ATIS-1000074.v002

ATIS Standard on

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

Alliance for Telecommunications Industry Solutions

Approved July 12, 2021

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.

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 3

4 Overview 5

4.1 STIR Overview 5
4.1.1 Personal Assertion Token (PASSporT) *5*
4.1.2 RFC 8224 ..... *5*
4.2 SHAKEN Architecture 6
4.3 SHAKEN Call Flow 7

5 STI SIP Procedures 8

5.1 PASSporT Overview 8
5.2 RFC 8224 Authentication procedures 9
5.2.1 PASSporT & Identity Header Construction *9*
5.2.2 PASSporT Extension "shaken" *10*
5.2.3 Attestation Indicator ("attest") *11*
5.2.4 Origination Identifier ("origid") *12*
5.3 RFC 8224 Verification Procedures 12
5.3.1 PASSporT & Identity Header Verification *12*
5.3.2 Verification Error Conditions *14*
5.3.3 Use of the Full Form of PASSporT *15*
5.3.4 Handing of Calls with Signed SIP Resource Priority Header Field *15*
5.4 SIP Identity Header Example for SHAKEN 16

Table of Figures

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

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 the Session Initiation Protocol (SIP) [IETF RFC 3261, *SIP: Session Initiation Protocol*], and the authentication and verification functions.

1.2 Purpose

Using the protocols defined in IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol,* and IETF RFC 8225, *Personal Assertion Token*, 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 Internet Engineering Task Force (IETF) Secure Telephone Identity Revisited (STIR) Working Group protocols and the architecture and use of STI-related X.509-based certificates [IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*]. 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 use of Caller ID spoofing in general.

Illegitimate Caller ID spoofing continues to be a 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 do. 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 standard 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 backwards-compatible and forward-looking manner.

2 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.

2.1 Normative References

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

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

[Ref 2] IETF RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks.*[1]

[Ref 3] IETF RFC 3326, *The Reason Header Field for the Session Initiation Protocol (SIP).*[2]

[Ref 4] IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*.[2]

[Ref 5] IETF RFC 4949, *Internet Security Glossary, Version 2.*[2]

[Ref 6] IETF RFC 5031, *A Uniform Resource Name (URN) for Emergency and Other Well-Known Services*.[2]

[Ref 7] IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*[2]

[Ref 8] IETF RFC 7515, *JSON Web Signature (JWS)*. [2]

[Ref 9] IETF RFC 8141, *Uniform Resource Names (URNs)*. [2]

[Ref 10] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*[2]

[Ref 11] IETF RFC 8225, *Personal Assertion Token.*[2]

[Ref 12] IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates.*[2]

[Ref 13] IETF RFC 8588, *Personal Assertion Token (PASSporT) for Signature-based Handling of Asserted information using toKENs (SHAKEN)*.[2]

[Ref 14] ATIS-1000080.v003, *SHAKEN: Governance Model and Certificate Management*[3]

[Ref 15] ATIS-1000085.v002, *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN): SHAKEN Support of "div" PASSporT.*[3]

[Ref 16] 3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).*[4]

[Ref 17] ATIS/TIA J-STD-036-C-2, Enhanced Wireless 9-1-1 Phase II, July 2017.[3]

2.2 Informative References

[Ref 101] ATIS-1000093, *ATIS Standard on Toll-Free Numbers in the SHAKEN Framework.*[3]

[Ref 102] ATIS-1000088, *A Framework for SHAKEN Attestation and Origination Identifier.*[3]

[Ref 103] ATIS-0300116, *Interoperability Standards between Next Generation Networks (NGN) for Signature-based Handling of Asserted Information using toKENs (SHAKEN).*[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

The following provides some key definitions used in this document. Refer to IETF RFC 4949, *Internet Security Glossary, Version 2,* for a complete Internet Security Glossary, as well as tutorial material for many of these terms.

Caller ID: The originating or calling party telephone number used to identify the caller carried either in the P-Asserted Identity or From header in the SIP [Ref 1] message.

---

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

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

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

(Digital) Certificate: Binds a public key to a Subject (e.g., the end entity). A certificate document in the form of a digital data object to which is appended a computed digital signature value that depends on the data object [IETF RFC 4949, *Internet Security Glossary, Version 2*]. See also STI Certificate.

Certification Authority (CA): An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate [Ref 5].

Certificate Validation: An act or process by which a certificate user establishes that the assertions made by a certificate can be trusted [Ref 5]. See also Path Validation.

Certificate Revocation List (CRL): A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire [Ref 5].

End Entity: An entity that participates in the Public Key Infrastructure (PKI). Usually a Server, Service, Router, or a Person. In the context of SHAKEN, it is the Service Provider on behalf of the originating endpoint.

Identity: Unless otherwise qualified (see, for example, Telephone Identity below), an identifier that unambiguously distinguishes an entity for authentication and other security and policy application purposes. In this standard, a Service Provider Code is an example of the identity of one kind of participant in the certificate management process.

Path Validation: The process of validating (a) all the digital certificates in a certification path and (b) the required relationships between those certificates, thus validating the contents of the last certificate in the path [Ref 5]. See also Certificate Validation.

Private Key: In asymmetric cryptography, the private key is kept secret by the end-entity. The private key can be used for both encryption and decryption [Ref 5].

Public Key: The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography [Ref 5].

Public Key Infrastructure (PKI): The set of hardware, software, personnel, policy, and procedures used by a CA to issue and manage certificates [Ref 5].

Secure Telephone Identity (STI) Certificate: A public key certificate, based on a service provider public and private key pair, used to sign and verify a PASSporT.

Service Provider Code: In the context of this document, this term refers to any unique identifier that is allocated by a Regulatory and/or administrative entity to a service provider.

Signature: Created by signing the message using the private key. It ensures the identity of the sender and the integrity of the data [Ref 5].

Telephone Identity: An identifier associated with an originator of a telephone call. In the context of the SHAKEN framework, this is a SIP identity (e.g., a SIP Uniform Resource Identifier [URI] or a TEL URI) from which a telephone number can be derived.

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
NS/EP	National Security / Emergency Preparedness
NS/EP PS	National Security / Emergency Preparedness Priority Service
OSP	Originating Service Provider
PASSporT	Personal Assertion Token
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
SPC	Service Provider Code
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 STIR Working Group that work together in an end-to-end architecture for the authentication and assertion of a Caller ID by an originating service provider and the verification of this 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 IETF RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks*, 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, for example, the P-Asserted-Identity header field can be populated by an enterprise Private Branch Exchange (PBX) and passed on without validation by the originating 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 an 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 originating service provider has an authenticated direct relationship with the originator 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 traceback mechanisms, as well as information to feed into any call analytics enabled on behalf of their customer.

4.1 STIR Overview

The documents IETF RFC 8224 [Ref 10] and IETF RFC 8225 [Ref 11] define a set of protocol-level tools that can be used in SIP for applying digital signatures to the Caller ID.

4.1.1 Personal Assertion Token (PASSporT)

The document IETF RFC 8225 [Ref 11] 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) 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. The public certificate is also used to validate the entity that signed the token through a Service Provider Code (SPC), as defined in IETF RFC 8226, *Secure Telephone Identity Credentials: 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 PASSporT, which could provide further input to determine the level of trust for the calling party information. Note that PASSporTs and signatures themselves are agnostic to network signaling protocols but are used in IETF RFC 8224 [Ref 10] to define specific SIP usage as described in the next clause.

4.1.2 RFC 8224

The document IETF RFC 8224 [Ref 10] defines a SIP-based framework for an authentication service and verification service for using the PASSporT signature in a SIP INVITE. It defines the 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.

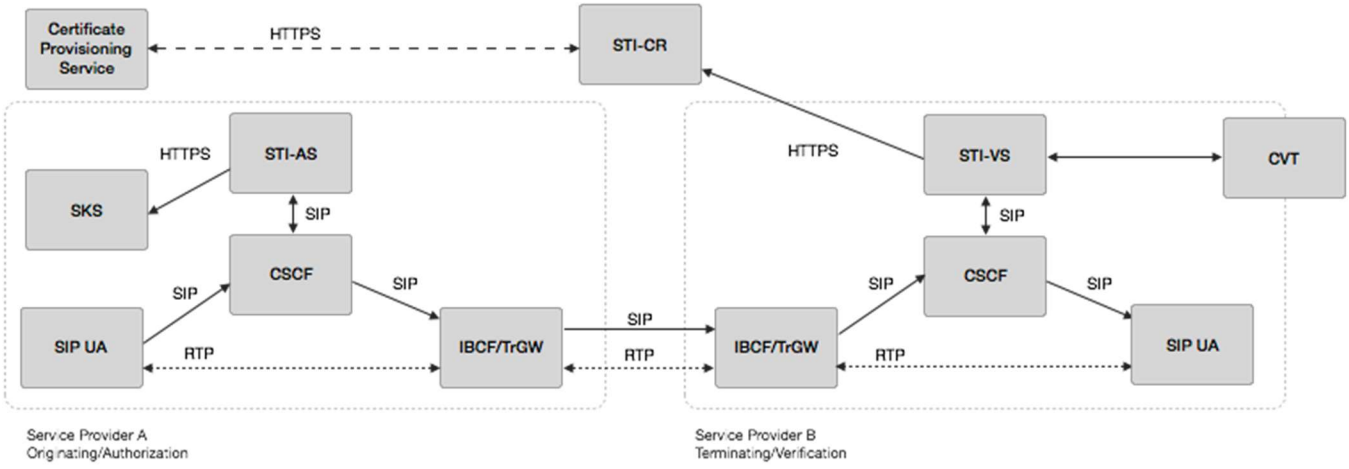

Figure 4.1 – SHAKEN Reference Architecture

This SHAKEN reference architecture includes the following elements:

- SIP User Agent (UA) – The SIP UA authenticated by the originating service provider (OSP) network. When the SIP UA is under direct management control of the OSP, the OSP's 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 IETF RFC 8224 [Ref 10]. It should either itself be highly secure 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 IETF RFC 8224 [Ref 10]. It has a 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 call analytics and treatment techniques once the signature is positively or negatively verified.
- 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 publicly accessible store for public key certificates. This is 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 is specified in separate document(s), including ATIS-1000080.v003, *SHAKEN: Governance Model and Certificate Management*.

4.3 SHAKEN Call Flow

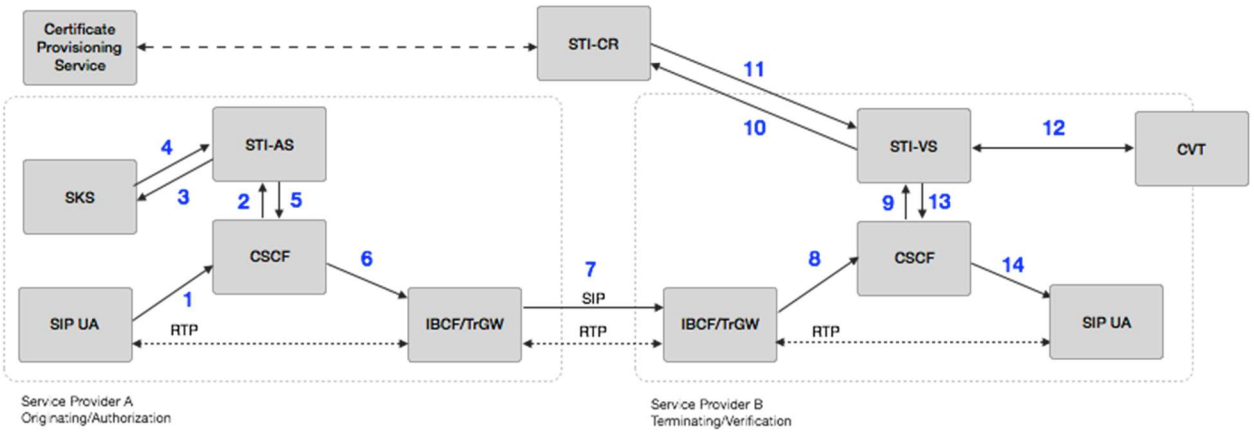

Figure 4.2 – SHAKEN Reference Call Flow

1. The originating SIP UA, which first registers and is authenticated to the CSCF, creates a SIP INVITE with a Telephone 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 should be invoked after processing of call features that may impact either the origination or destination telephone number.

3. The STI-AS in the originating SP (e.g., Service Provider A) network first determines through service provider-specific means the legitimacy of the Telephone 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 Identity header field(s) per IETF RFC 8224 [Ref 10] using the Caller ID in the P-Asserted-Identity header field.
5. The STI-AS passes the INVITE back to 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 (e.g., 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 should be invoked before processing of call features that may impact either the origination or destination number.

10. The terminating SP STI-VS uses the "x5u" field in the PASSporT Protected Header per IETF RFC 8225 [Ref 11] to determine the STI-CR URI and makes an HTTPS request to the referenced STI-CR.
11. The STI-VS validates the certificate (see Clause 5.3.1 for details) and then extracts the public key. It constructs the IETF RFC 8224 [Ref 10] 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's STI-AS.

12. The CVT is an optional function that can be invoked to perform call analytics or other spam mitigation techniques. The CVT may be integrated within the service provider network or outside the service provider network by a third party.
13. Depending on the result of the STI verification, the STI-VS determines that the call is to be completed with the appropriate "verstat" value (defined in 3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol [SIP] and Session Description Protocol [SDP]*) 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 Clause 5.3.2.

14. The terminating SIP UA receives the INVITE and normal SIP processing of the call continues.

5 STI SIP Procedures

Both IETF RFC 8224 [Ref 10] and IETF RFC 8225 [Ref 11] define a base set of normative procedures for how STI fits into the SIP call flow. IETF RFC 8224 [Ref 10] defines an authentication service, corresponding to the STI-AS in the SHAKEN reference architecture, as well as a verification service corresponding to STI-VS. This clause will detail the procedures required for the STI-AS to create the Identity header field.

5.1 PASSporT Overview

The document IETF RFC 8225 [Ref 11] specifies the process for creating and verifying PASSporTs.

PASSporTs 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.cer"
}
```

Payload

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

IETF RFC 8225 [Ref 11] has specific examples of PASSporTs.

5.2 Authentication procedures

5.2.1 Destination URI handling for SHAKEN authentication

In call scenarios where the originating SP is required to replace a non-routable dial string[5] in the Request-URI with an E.164 number in order to route the call, the originating SP shall also update the To header field to contain the same E.164 number. The To header field shall be updated before SHAKEN authentication services are applied to the originating call. This will ensure that the To header TN is of the form required to support SHAKEN verification; i.e., it will enable remote verifiers to unambiguously canonicalize the To header TN during PASSporT signature validation, and to positively confirm that the To header TN identifies the intended recipient of the call as part of replay attack detection.

> NOTE: Due to the unique routing requirements for emergency calls, the above procedure does not apply to emergency originations (i.e., where the To header field contains digits "911" or a service URN in the "sos" family). Also, the procedures for handling the conversion of a toll-free number to a routing number are specified in Clause 5.2.1, ATIS-1000085.v002, *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN): SHAKEN Support "div" PASSporT*, and ATIS-1000093, *ATIS Standard on Toll-Free Numbers in the SHAKEN Framework*.

5.2.2 PASSporT & Identity Header Construction

For the SHAKEN framework, standard PASSporT base claims shall be used as defined in both IETF RFC 8224 [Ref 10] and IETF RFC 8225 [Ref 11] documents, with the restrictions defined in this clause.

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

The "dest" claim shall be of type "tn" or shall be of type "uri" if the "dest" claim contains a service URN in the "sos" family [IETF RFC 5031, *A Uniform Resource Name (URN) for Emergency and Other Well-Known Services*].

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 one or more 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.

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

- For a "dest" claim of type "tn", the canonicalized value of the TN in the To header field value shall be used as the Telephone Identity.
- The action taken when the To header field does not contain either a tel URI identity with a valid telephone number or a service URN in the "sos" family is outside the scope of the SHAKEN framework.

The following special procedures shall be applied to support 9-1-1 call originations:

- If the To header and/or the Request-URI contains a service URN in the "sos" family (e.g., urn:service:sos), a "dest" claim of type "uri" containing a service URN in the "sos" family shall be permitted. The only dest

[5] Examples of non-routable dial strings include speed-dial codes, vertical service codes, NXX service codes, abbreviated extension numbers in a private dial plan, local numbers in a 7-digit dial plan (missing the NPA and country-code digits), non-toll-free 10-digit numbers (missing the country-code digit), dial-around digits (101xxxx), international dialing prefix (011+), and domestic or international operator codes (0-, 0+, 010-, 01+).

claim of type “uri” that is currently allowed is a service URN in the “sos” family, e.g.,`"dest":{"uri":["urn:service:sos"]}`.

- If the calling TN identified in the P-Asserted-Identity or From header field is a non-dialable callback number formatted according to Annex C of J-STD-036-C-2, *Enhanced Wireless 9-1-1 Phase II, July 2017*, then the authentication service shall treat that calling TN as if it were a valid E.164 number; i.e., it shall canonicalize the calling TN to remove any leading “+” sign or visual separators (i.e., “.”, “-”, “(”, and “)”), and then populate the “orig” claim with the resulting digit string. This special procedure shall be applied only if the non-dialable callback number is a string of 10 digits with leading digits “911” or 11 digits with leading digits “1911”.

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), a non-dialable callback number for an emergency call, or a telephone number that can be converted into a globally routable E.164 number, as specified in Clause 8.3 of IETF RFC 8224 [Ref 10].

IETF RFC 8224 [Ref 10] allows the Identity header to be inserted by a SIP proxy or UA. 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 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.

As discussed in IETF RFC 8224 [Ref 10], call features such as call forwarding can cause calls to reach a destination different from the number in the To header field. The method for determining whether or not these call features or other B2BUA functions have been used legitimately is specified in ATIS-1000085.v002 [Ref 15]. If the procedures in ATIS-1000085.v002 [Ref 15] are not supported for 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 authentication and add a SIP Identity header field.
- If the STI-AS receives a retargeted INVITE request that already contains an Identity header field, then authentication is not performed (i.e., no new Identity header(s) are generated).

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 verification by terminating service providers to ignore legitimately-authenticated calls (e.g., for the toll-free routing case where the To header field contains the 8YY number, while the Request-URI contains the routing telephone number for that 8YY call). If allowed by local policy and consistent with the particular use of retargeting, the originating network can update the To header TN to match the Request-URI TN before performing SHAKEN authentication to facilitate successful verification. Likewise, in support of emergency (i.e., 9-1-1) originations, if the To header contains a TN that is an emergency service number and the Request-URI contains an emergency service URN, the originating network may, based on local policy, update the To header to match the Request-URI prior to performing SHAKEN authentication.

5.2.3 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. IETF RFC 8588, *Personal Assertion Token (PASSporT) for Signature-based Handling of Asserted information using toKENs (SHAKEN),* defines the "shaken" extension to PASSporT to cover the following requirements of SHAKEN. The “shaken” extension to PASSporT shall be implemented with all extension claims as part of the signed PASSporT.

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

Protected Header

```
{
      "alg":"ES256",
      "typ":"passport",
```

```
        "ppt":"shaken",
        "x5u":"https://cert.example.org/passport.cer"
}
```

Payload

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

5.2.4 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.

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 telephone 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 TN was assigned to this customer by the signing service provider.
- This TN 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 TN (e.g., by business agreement or evidence the customer has access to use the number). This includes TNs assigned by another service provider.
- The TN 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 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.

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

- Has no relationship with the initiator of the call (e.g., international gateways).

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 an "A" or "B" attestation level 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 level defined above.

To support 9-1-1 call originations in which the P-Asserted-Identity header is populated by the originating service provider with a non-dialable callback number formatted according to Annex C of J-STD-036-C-2 [Ref 17], an attestation level of "A" shall be associated with the non-dialable callback number.

5.2.5 Origination Identifier ("origid")

In addition to attestation, the origination identifier ("origid") is defined as part of SHAKEN. The origination identifier shall be a string. The origination identifier should be a unique string corresponding to a Universally Unique Identifier (UUID) [IETF RFC 4122, *A Universally Unique Identifier (UUID) URN Namespace*].

The purpose of the origination identifier is to assign an opaque identifier corresponding to all or part of the originating service provider's network (data centers, IBCF nodes, access networks, IMS core complexes, etc.), customers, customer or interconnecting service provider nodes, classes of customer devices, or other groupings that a service provider might want to use to indicate common call sources for determining things such as reputation or traceback identification of customers or gateways.

The origination identifier is not intended to directly expose or be reverse-engineered to a customer or service provider identity, but it may be useful for call 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. See, for example, the origination identifier guidelines in ATIS-1000088, *A Framework for SHAKEN Attestation and Origination Identifier*.

5.3 RFC 8224 Verification Procedures

The document IETF RFC 8224 [Ref 10] 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 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 IETF RFC 5280 [Ref 7]. The steps are as follows:

1. If not already cached, the STI-VS retrieves the certificate referenced by the "x5u" field in the PASSporT protected header from the STI-CR as described in Clause 4.1.5 of IETF RFC 7515, *JSON Web Signature (JWS)*. The body of the "200 OK" response from the STI-CR contains the end entity certificate and the certificate chain that was previously downloaded from the STI-CA, as described in Clause 6.3.6 of ATIS-1000080.v003 [Ref 14].
2. If the certificate does not contain the required extensions as described in Clauses 6.3.5.1 and 6.4.1 of ATIS-1000080.v003 [Ref 14], then verification 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", or if the HTTPS response is valid but the returned CRL fails the CRL validation procedures in Clause 6.3 of IETF RFC 5280 [Ref 7], then verification shall fail.

NOTE: As part of CRL verification, the STI-VS shall retrieve the certificate referenced by the URL contained in the CRL Authority Information Access extension accessLocation field. The HTTPS response shall contain a Content-Type header field with a media type of "application/pem-certificate-chain", and a message body containing the STI-PA certificate that signed the CRL plus the additional certificates in the certification path. The STI-VS shall verify that the certification path is anchored at the STI-PA's root certificate that was previously provided to the STI-VS via an out-of-band mechanism.

4. If the certificate retrieved in Step 1 is not listed in the CRL, then the STI-VS follows the basic certificate path processing as described in IETF RFC 5280 [Ref 7], following the chain until the root is reached (i.e., Issuer name=Subject name).
5. The STI-VS then ensures that this root certificate is on the list of trusted STI-CAs.

If the "shaken" PASSporT is successfully validated, the attestation level shall be the value indicated by the "attest" claim, and not be altered by post STI-VS processing.

The presence of the certificate on the CRL shall be treated as a verification failure (response code 437 'Unsupported Credential'). The STI-VS shall retrieve a new CRL prior to the date/time of the Next Update field in the cached CRL to ensure the list is kept as up-to-date as possible. The exact timing is based on local policy.

The verifier validates that the PASSporT provided in the Identity header of the INVITE includes all of the baseline claims, as well as the SHAKEN extension claims as specified in ATIS-1000080.v003 [Ref 14]. The verifier shall also follow the IETF RFC 8224 [Ref 10]-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 clause.

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

The "dest" claim shall be of type "tn" or shall be of type "uri" if the "dest" claim contains a service URN in the 'sos' family.

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 be checked.
- If two or more P-Asserted-Identity values are received in an INVITE request, local policy shall determine which P-Asserted-Identity value(s) are passed to the verification server. If two or more P-Asserted-Identity values are received by the verification service, the verification server shall check each of them until it finds one that is valid and indicate the verification result of each value checked.
- If the call is to an emergency services destination, and the calling TN identified in the P-Asserted-Identity or From header field is a non-dialable callback number formatted as described in Annex C of J-STD-036-C-2 [Ref 17], then treat the calling TN as if it were an E.164 number; i.e., canonicalize the calling TN to remove any leading "+" sign or visual separators (i.e., ".", "-", "(", and ")"), and then use the resulting digit-string to check the "orig" claim. This special procedure shall be applied only if the non-dialable callback number is a string of 10 digits with leading digits "911" or 11 digits with leading digits "1911".

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

A "dest" claim that contains a service URN in the "sos" family, which will be of type "uri", shall be validated using the To header field "uri", normalized as specified in IETF RFC 8224 [Ref 10], and the URN equivalence procedures defined in IETF RFC 8141, *Uniform Resource Names (URNs)*.

As discussed in IETF RFC 8224 [Ref 10], call features such as call forwarding can cause calls to reach a destination different from the destination identified in the To header field. The method of determining whether or not these call features or other B2BUA functions have been used legitimately is specified in ATIS-1000085.v002 [Ref 15].

If the procedures in ATIS-1000085.v002 [Ref 15] are not supported, and in order to avoid "false" positive or negative validation results when a SIP Identity header field 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 this 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 will 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 terminating SP may cache the received Identity header to support subsequent traceback.

  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 result. This will apply to toll-free calls, where the To header field contains the dialed 8YY number, while the Request-URI contains the routing TN assigned to that 8YY call.

If the To header contains a TN that is an emergency service number and the Request-URI contains an emergency service URN, the verifier shall perform normal SHAKEN verification.

The terminating network conveys the verification result to the called user by including a tel URI “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 3GPP TS 24.229 [Ref 16].

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 3GPP TS 24.229 [Ref 16].

A verstat value of “TN-Validation-Passed” shall be included in the From and/or P-Asserted-Identity header fields of the INVITE request sent to the called endpoint device only if verification passes and one of the two following conditions exist:

1. The verified attestation level is “A”, or
2. The verified attestation level is also included in the INVITE request sent to the called endpoint device.

If the verified attestation level is “B” or “C”, and the attestation level is not included in the INVITE request sent to the called endpoint device, then the terminating network shall either set the “verstat” value in the INVITE request to “No-TN-Validation” or shall omit the “verstat” parameter from the INVITE request. The option selected is based on local policy.

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 INVITE can be delivered successfully. However, if these conditions are not satisfied, errors can be generated as defined in IETF RFC 8224 [Ref 10]. This clause 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[6], while providing diagnostic information back to the signer.

There are five main procedural errors defined in IETF RFC 8224 [Ref 10] that can identify issues with the verification of the Identity header field. The error conditions and their associated response codes and reason phrases are as follows:

[6] 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”).

403 – 'Stale Date' – Sent when the verification service receives a request with the "iat" value that is older than the local policy[7] 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" 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" field but the verifier doesn't support it, 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.

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:

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

The document IETF RFC 8224 [Ref 10] supports the use of both full and compact forms of the PASSporT in the Identity header. The full form of the PASSporT 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 errors being generated (the "iat" value in the payload that is protected by the signatures should be considered a more reliable indicator of PASSporT freshness than any time value in the SIP Date header).

5.3.4 Handling of Calls with Signed SIP Resource Priority Header Field

For calls that contain a SIP Resource Priority Header (RPH) field, post STI-VS information may be passed for Call Validation Treatment (CVT) depending on the value of the namespace parameter in the RPH field and in accordance with local policy and/or policy of the authority responsible for the specific service.

Emergency

Calls with a SIP RPH value in the "esnet" namespace may be passed for CVT depending on local policy.

National Security / Emergency Preparedness Priority Service (NS/EP PS)

Calls with SIP RPH values in the "ets" and/or "wps" namespaces may be passed for CVT depending on local policy.

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

An NS/EP call with an “rph” PASSporT that is successfully verified is treated as if it has a verified “shaken” PASSporT with an attestation level of “A”.

5.4 SIP Identity Header Example for SHAKEN

IETF RFC 8224 [Ref 10] defines the Identity header field for SIP. It uses the PASSporT 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-EScb9otFNDxOCTjerg
;info=<https://cert.example.org/passport.cer>;ppt="shaken"
Content-Length: 122


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
```