**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 4

5.1 STI-AS Base SHAKEN Authentication 4

5.2 STI-AS Base SHAKEN Verification 4

5.3 STI-AS "div" Authentication 4

5.4 STI-AS "div" Verification 4

5.5 In-network Call Diversion 4

5.6 End-user Device Call Diversion 5

5.6.1 Call Diversion via 302-Response 5

5.6.2 Call Diversion by Retargeting the INVITE Request 5

6 Appendix A 7

6.1 Overview of diverted calls and the impact to SHAKEN end-to-end call authentication 7

6.2 SHAKEN support of "div" PASSporT for in-network call diversion 9

6.3 SHAKEN support of "div" PASSporT for end-user device call diversion 10

6.3.1 SHAKEN functional requirements for call diverted by SIP-PBX 10

6.3.2 Call-Forwarding Procedures 11

6.3.3 Adding "div" PASSporT when SIP-PBX diverts call via 3xx Response 11

6.3.4 Adding "div" PASSporT when SIP-PBX diverts call via new-INVITE Request 12

**Table of Figures**

Figure 1. Replayed INVITE looks like a legitimately diverted INVITE 8

Figure 2. "div" PASSporT enables end-to-end authentication of legitimately diverted calls 9

Figure 3. Multiple Diversion Example: TN-a calls TN-b fwd🡪 TN-c fwd🡪 TN-d 10

Figure 4. Support of "div" PASSporT when SIP-PBX diverts call with 3xx-response 11

Figure 5. Support for PBX divert via new-INVITE; forwarding TN authority based on SHAKEN full-attestation criteria 13

**Table of Tables**

**No table of figures entries found.**
In your document, select the words to include in the table of contents, and then on the Home tab, under Styles, click a heading style. Repeat for each heading that you want to include, and then insert the table of contents in your document. To manually create a table of contents, on the Document Elements tab, under Table of Contents, point to a style and then click the down arrow button. Click one of the styles under Manual Table of Contents, and then type the entries manually.

# Scope & Purpose

## Scope

This document extends SHAKEN to support the PASSporT "div" extension defined in draft-ietf-stir-passport-divert.

## Purpose

The base STIR/SHAKEN replay-attack detection mechanisms are unable to distinguish between a legitimate call that is diverted by a feature such as call-forwarding, and a malicious call where the attacker attempts to masquerade as another user by replaying a legitimate To, From and Identity header within the Date freshness window. This document describes how draft-ietf-stir-passport-divert can be used to close this replay attack 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 draft-ietf-stir-passport-divert to SHAKEN.

# 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.

ATIS-0x0000x, *Technical Report*.

ATIS-0x0000x.201x, *American National Standard*.

# 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

**AAA**: xxxx.

**Bbbb**: xxxx.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions |

# 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.

The "div" extension enables a forwarding network to dynamically authenticate the forwarding TN that is diverting the call to a new "dest" TN as a call progresses. A terminating verification service (STI-VS) can then use this additional information to verify the associated TNs at each diversion of a call between the final destination TN and initial original destination TN.

[Editorial note: overall terminology needs to be consistent with SIP defined retargeting and draft-ietf-stir-passport-divert –the latter uses “retarget” and the “entity that’s doing the retargeting” (i.e., “the TN is not diverting the call”). The use of the word “divert” throughout this contribution is introducing new terminology that’s not consistent with SIP retargeting in general. Note, that draft-ietf-stir-passport-divert only uses the terms “divert” in the title and the abstract. The cases where a “div” PASSporT is added to the SIP INVITE is based on the “mp” type of retargeting as defined in RFC 7044 – i.e., “mp” is the case where the target user changes to an AOR(TN) unassociated with the AOR(TN) of the original target user.]

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 diverting TN before authenticating the current diversion event. As long as the "div" authentication service is authoritative for the diverting TN, then it simply adds a "div" PASSporT token containing the following claims:

* "orig" claim matches the "shaken" PASSporT "orig" claim,
* "div" claim matches the diverting TN,
* "dest" claim matches the Request-URI TN.

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 a “shaken” Identity header and one or more “div” Identity headers, 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.

## 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.

#### Delivering End-to-End SHAKEN Authentication when INVITE is Retargeted

The requirements in this section apply when the following criteria exist:

1. The end-user device uses INVITE retargeting to divert incoming calls,
2. As part of call diversion, the end-user device copies any Identity headers contained in the incoming INVITE request to the retargeted INVITE request, and
3. Host SP policies dictate that calls diverted by the end-user device provide the same user experience as calls diverted by an in-network application server; i.e., the calling identity and SHAKEN verification results displayed to the called user reflect the calling TN and SHAKEN authentication information asserted by the originating network.

During terminating call processing, the terminating 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. If allowed by local policy, the terminating SP shall not remove the Identity headers from the INVITE request sent to the end-user device. This requirement is extended and modified for the following cases:

* If the terminating INVITE request does not contain a SHAKEN Identity header, the terminating SP may add a SHAKEN Identity header before sending the INVITE request to the terminating end-user device. The attestation level of this added SHAKEN Identity header will be based on local policy; e.g., Gateway attestation to reflect the fact that the host SP does not have authority over the calling TN.

Note: adding a SHAKEN Identity header in the above case enables the host SP to detect if this INVITE request is subsequently retargeted by the end-user device.

* If the terminating INVITE request contains a Privacy header with a priv-value token of "id", then the host SP shall either remove the Identity headers, or convert all full form PASSporT tokens to compact form before sending the INVITE request to the terminating end-user device.

Note: the above requirement avoids revealing the identity of the calling user contained in the PASSporT “orig” claim to the end-user device. Choosing to send the compact form has the advantage that it enables the host SP to detect if this INVITE request is subsequently retargeted by the end-user device.

On receiving an INVITE request from an end-user device that supports INVITE retargeting, the STI-AS of the host SP shall perform "div" authentication as specified in section 5.3 if the following conditions exist:

1. The INVITE request contains an Identity header with a full form "shaken" PASSporT token, and zero or more "div" Identity headers, and
2. The end-user device is authorized to use the diverting TN, based on the SHAKEN authentication criteria for applying full attestation defined in [shaken].

How the STI-AS identifies the diverting TN will depend on the SIP profile supported by the end-user device and the host SP network. For example, for IMS-compliant networks, the diverting TN is asserted by the P-CSCF in the P-Asserted-Identity header. In this case, before sending the INVITE request to the next hop, the STI-AS shall update the P-Asserted-Identity header to match the "orig" claim in the "shaken" Identity header.

If either of the above conditions do not exist, then the STI-AS of the host SP shall perform the base SHAKEN authentication procedures defined in [shaken].

#### Support of SHAKEN for other End-User Device INVITE Retargeting Scenarios

This specification places no normative requirements on the support of SHAKEN for end-user device retargeting cases that fall outside the criteria listed in section 5.6.2.1; e.g., cases where the end-user device does not copy Identity headers from incoming to retargeted INVITE requests, or where host SP policies dictate that all Identity headers are removed from INVITE requests sent to the end-user device. In these cases, the SHAKEN authentication information added by the originating and other upstream networks is lost as the call traverses the retargeting end-user device. Therefore, the SHAKEN authentication information provided in the retargeted INVITE request sent to downstream entities by the host SP is based solely on the output of the authentication procedures performed by the host SP’s STI-AS, and as governed by the policies of the host SP.

For example, the host SP could choose to treat a retargeted INVITE request from the end-user device the same as an originating INVITE request, and perform SHAKEN authentication for the retargeting TN assigned to the end-user device. As a result, the calling identity and SHAKEN verification results information displayed to the called user would be associated with the retargeting TN, and not the actual calling TN asserted by the originating network.

Or, if the end-user device supports a profile of SIP that enables the host SP to detect when an INVITE has been retargeted, and to explicitly identify the calling and retargeting TNs in the retargeted INVITE, then the host SP could choose to perform SHAKEN authentication on the originating TN and “div” authentication for the retargeting TN. In this case, the called user display would show the calling TN and SHAKEN verification results associated with the actual caller, but based on information provided by the SP hosting the retargeting end-user device.

Ultimately, the treatment of these cases is based on the capabilities of the end-user device in conveying information about the calling and retargeting TNs to the host SP, and the policies of the host SP in how to use this information to provide SHAKEN authentication information to downstream entities.

# Appendix A

This Appendix provides background information the "div" PASSporT extension, and how it can enable end-to-end authentication of diverted calls.

Section 6.1 provides an overview of why SHAKEN needs an extension to support diverted calls.

Section 6.2describes how "div" PASSporT enables end-to-end call authentication when calls are diverted by a trusted in-network entity.

Section 6.3 describes how "div" PASSporT enables end-to-end call authentication for calls diverted by an untrusted end-user device.

## Overview of diverted calls and the impact to SHAKEN end-to-end call authentication

Based on the call authentication principles of SHAKEN, and specifically of PASSporT, in order for end-to-end call authentication to work properly, the SHAKEN authentication service in the originating network must both assert the telephone number identifying the originator of the call in the PASSporT "orig" claim, and specify the telephone number identifying the destination of the call in the PASSporT "dest" claim. The destination TN is included in the PASSporT token 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. In addition, PASSporT contains an "iat" claim that specifies the timestamp that the call was originated. 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.

A common SIP application functionality is to receive a call at the intended destination telephone number, and then retarget that call to another destination telephone number. This is generally referred to as call diversion, and is often used as part of a call-forwarding feature in a VoIP provider’s SIP application server or an end user’s SIP-PBX. Call diversion is also utilized by a number of other call scenarios in today’s telephone network; e.g., for features such as simultaneous ringing, where a call to the dialed TN is simultaneously offered to additional TN(s), and for toll-free number routing, where the dialed toll-free TN is replaced with its assigned routing TN.

Because call diversion inserts a new destination telephone number into the SIP INVITE without the explicit knowledge of the original calling party, this breaks the end-to-end call authentication model of SHAKEN/STIR. As a result, if not properly addressed, you could potentially have issues where a malicious entity may be able to utilize a call forwarding service to either inherit a valid call authentication or a valid entity may have the end-to-end call authentication broken because the original call authentication wasn’t applied to the resulting forwarded-to destination. Therefore, a specific solution is necessary to address the changed destination identity when a call is diverted.

To illustrate one of the potential vulnerabilities diversion presents into the SHAKEN call authentication framework, Figure 1 illustrates a man-in-the-middle replay attack window for the case where a malicious entity masquerades as another user by constructing an INVITE request that uses an Identity header from a legitimate call. The result of not specifying how diverted calls must be authenticated for every leg of the call enables the scenario illustrated in Figure 1, where the malicious call shown on the bottom of the figure is identical and indistinguishable from the legitimately forwarded/diverted call shown in the top of the figure.

 

Figure 1. Replayed INVITE looks like a legitimately diverted INVITE

Specifically, Figure 1 shows the initial INVITE message flow for a call from TN-a to TN-b that is forwarded to TN-c, where TN-a, TN-b and TN-c are served by SP-a, SP-b, and SP-c respectively. A malicious entity replays the To, P-Asserted-Identity and Identity headers in a new INVITE to called TN-x. Assuming the malicious user inserts a History-Info header corresponding to a “fake” forwarded call from TN-b to TN-x, the SHAKEN verification service is unable to distinguish between the legitimate [2] INVITE and the replayed [4] INVITE; they both pass the SHAKEN-defined verification tests. The fundamental issue is that the INVITE does not contain a PASSporT that proves the call was legitimately diverted from the original called TN identified in the To header field to a new destination TN identified in the Request-URI.

Corresponding to this scenario, a SHAKEN verification service that detects a valid SHAKEN PASSporT token where the PASSporT "dest" claim does not match the Request-URI TN, could result in interpretation of one of the following treatments:

* Treat as "verification passed” and incur the risk of providing a false-positive result, where a maliciously replayed INVITE is presented as "verification passed" to the called user.
* Treat as "verification failed” and incur the risk of providing a false-negative result, where a legitimately forwarded INVITE is presented as "verification failed" to the called user.

However, in order to avoid delivering a false-positive or false-negative indication to the called user, a baseline SHAKEN verification service must apply the flowing treatment:

* Treat as if no Identity header was received. The result is that SHAKEN is unable to deliver "verification passed" when an INVITE is legitimately forwarded or “verification failed” when an INVITE is maliciously retargeted within the "iat" freshness window, since neither condition can be determined or proven.

Call diversion, while not used in a large percentage of overall calls on a telephone network, is still significant and important for many telephone features, and ultimately needs to be addressed in the SHAKEN framework. The verification service behavior described above can be used temporarily for initial deployments of SHAKEN, with the goal of this document being to define the required extensions to SHAKEN to address end-to-end call authentication for call diversion.

There are two categories of call diversion applications that must be addressed. First is the case of in-network call diversion, where an application server that sits within a secure network domain applies call diversion. Second is the case end-user device call diversion, where an end user device such as a SIP-PBX, which is potentially in an untrusted domain, diverts a call back to the service provider network. The following two sections describe both of these categories of call diversion and how they apply to SHAKEN.

## SHAKEN support of "div" PASSporT for in-network call diversion

This section describes call authentication that would happen inside the trust domain of a service provider network. This general category of call features applied in the network corresponds to a relatively straightforward implementation of the “div” PASSporT extension to the SHAKEN framework.

As defined in draft-ietf-stir-passport-div, the “div” PASSporT extension defines a mechanism to provide a new PASSporT token at the point in the call where a diversion occurs.

Specific to SHAKEN, the first leg of the call is authenticated using the baseline SHAKEN Identity header containing a "shaken" PASSporT extension defined in draft-ietf-stir-passport-shaken as mandated by the SHAKEN framework. Each time a call is diverted, an additional Identity header will be added to the INVITE that follows the "div" PASSporT extension. Therefore, for diverted calls, there will be a single SHAKEN-based Identity header corresponding to the first leg of the call, and one or more "div" extension based Identity headers corresponding to each additional leg of the diverted call.

A "div" PASSporT token implicitly carries with it an attestation level of "Full Attestation” (using the “Full Attestation” semantics defined by SHAKEN). Therefore, an SP that adds a "div" Identity header is asserting with the strength indicated by "Full Attestation” that the diverting/forwarding TN is authorized to forward the call to the forward-to TN.

Figure 2 shows how the issue described in Figure 1 is resolved by the "div" PASSporT extension.



Figure 2. "div" PASSporT enables end-to-end authentication of legitimately diverted calls

As in Figure 1, Figure 2 shows the initial INVITE message sequence for a call from TN-a to TN-b that is forwarded to TN-c. Before forwarding the call, SP-b shall add a PASSporT "div" token to [2] INVITE to provide cryptographic proof that the call is being legitimately forwarded from TN-b to TN-c. Meanwhile, a malicious entity attempts to masquerade as TN-a by replaying the To, P-Asserted-Identity, Date and Identity headers from [2] INVITE into a new [4] INVITE to TN-x. The SHAKEN verification services in SP-c and SP-x can now distinguish between the legitimate call-forwarded call and the malicious call by verifying that the "shaken" and "div" PASSporT tokens provide an unbroken chain of authority between the final called TN identified in the Request-URI and the initial dialed TN identified in the "dest" claim of the "shaken" PASSporT token. In this example, the SHAKEN verification service in SP-x detects that the chain in [4] INVITE is broken, since the Request-URI TN does not match the “dest” claim in the “div” PASSporT token. As a result, SP-x includes a “fraud alert” indication in the [5] INVITE request to called UE-x.

An INVITE that is forwarded multiple times would have multiple "div" PASSporT tokens; one for each forwarded leg. The verification service that receives such an INVITE shall arrange the "div" PASSporT tokens in order, and verify the chain of authority from the Request-URI TN, through the multiple "div" PASSporT tokens to the "dest" TN in the "shaken" PASSporT token. Figure 3 illustrates the verification process for a multi-forwarding case, where TN-a calls TN-b, and the call is forward twice; first to TN-c, and then to TN-d.



 Figure 3. Multiple Diversion Example: TN-a calls TN-b fwd🡪 TN-c fwd🡪 TN-d

## SHAKEN support of "div" PASSporT for end-user device call diversion

This section describes how call authentication is supported when a call is diverted by an end-user device. (End-user devices that apply call diversion are typically SIP-PBX devices; therefore, we will refer to these devices using this term going forward.) A call leg diverted by a SIP-PBX can be authenticated using the "div" PASSporT extension, similar to the in-network call diversion cases described in section 4.2. If we were to apply the in-network procedures exactly, the diverting SIP-PBX would be responsible for adding the "div" PASSporT token. However, in order to speed up adoption, it would be preferable to have a solution that did not require the SIP-PBX to support "div" PASSporT. Therefore, the solution is designed such that host SP adds the "div" PASSporT token on behalf of the diverting SIP-PBX.

### SHAKEN functional requirements for call diverted by SIP-PBX

When a SIP-PBX applies call diversion, or more generally forwards a DID call, the calling number should be delivered to the forward-to service provider network. This calling number should correspond to the Identity header added by the SHAKEN authentication service in the originating network. For example, when a call is forwarded from a user’s office number to the user’s mobile number, the mobile phone should display both the actual calling number, and an accurate indication of the legitimacy of the calling number based on the SHAKEN verification results.

### Call-Forwarding Procedures

While there are many flavors of SIP-PBX devices that may act in slightly different ways, call diversion features are generally supported using similar procedures. The current prominent industry standard for SIP interworking between the SIP-PBX and its host service provider is SIPconnect 2.0. This document will therefore use SIPconnect 2.0 as the primary reference for describing how SHAKEN is supported for calls diverted by a SIP-PBX.

SIPconnect 2.0 defines two call-forwarding procedures for DID calls; the SIP-PBX can forward the call either by responding to the incoming INVITE request with a 302 Moved Temporarily response that redirects the call to the forward-to number, or by sending a new INVITE request to the forward-to number.

### Adding "div" PASSporT when SIP-PBX diverts call via 3xx Response

Figure 4 illustrates how "div" PASSporT can be utilized to provide end-to-end call authentication when a SIP-PBX diverts a DID call by sending a 302 Moved Temporarily response to the host SP to establish the forwarding leg of the call.



Figure 4. Support of "div" PASSporT when SIP-PBX diverts call with 3xx-response

**Figure 4 Message Sequence:**

1. SP-a performs SHAKEN authentication services for calling TN-a, and routes the call to SP-b.
2. On receiving [1] INVITE, SP-b verifies the SHAKEN PASSporT token, populates the P-Asserted-Identity header Verstat parameter with the "verification passed" result, and sends [2] INVITE to SIP-PBX-1.
3. SIP-PBX-1 responds to received [2] INVITE with [3] 302 Moved Temporarily response. The Contact header of the response contains the forward-to TN-c.
4. On receiving the 302-response, SP-b adds a 2nd Identity header to [4] INVITE containing a "div" PASSporT token that authenticates the forwarding leg of the call, and sends the [4] INVITE to SP-c.
5. On receiving [4] INVITE, SP-b verifies the received SHAKEN and "div" PASSporT tokens, populates the P-Asserted-Identity header Verstat parameter with the “verification passed” result, and sends [5] INVITE to UE-c. UE-c displays calling TN-a and a “verification passed” indication to the called user.

In order to add the "div" PASSporT token in step-4, SP-b must be authoritative for the forwarding TN identified in the "div" claim of the token (TN-b in this example). Fortunately, this will always be the case when a SIP-PBX diverts calls using a 3xx-response, since the SP that handles the 3xx-response is the same SP that routed the initial call leg to the SIP-PBX (i.e., by definition, the forwarding SP knows that the forwarding TN has been assigned to the SIP-PBX). This means that the message sequence shown in Figure 4 will support complex TN assignment cases where the SIP-PBX obtains TNs from multiple TN providers; e.g., SIP-PBX is assigned TNs from multiple host SPs, or toll-free TNs from a RespOrg, etc.

### Adding "div" PASSporT when SIP-PBX diverts call via new-INVITE Request

In this case, the host SP authenticates the forwarding (diverting) leg of a SIP-PBX call by adding an Identity header containing a "div" PASSporT token to the new-INVITE request that establishes the forward-to call leg. The host SP can do this only if it knows that the SIP-PBX is authorized to use the diverting TN. The host SP can establish the authority of the forwarding TN based on the STI authentication criteria for asserting full attestation defined in the base SHAKEN specification [ref].

The full attestation criteria defined by [shaken] enables a host SP to provide SHAKEN authentication with full attestation for DOD calls originated by a SIP-PBX; i.e., the host SP is able to verify with a high level of certainty that the originating SIP-PBX is authorized to originate calls from the calling TN. The following subsections describe how the full attestation criteria can be used by a host SP to verify the legitimacy of a SIP-PBX forwarding TN, so that the SP can add a “div” PASSporT token to a forwarding INVITE request received from a SIP-PBX.

#### Forwarding TN Authority based on SHAKEN Full Attestation criteria

Figure 5 shows the procedure for providing end-to-end call authentication when the SIP-PBX diverts a call by sending a new-INVITE to establish the forward-to leg, and the host SP determines the legitimacy of the forwarding TN based on the base SHAKEN authentication criteria for asserting full attestation; i.e., as specified by SHAKEN, the host Service Provider:

* 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.



Figure 5. Support for PBX divert via new-INVITE; forwarding TN authority based on SHAKEN full-attestation criteria

In addition to the fact that the call is diverted with a new INVITE request instead of a 302-response, the message sequence for Figure 5 differs from that shown in Figure 4 in two important ways:

1. SP-b knows that SIP-PBX-1 may divert DID calls using a new INVITE request. Therefore, in order to enable end-to-end delivery of the SHAKEN authentication information, SP-b includes the SHAKEN Identity header from [1] INVITE in the [2] INVITE request sent to SIP-PBX-1. SIP-PBX-1 in turn relays this Identity header in [3] INVITE back to SP-b so that it can be delivered to the forward-to network SP-c.
2. SP-b must implement logic to recognize that the [3] INVITE request received from SIP-PBX-1 is not establishing the initial leg of a DOD call, but is in fact establishing the forwarding leg of a previous DID call sent to the SIP-PBX. Therefore, instead of performing the base SHAKEN authentication procedures as it would for a normal DOD originating call, SP-b adds a "div" PASSporT token to authenticate the forwarding leg of the diverted call.

SP-b can assume that the received INVITE is legitimately establishing the forwarding leg of a diverted call if the following three conditions exist:

1. The received INVITE request contains a valid SHAKEN Identity header, and
2. The SIP-PBX is authorized to use the forwarding TN (based on SHAKEN full-attestation criteria).