**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

4.1 Overview of diverted calls and the impact to SHAKEN end-to-end call authentication 3

4.2 SHAKEN support of "div" PASSporT for in-network call diversion 5

4.3 SHAKEN support of "div" PASSporT for end-user device call diversion 7

4.3.1 SHAKEN functional requirements for call diverted by SIP-PBX 7

4.3.2 SIPconnect 2.0 Call-Forwarding Procedures 7

4.3.3 Adding "div" PASSporT when SIP-PBX diverts call via 3xx Response 8

4.3.4 Adding "div" PASSporT when SIP-PBX diverts call via new-INVITE Request 9

A Annex Title 12

**Table of Figures**

Figure 1. Replayed INVITE looks like a legitimately diverted INVITE 4

Figure 2. "div" PASSporT enables end-to-end authentication of legitimately diverted calls 6

Figure 3. Multiple Diversion Example: TN-a calls TN-b fwd🡪 TN-c fwd🡪 TN-d 7

Figure 4. Support of "div" PASSporT when SIP-PBX diverts call with 3xx-response 8

Figure 5. Support for PBX divert via new-INVITE; forwarding TN authority based on SHAKEN full-attestation criteria 10

Figure 6. Support for PBX divert via new-INVITE; forwarding TN authority based on TN-PoP 11

**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 diverted, the verification process becomes less certain due to the fact that the PASSporT "dest" claim no longer matches 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 diverted legs of the call and the associated changed telephone destinations. This document presents the solution for extending the SHAKEN framework to support these call diversion scenarios.

draft-ietf-stir-passport-div defines a PASSporT extension, "div", as a basis for accommodating the diversion or diversions that may occur for various SIP applications. 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.

What follows in this document is the details and specification of how the PASSporT "div" extension must be used as part of the SHAKEN framework for providing end-to-end SHAKEN validation for diverted calls. As SHAKEN is deployed in various service provider networks we will encounter a transitionary period where the mechanisms described in this document and the “div” PASSporT extension is not supported by all verification services (STI-VS). Therefore this document also provides details on how both baseline SHAKEN compliant only STI-VS and SHAKEN and “div” supporting STI-VS should interwork.

Section 4.1 provides an overview of why SHAKEN needs an extension to support diverted calls.

Section 4.2 describes how "div" PASSporT enables end-to-end call authentication when calls are diverted by a trusted in-network entity.

Section 4.3 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.

### SIPconnect 2.0 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.

For the 302-response case, the host service provider consumes the response, and forwards the call by updating the INVITE Request-URI to identify the forward-to user. It should be noted that there are certain call-diversion features, such as simultaneous ringing, that cannot be supported using the 302-respose mechanism.

For the "new-INVITE" case, the SIP-PBX must populate the new INVITE request as follows:

* The Request-URI must contain the forward-to TN
* The From header must contain the original calling TN
* The P-Asserted-Identity header must contains the SIP-PBX forwarding TN
* The History-Info header must record the forwarding event

SIPconnect 2.0 does not place any requirements on populating the To header, so presumably it contains the original called TN.

### 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 in one of two ways:

1. Based on the STI authentication criteria for asserting full attestation defined in the base SHAKEN specification [ref].
2. Based on TN-PoP; i.e., the diverting SIP-PBX provides a valid "pop" PASSporT token that proves it has the authority to use the diverting TN (this option assumes the eventual ratification by SHAKEN of TN-PoP as a mechanism to demonstrate authority over a telephone number).

These two mechanisms enable 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 these same mechanisms can also be used by a host SP to verify the legitimacy of a 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 forwarding TN matches the "dest" claim of the SHAKEN PASSporT token, and
3. The SIP-PBX is authorized to use the forwarding TN (based on SHAKEN full-attestation criteria).

SP-b can verify Condition-2 above in one of two ways:

1. SP-b compares the forwarding TN identified in [3] INVITE with the SHAKEN "dest" claim from [3] INVITE. This can only be done if SP-b can reliably identify the forwarding TN from the [3] INVITE request; e.g., SP-b knows that the SIP-PBX populates the forwarding TN in the P-Asserted-Identity header (per SIPconnect 2.0), or in an included History-Info header.
2. If SP-b cannot reliably identify the forwarding TN in [3] INVITE, then it can perform the check before sending [2] INVITE to SIP-PBX-1. In this case, SP-b verifies that the SHAKEN “dest” claim matches the Request-URI TN in received [1] INVITE. If the TNs match, then SP-b includes the received “shaken” Identity header in [2] INVITE sent to the SIP-PBX; otherwise the SP-b discards the "shaken" Identity header. As a result, SP-b knows that any “shaken” Identity header received in an incoming [3] INVITE satisfies Condition-2.

If the call had been legitimately diverted before reaching SIP-PBX-1 by an SP that supports "div" PASSPorT, then [1] INVITE will contain one or more "div" Identity headers. In this case, the procedures described above still apply, except that instead of checking for a direct match between forwarding TN and SHAKEN "dest" claim TN, SP-b checks for an complete chain of authority from the forwarding TN through the one or more "div" PASSporT tokens, to the SHAKEN "dest" TN.

If [3] INVITE contains "shaken" (and possible "div") Identity header(s), but one or more of the above criteria are not met, or if [3] INVITE contains no Identity header, then the host SP must assume that the INVITE is establishing the initial leg of a DOD call. In this case, the host SP shall remove any received Identity headers in [3] INVITE, and perform the base SHAKEN verification procedures.

#### Forwarding TN Authority based on TN-PoP

Figure 6 illustrates the call-forwarding message flow similar to that shown in Figure 5, except that the SIP-PBX establishes its authority to use the forwarding TN using TN-PoP. TN-PoP is being used in this example because SIP-PBX-1 is hosted by two service providers; SP-b and SP-x. SP-b has delegated a range of its assigned telephone numbers, including TN-b, to SIP-PBX-1. SP-b has also provided SIP-PBX-1 with a PoP certificate covering this set of delegated TNs. Since TN-b is assigned to SP-b, the initial DID leg of the call is routed via SP-b to the SIP-PBX. SIP-PBX-1 happens to select its other host SP, SP-x, to establish the forward-to leg of the diverted call.



Figure 6. Support for PBX divert via new-INVITE; forwarding TN authority based on TN-PoP

As shown in Figure 6, the SIP-PBX includes a PoP PASSporT token in the forwarding [3] INVITE request sent to SP-x. SP-x determines that [3] INVITE is establishing the forward-to leg of a diverted DID call as described in section 4.3.4.1, but instead of applying the SHAKEN full-attestation criteria to validate forwarding TN-b, SP-x verifies the received PoP PASSporT token to establish SIP-PBX-1’s authority to use TN-b. SP-x then replaces the PoP PASSporT token with a "div" PASSporT token in [4] INVITE sent to the forward-to network SP-c.

# A Annex Title

Xxx