allows the Identity header to be inserted by a SIP proxy or UA ~~and for multiple instances of the Identity header to occur~~. The Identity header shall be transited by SIP proxies and Back-to-Back User Agents (B2BUAs), unless otherwise prevented by local service provider policy. A SIP proxy or B2BUA ~~may~~ shall not insert an additional Identity header to a received INVITE request that already contains an Identity header, unless local policy dictates the received Identity header is to be removed. ~~in the event that the SIP node needs to make a new claim.~~

As discussed in RFC 8224, 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 this specification. It is expected that future SHAKEN documents will address these use cases. Until future SHAKEN specifications clarify the handling of call diversion, the following authentication procedures shall be performed by the STI-AS when an SP that is not the originating network retargets an INVITE request to a new destination:

- If the STI-AS receives a retargeted INVITE request that does not contain an Identity header field then perform SHAKEN authentication and add a SHAKEN Identity header field.
- If the STI-AS receives a retargeted INVITE request that already contains an Identity header field, then take no action.

Performing SHAKEN authentication when the To header TN does not match the Request-URI TN (e.g., which may occur as a result of INVITE retargeting by the originating network in support of toll-free routing) can cause terminating verification services to ignore legitimately authenticated calls (e.g., for the toll-free routing case where the To header field contains the 8YY number, while Request-URI contains the routing number for that 8YY number). If allowed by local policy, the originating network can avoid these false verification results by updating the To header TN to match the Request-URI TN before performing SHAKEN authentication.

5.2.2 PASSporT Extension “shaken”

The base PASSporT set of claims cover the assertion of the originating telephone number along with date and destination telephone numbers to avoid replay attacks using valid Identity header fields. draft-ietf-stir-passport-shaken defines~~This section will detail a specific~~ the "shaken" extension to ~~the~~ PASSporT to cover the following requirements of SHAKEN. The ~~SHAKEN~~ “shaken” extension to PASSporT shall be implemented with all extension claims as part of the signed PASSporT ~~token~~.

1. The ability to provide an attestation indicator for the context of how the call was originated.
2. The ability to provide a unique originating identifier, as described in Section 5.2.4~~,~~ that can serve as an opaque indication of where in the originating service provider’s network the call was originated. ~~This identifier shall be globally unique and consistent so it can be used in analytics for tracking the reputation of a particular originating service and could also be used for any traceback efforts if a particular originator is a consistent or pervasive “bad actor”.~~

The PASSporT “shaken” extension shall include both an attestation indicator (“attest”), as described in section 5.2.3 and an origination identifier (“origid”) as described in section 5.2.4. The SHAKEN PASSporT ~~token~~ would have the form given in the example below:

Protected Header

```
{
      "alg":"ES256",
      "typ":"passport",
       "ppt":"shaken",
       "x5u":"https://cert.example.org/passport.cer~~rt~~"
}
```

Payload

```
{
       "attest":"A",
       "dest":{"tn":["12125551213~~—~~"]},
       "iat":~~"~~1471375418~~1443208345"~~,
       "orig":{"tn":"12155551212"},
       "origid":"123e4567-e89b-12d3-a456-426655440000"
}
```

5.2.3 Attestation Indicator ("attest")

The "attest" claim allows the originating service provider that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call.

~~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~~ 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.

NOTE: By populating this value, the service provider attests that it can trace the source of the call to a customer for policy enforcement purposes~~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".)~~

NOTE: The signer/originating service provider should be able to trace a call to an interconnecting service provider and/or peer node for traceback or policy enforcement purposes. Gateway attestation may also be used when the STI-AS does not have sufficient information for determining that A or B attestation applies even when the call was received at a customer interface.

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.

5.2.4 Origination Identifier ("origid")

In addition to attestation, the unique origination identifier ("origid") is defined as part of SHAKEN. This unique origination identifier should be a globally unique string corresponding to a Universally Unique Identifier (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.)~~initiated calls themselves~~, 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.

The origid is not intended to directly expose or be reverse-engineered to a customer or service provider identity, but it should be useful for analytics purposes in remote networks and traceback within the originating service provider network.

Best practices will specify when it is appropriate to use groupings less-granular than per-customer, customer device or node, or interconnecting service provider or interconnecting service provider node for origination identifier marking. Where origination identifier granularity is at the customer level or finer, best practices should also cover methods to protect the privacy of individual customers whose identity might be deduced through calling patterns.~~For Full Attestation, in general, a single identifier will be used as part of the certificate representing direct service provider-initiated calls on its VoIP network. A service provider may, for example, also choose to have a pool of identifiers to differentiate geographic regions or classes of customers. Best practices will likely develop as trace back and illegitimate call identification practices evolve.~~

~~For Partial Attestation, a single identifier per customer is required in order to differentiate calls both for trace back and reputation segmentation so that one customer's reputation doesn't affect other customer's or the service provider's call reputation. A service provider may choose to be more granular (e.g., per node per customer) depending on its size and classes of services that the service provider offers.~~

~~For Gateway Attestation, best practices will dictate that the "origid" should be sufficiently granular to identify the originating node or trunk to allow for trace back identification and reputation scoring.~~

5.3 ~~4474bis~~ RFC 8224 Verification Procedures

~~Draft-ietf-stir-rfc4474bis~~RFC 8224 defines the procedures for verification services including the methods used to verify the signature contained in the Identity header field.

5.3.1 PASSporT & 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 STI-VS shall determine the validity of the certificate referenced in the "x5u" field in the PASSporT protected header, applying the basic path validation as defined in [RFC 5280]. The basic steps are as follows:

1. The STI-VS retrieves the certificate referenced by the "x5u" field in the PASSporT protected header from the STI-CR, if not already cached. The STI-CR returns the end-entity certificate and the certificate chain that it previously downloaded from the STI-CA, as described in section 6.3.6 of ATIS-1000080.
2. If the certificate does not contain the required extensions as described in section 6.3.5.1 of [ATIS-1000080], then validation shall fail.
3. If not already cached, the STI-VS dereferences the URL for the CRL contained in the CRL Distribution Point extension. If the content-type header in the HTTPS response is not the media type application/pkix-crl validation shall fail.
4. The STI-VS follows the basic certificate path processing as described in [RFC 5280], following the chain until the root is reached (i.e., Issuer name=Subject name).
5. The STI-VS ensures that the root certificate is on the list of trusted STI-CAs.

The presence of the certificate on the CRL shall be treated as a verification failure (response code 437 'unsupported credential').

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~~RFC 8224-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), with the restrictions specified in this section.

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.

The "dest" claim "tn" value shall be validated using the canonicalized value of the To header field TN.

~~NOTE:~~ As discussed in [~~draft-ietf-stir-rfc4474bis~~RFC 8224], call features such as call forwarding can cause calls to reach a destination different from the ~~number~~ destination identified 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 this specification~~STIR~~. It is expected that future SHAKEN documents will address these use cases.

Subject to future specifications related to call forwarding or diversion cases, and in order to avoid false positive or false negative validation results when a SHAKEN Identity header is conveyed in a retargeted INVITE request, the verifier shall validate a received "shaken" PASSporT as specified above, with the following exception:

- If the canonicalized value of the Request-URI TN does not match the canonicalized value of the TN in the To header field, then the verifier shall skip verification, and treat the verification event as if no Identity header was received (NOTE-1).

- As an optional enhancement to the above exception, if the verifier is able to determine that the mismatching TNs in the Request-URI and To header field identify the same destination, then it may perform normal SHAKEN verification (NOTE-2).

NOTE-1: This exception would skip verification for all cases where an INVITE request is retargeted to a new TN, since the verification service is unable to determine whether the INVITE was legitimately retargeted or maliciously replayed. Also, even though verification is skipped in this case, the SP may cache the received Identity header to support subsequent trace back.

NOTE-2: This option narrows the number of cases where verification is skipped due to INVITE retargeting. If the verifier is able to determine that the TNs in the Request-URI and the To header field don't match, but they identify the same destination, then it can be confident that the INVITE was legitimately retargeted. It can therefore perform the normal SHAKEN verification procedures, and generate a valid pass/fail result. This would apply to toll-free calls, where the To header field contains the dialed 8YY number, while Request-URI contains the routing TN assigned to that 8YY number.

The terminating network conveys the verification result to the called user by including a "verstat" parameter in the From and/or P-Asserted-Identity header fields of the INVITE request sent to the called endpoint device, as defined in [TS 24.229].

If the calling user has requested privacy (i.e., the INVITE request contains a Privacy header field populated with the privacy-type "id"), then the verifier shall perform the SHAKEN validation procedures as defined above. Since the P-Asserted-Identity header is not included in the INVITE request sent to the called user when the call is private, any "verstat" parameter that is sent to the called endpoint device shall be conveyed in the From header field, as defined in [TS 24.229].

5.3.2 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~~RFC 8224. 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[4] while providing diagnostic information back to the signer.

There are five main procedural errors defined in ~~draft-ietf-stir-rfc4474bis~~RFC 8224 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[5] 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 "x5u~~info~~" ~~parameter~~ field 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 "x5u~~info~~" ~~parameter~~ field but the verifier doesn't support it or it doesn't contain the proper certificate chain in order to trust the credentials or the certificate has been revoked.

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

[4] 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").

[5] For operational considerations, please see ATIS-0300116, *Interoperability Standards between Next Generation Networks (NGN) for Signature-Based Handling of Asserted Information Using Tokens (SHAKEN)*.

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, as follows: ~~. 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, i~~
- 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.

5.3.3 Use of the Full Form of PASSporT

~~Draft-ietf-stir-rfc4474bis~~RFC 8224 supports the use of both full and compact forms of the PASSporT ~~token~~ in the Identity header. The full form of the PASSporT ~~token~~ shall be used to avoid any potential SIP network element interaction with headers, in particular the Date header field, which could lead to large numbers of 438 ('Invalid Identity Header') errors being generated.

5.3.4 Handing of Calls with Signed SIP Resource Priority Header Field

For calls that contain a SIP Resource Priority Header (RPH) field, post STI-VS information MUST not be passed for Call Validation Treatment (CVT). This is to ensure the highest probability of call completion for these types of calls.

5.4 SIP Identity Header Example for SHAKEN

~~Draft-ietf-stir-rfc4474bis~~RFC 8224 defines the Identity header field for SIP. It uses the PASSporT ~~token~~ as a basis for creation of the Identity header field in SIP INVITE messages.

An example of an INVITE with an Identity header field is as follows:

```
INVITE sip:+12155551213@tel.example1.net SIP/2.0
Via: SIP/2.0/UDP 10.36.78.177:60012;branch=z9hG4bK-524287-1---
77ba17085d60f141;rport
Max-Forwards: 69
Contact: <sip:+12155551212@69.241.19.12:50207;rinstance=9da3088f36cc528e>
To: <sip:+12155551213@tel.example1.net>
From: "Alice"<sip:+12155551212@tel.example2.net>;tag=614bdb40
Call-ID: 79048YzkxNDA5NTI1MzA0OWFjOTFkMmFlODhiNTI2OWQ1ZTI
P-Asserted-Identity: "Alice"<sip:+12155551212@tel.example2.net>,<tel:+12155551212>
CSeq: 2 INVITE
Allow: SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE, REFER, INFO, MESSAGE, OPTIONS
Content-Type: application/sdp
Date: Tue, 16 Aug 2016 19:23:38 GMT
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9
jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyIxM
jEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1NTEyMTIifSwib3Jp
Z2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0._V41ThRJ74MktxeLGaZQGAi
```

```
r8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-
EScb9otFNDxOCTjergeyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwicHB0Ijoic2hha2VuIiwie
DV1IjoiaHR0cDovL2NlcnQtYXV0aC5wb2Muc3lzLmNvbWNhc3QubmV0L2V4YW1wbGUuY2VydCJ9eyJhdHRl
c3QiOiJBIiwiZGVzdCI6eyJ0biI6IisxMjE1NTU1MTIxMyJ9LCJpYXQiOiIxNDcxMzc1NDE4Iiwib3JpZyI
6eyJ0biI64oCdKzEyMTU1NTUxMjEyIn0sIm9yaWdpZCI6IjEyM2U0NTY3LWU4OWItMTJkMy1hNDU2LTQyNj
Y1NTQ0MDAwMCJ9._28kAwRWnheXyA6nY4MvmK5JKHZH9hSYkWI4g75mnq9Tj2lW4WPm0PlvudoGaj7wM5Xu
jZUTb_3MA4modoDtCA
;info=<https://cert.example.org/passport.crthttp://cert.example2.net/example.cert>;
ppt="”shaken" ;alg=ES256
Content-Length: 153122

v=0
o=- 13103070023943130 1 IN IP4 10.36.78.177
s=-
c=IN IP4 10.36.78.177
t=0 0
m=audio 54242 RTP/AVP 0
a=sendrecv
```