**A****TIS-0x0000x**

ATIS Standard on

**Signature-Based Handling of Asserted Information Using Tokens (SHAKEN):**

**SHAKEN Support of "div" PASSporT Token**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

The base SHAKEN specification provides replay-detection mechanisms to identify cases where a malicious entity attempts to masquerade as another user by replaying parts of a legitimate INVITE request. However, these mechanisms don’t cover cases where the INVITE is replayed within the short Date freshness window. This technical report describes how the mechanisms defined by draft-ietf-stir-passport-divert can be integrated within the SHAKEN framework to close this replay attack window.

**Foreword**

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [**COMMITTEE NAME**] Committee [**INSERT MISSION**]. [**INSERT SCOPE**].

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 a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

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

At the time of consensus on this document, [**COMMITTEE NAME**], which was responsible for its development, had the following leadership:

[**LEADERSHIP LIST**]

The **[SUBCOMMITTEE NAME]** Subcommittee was responsible for the development of this document.

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
|  |  |  |  |

**Table of Contents**

1 Scope & Purpose 1

1.1 Scope 1

1.2 Purpose 1

1.2.1 Document Organization 1

2 Normative References 2

3 Definitions, Acronyms, & Abbreviations 2

3.1 Definitions 2

3.2 Acronyms & Abbreviations 2

4 Overview 3

5 Normative Requirements 5

5.1 STI-AS Base SHAKEN Authentication Assumptions 5

5.2 STI-VS Base SHAKEN Verification Assumptions 5

5.3 STI-AS "div" Authentication 5

5.4 STI-VS "div" Verification 5

5.5 In-network Call Diversion 5

5.6 End-user Device Call Diversion 6

5.6.1 Call Diversion by Redirecting the INVITE Request 6

5.6.2 Call Diversion by Retargeting the INVITE Request 6

**Table of Figures**

Figure 1. Using "div" PASSporT to authenticate the forwarding leg of call 4

Figure 2. STI-AS Authentication Examples 8

Figure 3. STI-AS logic to determine authentication procedures for INVITE from CPE 9

Figure 4. Message sequence diagram template 10

Figure 5. Case-1a – [1] INVITE contains valid Identity header 11

Figure 6. Case-1b – [1] INVITE contains no Identity header 12

Figure 7. Case-1c – [1] INVITE contains invalid Identity header 13

Figure 8. Case-2a – [1] INVITE contains valid Identity header 14

Figure 9. Case-2b – [1] INVITE contains no Identity header 15

Figure 10. Case-2c – [1] INVITE contains invalid Identity header 16

Figure 11. Case-3a – [1] INVITE contains valid Identity header 17

Figure 12. Case-4a – [1] INVITE contains valid Identity header 18

Figure 13. Case-4b – [1] INVITE contains no Identity header 19

Figure 14. Case-4c – [1] INVITE contains invalid Identity header 20

**Table of Tables**

Table 1 – SIP-PBX cases 10

# Scope & Purpose

## Scope

This document describes how the PASSporT "div" extension defined in [draft-ietf-stir-divert] can be utilized within the SHAKEN framework to provide end-to-end SHAKEN authentication for calls that are retargeted by features such as call-forwarding.

## Purpose

The SHAKEN authentication service in an originating network asserts two telephone numbers in the PASSporT token; the number identifying the originator of the call in the "orig" claim, and the number identifying the destination of the call in the "dest" claim. The originating number is included to cryptographically assert that the calling TN identifies the calling user. The destination TN is included to provide protection from replay attacks where a man-in-the-middle replays a valid Identity header in a new INVITE sent to a different destination TN. In addition, PASSporT contains an "iat" claim that specifies the timestamp that the PASSporT was created. Including the "iat” claim further limits the time associated with a potential replay of the specific "orig" and "dest" claims, to prevent a potential malicious flood of validated calls to the same destination TN.

There are a number of call features that can legitimately retarget an INVITE request to a new destination. Examples include the various forms of call forwarding, where a call is diverted from the original destination to a new forward-to destination, simultaneous ringing, where a call to the dialed TN is simultaneously offered to additional TN(s), and toll-free number routing, where the dialed toll-free TN is replaced with its assigned routing TN. These features break the end-to-end call authentication model of SHAKEN/STIR since the verification service in the terminating network is unable to distinguish between an INVITE that has been legitimately retargeted, and an INVITE that has been maliciously replayed within the "iat" freshness window.

This document describes how the mechanisms defined in [draft-ietf-stir-passport-divert] enable SHAKEN to authenticate each retargeted leg of the call, so that a terminating network verification service has sufficient information to distinguish between an INVITE that has been legitimately retargeted, and an INVITE that has been maliciously replayed within the "iat" freshness window.

### Document Organization

Section 4 provides an informative overview of the replay attack window that exists within the base SHAKEN framework, and describes how the PASSporT "div" extensions can be used to close the window.

Section 5 specifies the normative requirements to add support draft-ietf-stir-passport-divert to SHAKEN.

Appendix A describes how the normative requirements in Section 5 can be applied to a sample of real-world deployment use cases.

# Normative References

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

RFC 8225, *Personal Assertion Token.*[[1]](#footnote-1)

RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*1

RFC 8226, *Secure Telephone Identity Credentials: Certificates.*1

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

draft-ietf-stir-passport-shaken, *PASSporT Extension for Diverted Calls.*

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

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

RFC 5806, *Diversion Indication in SIP*.

RFC 7044, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*.

# 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> >.

## Definitions

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| 3GPP | 3rd Generation Partnership Project |
| ATIS | Alliance for Telecommunications Industry Solutions |
| CSCF | Call Session Control Function |
| 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 | Persona 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 |
| 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 |

# Overview

The baseline SHAKEN framework and the core STIR protocols from which SHAKEN is based support the end-to-end call authentication for the common 2-way call scenario where user-a calls user-b. For this case, the originating network generates a PASSporT token containing "orig", "dest" and "iat" claims to assert that the calling telephone number (TN) is authorized to be used as the originating identity for that specific call. The terminating network can then verify that the PASSporT signature is valid, and that the "dest" claim matches the target called TN, to determine with a high degree of certainty that the calling TN identifies the calling user.

However, for call scenarios where a call is retargeted, the verification process becomes less certain due to the fact that the PASSporT "dest" claim may no longer match the target called TN. Based only on the SHAKEN Identity header from the first leg of the call, the verification service is unable to validate the associated changed telephone destinations. This document presents the solution for extending the SHAKEN framework to support these call retargeting scenarios.

draft-ietf-stir-passport-divert defines a PASSporT extension, "div", as a basis for accommodating the retargeting that may occur for various SIP applications. The “div” PASSporT provides an indication that the original called number in the “shaken” PASSporT no longer reflects the destination to which a call is likely to be delivered.

When an INVITE is retargeted, the "div" PASSporT extension enables an STI-AS to authenticate the TN of the retargeting entity. Therefore, when a retargeted INVITE request arrives at its final destination, a verification service (STI-VS) can use the received "div" PASSporT authentication information to verify the identity of each entity that retargeted the INVITE.

The basic “div” PASSporT operation is illustrated in Figure 1 for the call scenario where a call from TN-a to TN-b is forwarded to TN-c (TNs a/b/c are assigned to SP-a, SP-b and SP-c, respectively). The STI-AS authentication service in SP-a adds a "shaken" PASSporT as specified by [shaken], where the “orig” and “dest” claims contain the calling and called TNs. When the call is forwarded, the SP-b authentication service adds a “div” PASSporT as specified in [draft-ietf-stir-passport-divert], where the “orig” claim matches the “shaken” PASSporT “orig” claim (TN-a), the “dest” claim contains the forward-to TN (TN-c), and the “div” claim contains the TN of the forwarding entity (TN-b). When the INVITE arrives at SP-c, the STI-VS performs both shaken and “div authentication procedures. This includes verifying that there is an unbroken chain of authority from the INVITE Request-URI TN to the shaken “dest” claim.



Figure 1. Using "div" PASSporT to authenticate the forwarding leg of call

What follows in this document is the specification of how the PASSporT "div" extension shall be used as part of the SHAKEN framework for providing end-to-end SHAKEN validation for diverted calls.

# Normative Requirements

This section contains the normative requirements to enable the end-to-end delivery of SHAKEN authentication information for diverted calls.

## STI-AS Base SHAKEN Authentication Assumptions

This document assumes that the base SHAKEN authentication procedures defined in [shaken] require the STI-AS to populate the "shaken" PASSporT "dest" claim with the canonicalized value of the Request-URI TN, and not the To header TN.

## STI-VS Base SHAKEN Verification Assumptions

On receiving an INVITE request containing an Identity header with a “shaken” PASSporT and no Identity headers with a “div” PASSporT, the STI-VS will perform the base SHAKEN verification procedures as defined in [shaken]. This document assumes that as part of base SHAKEN verification, the STI-VS will use the canonical value of the Request-URI TN, and not the To header TN, as the locally created "dest" claim used during PASSporT signature verification.

## STI-AS "div" Authentication

The STI-AS shall provide "div" authentication services as defined in [draft-ietf-stir-passport-divert], with the following restrictions:

* The requirement that the INVITE request must contain at least one Identity header is modified here to mandate that the INVITE contains at least one Identity header with a “shaken” PASSporT,
* The "orig", "dest" and "div" claims shall be of type "tn",
* The "orig" claim value shall be copied from the “shaken” PASSporT "orig" claim,
* The "opt" claim shall not be used (no nesting).

Note that per draft-ietf-stir-passport-div, the "div" authentication service is not required to check for an unbroken chain of authority from the "shaken" PASSporT "dest" TN to the TN of the retargeting entity before authenticating the current retargeting event. As long as the "div" authentication service is authoritative for the TN of the retargeting entity, then it simply adds a "div" PASSporT token. Any breakage in the chain of authority between a "shaken" PASSporT "dest" claim and a Request-URI TN will be detected by the remote verification service in the terminating network to which the request was retargeted.

## STI-VS "div" Verification

On receiving an INVITE request containing an Identity header with a “shaken” PASSporT token, and one or more Identity headers with “div” PASSporT tokens, an STI-VS shall perform the “div” verification procedures defined in [draft-ietf-stir-passport-divert], with the following restrictions:

* The "div" PASSporT "orig", "dest" and "div" claims must be of type “tn”,
* The "div" PASSporT "opt" claim must be absent.

The STI-VS shall verify the “shaken” Identity header as defined in [shaken], and in addition, shall verify that the "div" PASSporT token(s) create an unbroken chain of authority from the "shaken" PASSporT "dest" claim to the canonicalized value of the INVITE Request-URI TN. If verification of the “shaken” PASSporT token fails using the P-Asserted-Identity header TN, and the canonicalized value of the TNs in the From and P-Asserted-Identity headers are different, then the STI-VS shall retry the verification procedure using the From header TN.

Editor’s Note: determine whether to keep the process of retrying with From.

## In-network Call Diversion

The STI-AS shall perform "div" authentication as specified in section 5.3 for in-network call diversion; i.e., where an in-network call feature or routing function retargets an INVITE request by updating the canonical value of the TN contained in the Request-URI of an INVITE request. As specified in [draft-ietf-stir-passport-divert], an authentication service adds an Identity header containing a "div" PASSporT token only if the SIP request contains at least one Identity header field. Therefore, if the retargeted INVITE request does not contain an Identity header, the STI-AS may choose to either skip authentication altogether, or to perform authentication based on local policy; e.g., perform base SHAKEN authentication with Gateway attestation.

If an originating SP retargets an INVITE request containing an Identity header with a “shaken” PASSporT, and the originating SP has authority over the "orig" claim in the "shaken" PASSporT, then instead of performing "div" authentication, the originating SP may choose to perform base SHAKEN authentication, and replace the existing Identity header with a new "shaken" Identity header that reflects the new destination.

## End-user Device Call Diversion

Certain types of end-user devices such as SIP-PBXs are capable of diverting incoming calls received from the host SP to a new destination in the global network. The end-user device diverts the call either by redirecting the incoming INVITE request with a 302 Moved Temporarily response, or by retargeting the incoming INVITE request to establish the divert-to call leg. The requirements in this section apply to the case where device capabilities and service provider policies enable the end-user device to divert calls using either of these mechanisms.

### Call Diversion by Redirecting the INVITE Request

If host SP policies allow the end-user device to divert calls via redirection, then the host SP shall consume the 302 response, and retarget the INVITE request on behalf of the end-user device. The SP STI-AS shall perform "div" authentication for the retargeting event before sending the INVITE to the new destination.

### Call Diversion by Retargeting the INVITE Request

The STI-AS provides authentication services for INVITE requests received from an end-user device. When the request is a retargeted INVITE, the type of authentication performed will depend on the capabilities of the end-user device, and the policies of the host SP in how it uses information in retargeted INVITE requests to provide SHAKEN authentication information to downstream entities.

During terminating call processing of an inbound INVITE request destined for an end-user device, the terminating host SP STI-VS shall verify the Identity header(s) contained in the terminating INVITE request as specified by [shaken], and in section 5.4 of this document. The host SP shall convey the verification results in the INVITE request sent to the end-user device using the tel URI "verstat" parameters, as specified in [3gpp TS 24.229]. If allowed by local policy, the terminating SP shall not remove the Identity headers from the INVITE request sent to the end-user device.

When the host SP receives an INVITE request from the end-user device, the STI-AS shall provide authentication services based on the contents of the request. If the information contained in the INVITE request indicates that the request has been retargeted by the end-user device, and the INVITE contains an Identity header with a SHAKEN PASSporT token, then the STI-AS shall perform “div” authentication as specified in section 5.3. The criteria used to determine that an INVITE request has been retargeted by an end-user device shall be based on the capabilities of the end-user device, and the policies of the host SP. For example, an SP could apply the following criteria to determine that an INVITE has been retargeted:

* The INVITE is received from a device that is capable of and allowed to retarget INVITEs,
* Local policy dictates that Identity headers are included in inbound INVITE requests sent to the end-user device,
* The received INVITE contains one or more instances of a SIP header that indicates retargeting has occurred (e.g., Diversion, History-Info, Referred-By), and the instance of the header that identifies the retargeted entity contains a TN that the end-user device is authorized to use, based on the full attestation criteria defined by [shaken].

If the received INVITE contains information that indicates it was retargeted internally by the end-user device before being retargeted to an externally assigned TN (i.e., the INVITE was retargeted multiple times), then the STI-AS shall perform "div" authentication in order to create an unbroken chain of authority from the "shaken" PASSporT "dest" claim to the final retargeted TN (the Request-URI TN). The STI-AS can do this either by performing "div" authentication for each retargeting event, or by performing "div" authentication for a single retargeting event that links the SHAKEN "dest" claim to the Request-URI TN.

If the information contained in an INVITE request received from an end-user device indicates that the request has not been retargeted, then the STI-AS shall remove any Identity headers contained in the request and perform base SHAKEN authentication as defined in [shaken].

If the information contained in an INVITE request received from an end-user device indicates that the request has been retargeted, but the request does not contain an Identity header, then the STI-AS shall perform base SHAKEN authentication as defined in [shaken].

1. **Authentication of End-user Device Retargeted Calls**

Implementation of the normative procedures for authentication of in-network INVITE retargeting cases (section 5.5) is relatively straightforward, since the STI-AS of the retargeting network has direct access to the information it needs to perform “div” authentication for the retargeted leg of the call. The situation for end-user device INVITE retargeting (section 5.6.2) is somewhat more complex, since variations in SIP-PBX implementations mean that the STI-AS has to support a wider range of use cases in terms of the varying levels of information made available to the authentication service in the retargeted INVITE request. Therefore, this appendix provides information that shows how the generic requirements in section 5.6.2 can be applied to different end-user device retargeting use cases.

The information in this appendix is not normative. Also, this section does not address the entire set of end-user device retargeting scenarios that could be encountered in real-world deployments, but is meant to serve as an example of how a service provider can support SHAKEN within the limits of operator policies and end-user device capabilities.

* 1. ***STI-AS Procedures***

As shown in Figure 2, the procedures performed by the STI-AS to authenticate an INVITE retargeting event depend on the capabilities of the retargeting entity, and specifically on the information provided by the retargeting entity to the STI-AS in the retargeted INVITE. Figure 2 illustrates the type of scenarios that the STI-AS is required to support, where an originating [1] INVITE request could be retargeted by one of three different retargeting entities; an in-network Application Server or end-user device-1 that convey the received Identity header in the retargeted [2] INVITE, or an end-user device-2 that does not convey the received Identity header in the retargeted [4] INVITE.

On receiving [2] INVITE from the in-network AS, or from end-user device-1, the STI-AS uses information such as the presence and contents of the Diversion, From, and Identity headers, and the contents of the Request-URI, to determine that an INVITE from TN-a to TN-b has been legitimately retargeted to TN-c. Since the retargeted INVITE contains a SHAKEN Identity header, the STI-AS performs “div” authentication for the TB-b🡪TN-c leg of the call, and adds a second Identity header containing the “div” PASSporT in [3] INVITE sent to SP-c.

However, for the case where the STI-AS receives [4] INVITE from end-user device-2, the STI-AS knows that the INVITE has been retargeted, but it cannot perform “div” authentication because [4] INVITE does not contain a SHAKEN Identity header. Therefore, the STI-AS performs SHAKEN authentication based on the information that it does have; i.e., that a TN-a is calling TN-c. Since SP-b has no relationship with the originator of the call, it asserts an attestation level of Gateway in the “shaken” PASSporT. The STI-AS includes the resulting SHAKEN Identity header in [5] INVITE to SP-c.



Figure 2. STI-AS Authentication Examples

Figure 3 provides an overview of the logic applied by the STI-AS to determine whether “shaken”” or “div” authentication is performed for an INVITE request received from an end-user device (CPE).

1. If the CPE device is not able or allowed to retarget INVITE requests, then the STI-AS performs “shaken” authentication (else continue).
2. A CPE that is allowed to retarget calls may provide sufficient information in INVITE requests to enable the STI-AS to distinguish between originating and retargeted requests; e.g., the CPE includes a Diversion header identifying the TN of the retargeting entity if and only if the INVITE is retargeted. Therefore, if the STI-AS is able to explicitly identify that the INVITE is “originating”, or if the STI-AS cannot distinguish between originating and retargeted INVITEs from this CPE, then it performs “shaken” authentication (else continue).
3. If the CPE is not able or allowed to convey Identity header(s) in retargeted INVITE requests, then then the STI-AS performs “shaken” authentication (else continue).
4. If the INVITE request contains an Identity header then the STI-AS performs “div” authentication; otherwise it performs “shaken” authentication.



Figure 3. STI-AS logic to determine authentication procedures for INVITE from CPE

* 1. ***End-user Device Retargeting Examples***

The message sequence diagrams in this section use the template shown in Figure 4, where an inbound call from TN-a to TN-b is forwarded to TN-c. TN-a, TN-b, and TN-c are hosted by SP-a, SP-b, and SP-c respectively. SP-b has delegated TN-b to SIP-PBX-1. SIP-PBX-1 supports call forwarding by INVITE retargeting, where inbound [2] INVITE to TN-b is retargeted to [3] INVITE to forward-to TN-c.



Figure 4. Message sequence diagram template

This section describes the SHAKEN procedures for four different SIP-PBX use cases that vary based on the PBX’s ability to convey SHAKEN authentication information from inbound [2] INVITE to retargeted [3] INVITE. These four SIP-PBX cases are summarized in Table-1.

Table 1 – SIP-PBX cases



Three different scenarios are documented for each SIP-PBX case. The scenarios differ based on the SHAKEN authentication information added by SP-a to [1] INVITE, as follows:

1. INVITE contains a valid SHAKEN Identity header
2. INVITE contains no Identity header
3. INVITE contains an invalid Identity header

(Note, the following sub-sections use the term "PAID" to refer to the P-Asserted-Identity header.)

* + 1. ***Case-1: Identity/PAID/From conveyed in retargeted INVITE***

**SP-b policy**:

* Include received Identity headers in inbound [2] INVITE requests sent to SIP-PBX-1
* Trust P-Asserted-Identity header received in retargeted [3] INVITE requests from SIP-PBX-1

**SIP-PBX-1 capabilities:**

* When inbound [2] INVITE is retargeted, SIP-PBX-1 populates retargeted [3] INVITE with Identity, P-Asserted-Identity and From headers from [2] INVITE.

**Case-1a: Originating [1] INVITE contains valid SHAKEN Identity header**

On receiving [1] INVITE in Figure 5, SP-b STI-VS verifies that the received SHAKEN Identity header is valid. SP-b includes the Identity header and a “TN-Verification-Passed” indication in [2] INVITE to SIP-PBX-1. On receiving [3] INVITE from SIP-PBX-1, SP-b detects that a previous inbound INVITE to SIP-PBX-1 has been retargeted by the presence of the Diversion header. Since [3] INVITE contains an Identity header, the STI-AS performs normal “div” authentication, adds a second Identity header containing the “div” PASSporT, and routes [4] INVITE to SP-c.



Figure 5. Case-1a – [1] INVITE contains valid Identity header

**Case-1b: Originating [1] INVITE contains no Identity header**

On receiving [1] INVITE in Figure 6, SP-b STI-VS skips verification since there is no Identity header. Based on local policy, SP-b STI-AS performs authentication for calling TN-a, and adds a SHAKEN Identity header with an attestation level of "Gateway" to [2] INVITE. On receiving [3] INVITE from SIP-PBX-1, SP-b STI-AS performs normal “div” authentication, adds a second Identity header containing the “div” PASSporT, and routes [4] INVITE to SP-c.

As an alternative, SP-b could choose not perform SHAKEN authentication on [1] INVITE, in which case [2] INVITE to SIP-PBX-1 would not contain an Identity header. In this case, SP-b would perform SHAKEN authentication on [3] INVITE (since it doesn’t contain a SHAKEN Identity header), and include a single SHAKEN Identity header for calling TN-a with "Gateway" attestation in [4] INVITE to SP-c.

The first option, where SP-b authenticates [1] INVITE, has a slight advantage in that SP-b assigns a "shaken" PASSporT "origid" claim that could be used during subsequent trace-back activity to identify the ingress gateway that received [1] INVITE, and possibly identify originating SP-a. Ultimately, the option selected is a policy decision for SP-b.



Figure 6. Case-1b – [1] INVITE contains no Identity header

**Case-1c: Originating [1] INVITE contains invalid Identity header**

On receiving [1] INVITE in Figure 7, SP-b STI-VS verification service produces a failure result (PASSporT signature validation fails since "orig" claim does not match the calling TN in the P-Asserted-Identity header). SP-b sends the invalid Identity header in [2] INVITE to SIP-PBX-1. On receiving retargeted [3] INVITE from SIP-PBX-1, SP-b STI-AS performs “div” authentication, and adds a second Identity header containing a “div” PASSporT to [4] INVITE. Verification fails at SP-c, and a “TN-Validation-Failed” indication is delivered to UE-c in [5] INVITE.



Figure 7. Case-1c – [1] INVITE contains invalid Identity header

* + 1. ***Case-2: Identity conveyed in retargeted INVITE, but not PAID/From***

**SP-b policy**:

* Include received Identity headers in inbound [2] INVITE requests sent to SIP-PBX-1

**SIP-PBX-1 capabilities:**

* SIP-PBX-1 populates retargeted [3] INVITE with Identity header from [2] INVITE, and with P-Preferred-Identity and From headers containing TN of retargeting entity (TN-b). P-Asserted-Identity from [2] INVITE is discarded.
* SIP-PBX does not include Diversion header in retargeted INVITE requests.

**Case-2a: Originating [1] INVITE contains valid SHAKEN Identity header**

On receiving [1] INVITE in Figure 8, SP-b STI-VS verifies that the received SHAKEN Identity header is valid, and includes the Identity header and “verification passed” indication in [2] INVITE to SIP-PBX-1. On receiving [3] INVITE from SIP-PBX-1, SP-b detects that a previous inbound INVITE to SIP-PBX-1 has been retargeted by the presence of the SHAKEN Identity header. SP-b STI-AS performs normal “div” authentication, adds a second Identity header containing the “div” PASSporT, and routes [4] INVITE to SP-c.

Normally, SP-b would assert the identity (TN-b) received in the P-Preferred-Identity header of [3] INVITE in the P-Asserted-Identity header of [4] INVITE to SP-c. However, this would result in a verification failure at SP-c, since the “shaken” PASSporT “orig” claim would not match the P-Asserted-Identity TN. Therefore, before sending [4] INVITE, SP-b will update the P-Asserted-Identity header to identify calling TN-a (i.e., the TN from the “shaken” PASSporT “orig” claim).



Figure 8. Case-2a – [1] INVITE contains valid Identity header

**Case-2b: Originating [1] INVITE contains no Identity header**

On receiving [1] INVITE in Figure 9, SP-b STI-VS skips verification since there is no Identity header. Based on local policy, SP-b STI-AS performs authentication for calling TN-a, and adds a SHAKEN Identity header with an attestation level of Gateway to [2] INVITE. On receiving [3] INVITE from SIP-PBX-1, SP-b STI-AS performs normal “div” authentication, adds a second Identity header containing the “div” PASSporT, and routes [4] INVITE to SP-c. As in Case-1a, SP-b updates the P-Asserted-Identity with calling TN-a.

As an alternative, SP-b could choose not perform SHAKEN authentication on [1] INVITE, in which case [2] INVITE to SIP-PBX-1 would not contain an Identity header. In this case, SP-b would perform SHAKEN authentication on [3] INVITE, and include a single SHAKEN Identity header for calling TN-b with Full attestation in [4] INVITE to SP-c.



Figure 9. Case-2b – [1] INVITE contains no Identity header

**Case-2c: Originating [1] INVITE contains invalid Identity header**

On receiving [1] INVITE in Figure 10, SP-b STI-VS verification service produces a failure result (PASSporT signature validation fails since "orig" claim does not match the calling TN in the P-Asserted-Identity header). There are multiple ways SP-b could handle this case. Here are two possible options:

1. As shown in Figure 10, SP-b replaces the invalid Identity header with a valid Identity header in [2] INVITE that authenticates calling TN-a with Gateway attestation. When it receives [3] INVITE, SP-c adds a second Identity header containing a “div” PASSporT token. In this case, verification of [4] INVITE would pass at SP-c, but since attestation is “Gateway”, a verification result of “No-TN-Validation” would be sent to UE-c.
2. SP-b removes the invalid Identity header from [2] INVITE sent to the SIP-PBX, and then adds a SHAKEN Identity header authenticating calling TN-a with “Gateway” attestation on receiving [3] INVITE. As with option-1, this would provide a “No-TN-Validation” result to UE-c.

Note: For Case-2c, SP-b does not send the invalid Identity header in [2] INVITE to SIP-PBX-1. The reason for this is that SP-b would be unable to distinguish between the resulting [3] INVITE request for this Case-2c, and the [3] INVITE for Case-2a. In order for Case-2a to work as described, SP-b assumes that the received Identity header in [3] INVITE is valid, and that the PASSporT "orig" claim identifies that calling TN. Sending an invalid Identity header in [2] INVITE for Case-2c would break this assumption.



Figure 10. Case-2c – [1] INVITE contains invalid Identity header

* + 1. ***Case-3: PAID/From conveyed in retargeted INVITE, but not Identity***

**SP-b policy**:

* Do not include received Identity headers in inbound [2] INVITE requests sent to SIP-PBX-1.

**SIP-PBX-1 capabilities:**

* SIP-PBX-1 does not populate [3] INVITE with an Identity header, either because it did not receive one from host SP, or because it doesn’t convey Identity headers in retargeted INVITE requests.
* SIP-PBX-1 populates [3] INVITE with the P-Asserted-Identity and From headers received in [2] INVITE.

**Case-3a: Originating [1] INVITE contains valid SHAKEN Identity header**

On receiving [1] INVITE in Figure 11, SP-b STI-VS verifies that the received SHAKEN Identity header is valid, and therefore includes a “TN-Validation-Passed” indication in [2] INVITE to SIP-PBX-1. Per local policy, SP-b does not include the received Identity header in [2] INVITE to the SIP-PBX. On receiving [3] INVITE from SIP-PBX-1, SP-b STI-AS performs SHAKEN authentication for calling TN-a with Gateway attestation, and adds the resulting Identity header to [4] INVITE to SP-c. On receiving [4] INVITE, SP-c STI-VS verifies the received Identity header (result is valid with Gateway attestation), and sends an indication of “No-TN-Validation” to UE-c.

****

Figure 11. Case-3a – [1] INVITE contains valid Identity header

**Case-3b/3c: Originating [1] INVITE contains no/invalid Identity header**

The procedure for Case-3b/3c is the same as Case-3a, except that for Case-3b, SP-b skips verification of [1] INVITE and sets the verification result indication in [2] INVITE to “No-TN-Validation”, while for Case-3c, verification of [1] INVITE fails and SP-b sets verification result indication in [2] INVITE to “TN-Validation-Failed”.

* + 1. ***Case-4: Retargeted INVITE does not convey Identity/PAID/From***

**SP-b policy**:

* Do not include received Identity headers in inbound [2] INVITE requests sent to SIP-PBX-1

**SIP-PBX-1 capabilities:**

* SIP-PBX-1 does not populate [3] INVITE with an Identity header, either because it did not receive one from host SP, or because it doesn’t convey Identity headers in retargeted INVITE requests.
* SIP-PBX-1 populates retargeted [3] INVITE with P-Preferred-Identity and From headers containing TN of retargeting entity. SIP-PBX-1 does not include the P-Asserted-Identity header from [2] INVITE in the [3] INVITE request.
* SIP-PBX does not include Diversion header in retargeted INVITE requests.

**Case-4a: Originating [1] INVITE contains valid SHAKEN Identity header**

On receiving [1] INVITE in Figure 12, SP-b STI-VS verifies that the received SHAKEN Identity header is valid, and includes a “TN-Validation-Passed” indication in [2] INVITE to SIP-PBX-1. Per local policy, SP-b does not include the received Identity header in [2] INVITE to the SIP-PBX. On receiving [3] INVITE from SIP-PBX-1, SP-b STI-AS performs SHAKEN authentication for calling TN-b with Full attestation, and adds the resulting Identity header to [4] INVITE to SP-c. On receiving [4] INVITE, SP-c STI-VS verifies the received Identity header (result is valid with Full attestation), and sends an indication of “TN-Validation-Passed” to UE-c.

****

Figure 12. Case-4a – [1] INVITE contains valid Identity header

**Case-4b: Originating [1] INVITE contains no Identity header**

As shown in Figure 13, the procedure for Case-4b is the same as Case-4a, except that SP-b sets the verification result indication in [2] INVITE to “No-TN-Validation”.



Figure 13. Case-4b – [1] INVITE contains no Identity header

**Case-4c: Originating [1] INVITE contains invalid Identity header**

As shown in Figure 14, the procedure for Case-4c is the same as Case-4a, except that SP-b sets the verification result indication in [2] INVITE to “TN-Validation-Failed”.



Figure 14. Case-4c – [1] INVITE contains invalid Identity header

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