ATIS-1000085.v002

Signature-based handling of Asserted information using toKENs (SHAKEN):

SHAKEN Support of "div" PASSporT

JOINT STANDARD

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

The SIP Forum is a leading IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations; interoperability testing events and special workshops, educational activities, and general promotion of IP communications standards, services, and technology for service provider, enterprise, and governmental applications. The SIP Forum is also the producer of the annual SIPNOC conferences (for SIP Network Operators Conference), focused on the technical requirements of the service provider community. One of the Forum's technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation that provides detailed guidelines for direct IP peering and interoperability between IP PBXs and SIP-based service provider networks, and the SIPconnect Certification Testing Program, a unique certification testing program that includes a certification test suite and test platform, and an associated "SIPconnect Certified" logo program that provides an official "seal of certification" for companies products and services that have officially achieved conformance with the SIPconnect specification. Other important Forum initiatives include work in security, SIP and IPv6, and IP-based Network-to-Network Interconnection (IP-NNI). For more information about all SIP Forum initiatives, please visit:

< http://www.sipforum.org/ >

ATIS-1000085.v002, Signature-based Handling of Asserted information using toKENs (SHAKEN): SHAKEN Support of "div" PASSporT

Is an ATIS & SIP Forum Joint Standard developed by the **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **Technical Working Group (TWG)** under the **SIP Forum**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

SIP Forum LLC
733 Turnpike Street, Suite 192
North Andover, MA 01845

ATIS-1000085.v002

ATIS Standard on

Signature-based Handling of Asserted information using toKENs (SHAKEN):
SHAKEN Support of "div" PASSporT

Alliance for Telecommunications Industry Solutions

Approved September 25, 2020

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 time freshness window. This technical report describes how the mechanisms defined by draft-ietf-stir-passport-divert [Ref 4] can be integrated within the SHAKEN framework to close this replay attack window.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. International Telecommunication Union Telecommunication Sector (ITU-T) and U.S. ITU Radiocommunication Sector (ITU-R) Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The SIP Forum is an IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations, the SIPit, SIPconnect-IT, and RTCWeb-it interoperability testing events, special workshops, educational seminars, and general promotion of SIP in the industry. The SIP Forum is also the producer of the annual SIP Network Operators Conference (SIPNOC), focused on the technical requirements of the service provider community. One of the Forum's notable technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation for direct IP peering and interoperability between IP Private Branch Exchanges (PBXs) and SIP-based service provider networks. Other important Forum initiatives include work in Video Relay Service (VRS) interoperability, security, Network-to-Network Interoperability (NNI), and SIP and IPv6.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005, and/or to the SIP Forum, 733 Turnpike Street, Suite 192, North Andover, MA, 01845.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

The **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **SIP Forum Technical Working Group (TWG)** was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

1 Scope & Purpose

1.1 Scope

This document describes how the PASSporT "div" extension defined in draft-ietf-stir-passport-divert [Ref 4] 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.

1.2 Purpose

The SHAKEN authentication service in an originating network asserts two telephone numbers (TNs) in the "shaken" PASSporT [Ref 1]; 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 [Ref 4] 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.

1.2.1 Document Organization

Clause 4 provides an informative overview of the PASSporT "div" extension, and how it enables end-to-end delivery of SHAKEN authentication information for retargeted calls.

Clause 5 specifies the normative requirements to support draft-ietf-stir-passport-divert [Ref 4] to SHAKEN.

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

Annex B shows an example of a SIP Identity header containing a "div" PASSporT.

2 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.

[Ref 1] ATIS-1000074, *Signature-based Handling of Asserted Information using Tokens (SHAKEN).*[1]

[Ref 2] IETF RFC 3892, *The SIP Referred-By Mechanism*. [2]

[Ref 3] IETF RFC 8588, *Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)*.[2]

[Ref 4] draft-ietf-stir-passport-divert, *PASSporT Extension for Diverted Calls.* [2]

[Ref 5] IETF RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks.*[2]

[Ref 6] IETF RFC 3261, *SIP: Session Initiation Protocol.*[2]

[Ref 7] IETF RFC 5031, *A Uniform Resource Name (URN) for Emergency and Other Well-Known Services*. [2]

[Ref 8] IETF RFC 5806, *Diversion Indication in SIP*. [2]

[Ref 9] IETF RFC 7044, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*. [2]

[Ref 10] 3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)*.[3]

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

3.1 Definitions

Call Diversion: Any call feature that updates the destination telephone number of a call to a new or alternate telephone number. Example call features include the various forms of call forwarding, find-me/follow-me (simultaneous or sequential ringing), and automatic call distribution.

Redirect: As defined in RFC 3261 [Ref 6], "redirect" refers to the process where a SIP entity redirects a SIP request to a new destination by responding to the request with a 3xx Redirection class response. This specification addresses redirection only for INVITE requests, and only for the case where the 3xx response is handled by a recursing SIP proxy that retargets the INVITE request to the new destination.

Retarget: As defined in RFC 7044 [Ref 9], "retarget" refers to the process where a SIP entity updates the Request-URI of a SIP request. This specification narrows the scope of the RFC 7044 [Ref 9] definition to include only INVITE requests, and only for cases where the update changes the canonical value of the telephone number identified by the INVITE Request-URI.

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < http://www.atis.org >.
[2] This document is available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org >.
[3] This document is available from 3rd Generation Partnership Project (3GPP) at: < https://www.3gpp.org >

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
ATIS	Alliance for Telecommunications Industry Solutions
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
PAID	P-Asserted-Identity
PPI	P-Preferred-Identity
PASSporT	Personal Assertion Token
PBX	Private Branch Exchange
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
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
TN	Telephone Number
URI	Uniform Resource Identifier

4 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 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 TN destination. This document presents the solution for extending the SHAKEN framework to support these call retargeting scenarios.

draft-ietf-stir-passport-divert [Ref 4] defines a PASSporT extension, "div", as a basis for accommodating the retargeting that may occur for various SIP call diversion 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 4.1 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 an Identity header field containing a "shaken" PASSporT [Ref 3] to the INVITE request, as specified by ATIS-1000074 [Ref 1], where the “orig” and “dest” claims of the "shaken" PASSporT contain the calling and called TNs. When the call is forwarded, the SP-b authentication service adds a second Identity header containing a “div” PASSporT as specified in draft-ietf-stir-passport-divert [Ref 4], 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" PASSporT “dest” claim.

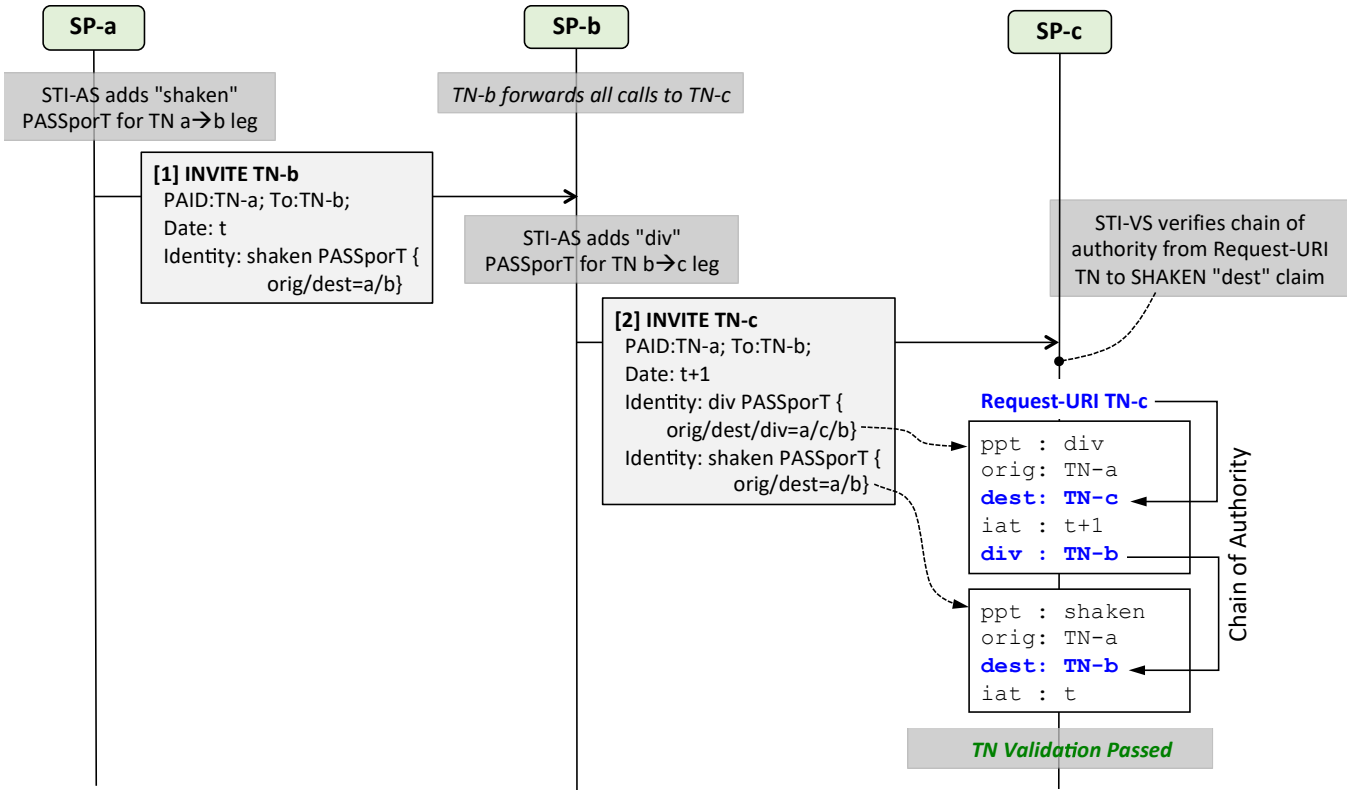

Figure 4.1 – Using "div" PASSporT to authenticate the forwarding leg of call

What follows in Clause 5 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.

5 Normative Requirements

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

5.1 STI-AS Base SHAKEN Authentication Assumptions

This document assumes that the base SHAKEN authentication procedures defined in ATIS-1000074 [Ref 1] require the STI-AS to populate the "shaken" PASSporT "dest" claim as follows:

- If the To header contains a service URN in the 'sos' family then use the service URN,
- Else, use the canonicalized value of the To header TN.

5.2 STI-VS Base SHAKEN Verification Assumptions

On receiving an INVITE request containing an Identity header with a “shaken” PASSporT, and no Identity headers with “div” PASSporTs, the STI-VS will perform the base SHAKEN verification procedures as defined in ATIS-1000074 [Ref 1]. This document assumes that as part of base SHAKEN, when the received Identity header contains a “shaken” PASSporT, the STI-VS will populate the local “dest" claim during PASSporT signature verification as follows:

- If the To header contains a service URN in the 'sos' family then use the service URN,
- Else, use the canonicalized value of the To header TN.

5.3 STI-AS "div" Authentication

The STI-AS shall provide "div" authentication services as defined in draft-ietf-stir-passport-divert [Ref 4], with the following restrictions:

- The requirement that the INVITE request must contain at least one Identity header is qualified as the INVITE shall contain at least one Identity header with a “shaken” PASSporT,
- The "orig" claim shall be of type "tn",
- The "orig" claim value shall be copied from the “shaken” PASSporT "orig" claim,
- The "div" and "dest" claims can each have an identity type of either "tn" or "uri". When the identity type is "uri", the identity value shall identify a service URN in the 'sos' family, as defined in RFC 5031 [Ref 7],
- The "opt" claim shall not be used (no nesting).

To support retargeting when the INVITE Request-URI before retargeting contains a service URN in the 'sos' family (e.g., urn:service:sos), the “div” PASSporT shall contain a "div” claim of type "uri" with a value identifying the service URN. Likewise, to support retargeting when the INVITE Request-URI after retargeting contains a service URN in the ‘sos’ family, the “div” PASSporT shall contain a “dest” claim of type “uri” with a value identifying the service URN. For “div” PASSporT "div" or “dest” claims of type "uri", the only identity value allowed by this specification is a service URN in the 'sos' family. Based on local policy, the STI-AS may skip "div" authentication when an INVITE is retargeted from one emergency destination to another emergency destination (i.e., when the INVITE Request-URI before and after retargeting is identified by the digits '911', or by a service URN in the ‘sos’ family).

5.4 STI-VS "div" Verification

On receiving an INVITE request containing an Identity header with a “shaken” PASSporT, and one or more Identity headers with “div” PASSporTs, an STI-VS shall perform the “div” verification procedures defined in draft-ietf-stir-passport-divert [Ref 4], with the following restrictions:

- The "div" PASSporT "orig" claim shall be of type “tn”,
- The "div" PASSporT "div" and "dest" claims can each have an identity type of either "tn" or "uri". When the identity type is "uri", the identity value shall identify a service URN in the 'sos' family, as defined in RFC 5031 [Ref 7],
- The "div" PASSporT "opt" claim shall be absent.

The STI-VS shall verify that the received "div" PASSporTs create an unbroken chain of authority from the INVITE Request-URI TN to the “dest” claim of the "shaken" PASSporT. During construction of the chain, the digits ‘911’ and any services URN in the ‘sos’ family shall be considered equivalent. The STI-VS shall verify each “div” PASSporT as specified in this document. The STI-VS shall verify the “shaken” PASSporT as specified in ATIS-1000074 [Ref 1], with the exception that it shall not use the identity in the To header field to validate the "shaken" PASSporT "dest" claim.

The STI-VS shall verify the freshness of the most recently added PASSporT as specified in ATIS-1000074 [Ref 1] (e.g., using the recommended 60 second freshness window). To accommodate call features that legitimately insert a delay before retargeting the INVITE, the STI-VS shall, based on local policy, either skip the freshness check for any earlier PASSporTs, or extend the freshness window of these earlier PASSporTs beyond the normal limit.

If the most recently added PASSporT fails the "iat" freshness test, then the STI-VS shall remove all received Identity headers. This will avoid the situation where a subsequent retargeting event adds a fresh "div" PASSporT that causes the stale PASSporT to appear fresh to downstream verifiers. This requirement shall be applied to all verification cases; i.e., whether the INVITE request contains a single "shaken" PASSporT, or a "shaken" PASSporT plus one or more "div" PASSporTs.

5.5 In-network Call Diversion

This clause describes the authentication procedures when an in-network call feature or routing function retargets an INVITE request by updating an INVITE Request-URI to identify a new destination.

As specified in draft-ietf-stir-passport-divert [Ref 4], an authentication service adds an Identity header containing a "div" PASSporT only if the SIP request contains at least one Identity header field[4]. Therefore, if the retargeted INVITE request does not contain an Identity header, then the STI-AS of the retargeting network:

- Shall for the cases covered in Clause 5.1, first perform SHAKEN authentication as specified in ATIS-1000074 [Ref 1] and then perform “div” authentication,
- Otherwise, may choose to either skip authentication altogether, or to perform authentication based on local policy; e.g., perform base SHAKEN authentication with Gateway attestation, and then perform div authentication

5.5.1 Retarget-from and Retarget-to Identities are TNs

If both the in-network retargeting entity and the retarget-to destination are identified by TNs, and if the retargeting and retarget-to TNs have different canonical values, then the STI-AS shall perform "div" authentication as specified in Clause 5.3. The STI-AS shall not perform "div" authentication during INVITE retargeting if the canonicalized value of the TN contained in the Request-URI before retargeting is different than the "dest" claim of the PASSporT that was most recently added to the INVITE request.

When providing authentication services for an originating INVITE request where the canonicalized values of the To header and Request-URI TNs do not match because the INVITE was retargeted by the originating network, and the originating network has established an association between an identified and authenticated retargeting entity and its retargeting TN, the STI-AS of the originating SP shall first perform SHAKEN authentication as specified in ATIS-1000074 [Ref 1], and then perform “div” authentication as described in this document. The resulting INVITE request shall contain two Identity headers, one containing the "shaken" PASSporT and one containing a “div” PASSporT. The “div” PASSporT shall provide an intact chain of valid TN claims from the Request-URI TN to the “shaken” PASSporT “dest” claim. If the STI-AS has not established an association between an identified and authenticated retargeting entity and its retargeting TN, then it will be unable to perform “div” authentication, which will result in a broken chain of authority from To header to Request-URI. If allowed by local policy, the STI-AS may resolve this issue by updating the To header TN to match the Request-URI TN before performing SHAKEN authentication.

> Note: The case described in the above paragraph, where the originating network authentication service discovers a mismatch between the To header and Request-URI TNs, can occur when a toll-free routing database dip in the originating network returns the toll-free routing number. This can create the situation where the To header contains the dialed 8YY number, while the Request-URI contains the routing TN assigned to that 8YY number. After completing the authentication procedures as specified in the above paragraph, the TN-related claims of the two PASSporTs are populated as follows:
>
> **"shaken" PASSporT TN claims:**
>
> - “orig” contains calling TN from P-Asserted-Identity header
> - “dest” contains dialed 8YY number from To header.
>
> **"div" PASSporT TN claims**

[4] The procedures described in Clause 5.5 assume that the in-network retargeting entity will convey received Identity header fields in the retargeted INVITE request. However, early deployments of SHAKEN may encounter in-network retargeting entities that discard received Identity headers. In this case, the retargeting entity should be treated as a retargeting end-user device that does not convey Identity headers, as described in Clause 5.6.2.

- “orig” contains calling TN from “shaken” PASSporT “orig” claim
- “div” contains dialed 8YY number from “shaken” PASSporT “dest” claim
- “dest” contains toll-free routing TN from Request-URI.

5.5.2 Retarget-from or Retarget-to Identity is an Emergency Services URN

If the retargeting event is from a non-emergency destination to an emergency services destination, or from an emergency services destination to a non-emergency destination, then the STI-AS shall perform "div" authentication as specified in Clause 5.3. For example, a retargeting event that updates the Request-URI from urn:service:sos to TN 1-303-555-1212 (or vice versa) requires “div” authentication. Whether the STI-AS performs "div" authentication for retargeting events that update the Request-URI from digits ‘911’ to an ‘sos’ service URN, or from one ‘sos’ service URN to another ‘sos’ service URN, is based on local policy.

5.6 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 clause apply to the case where device capabilities and service provider policies enable the end-user device to divert calls using either of these mechanisms.

5.6.1 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 as specified by IETF RFC 3261 [Ref 6], 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.

5.6.2 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 ATIS-1000074 [Ref 1], and in Clause 5.4 of this document. The host SP may convey the verification result in the INVITE request sent to the end-user device using the tel URI "verstat" parameter, as specified in 3GPP TS 24.229 [Ref 10]. If allowed by local policy, the terminating SP shall deliver the Identity headers in the INVITE request sent to the end-user device.

> Note: As stated in Clause 5.4, if the most recently added PASSporT fails the 60 second freshness check, then all received Identity headers are removed before sending the INVITE request to the end-user device. This will avoid the case where an INVITE request containing a stale "shaken" PASSporT is retargeted by the end-user device, and the host SP “div” authentication service adds a fresh "div" PASSporT, thus making the stale “shaken” PASSporT appear fresh to downstream verifiers.

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 valid "shaken" PASSporT, and zero or more Identity headers with valid "div" PASSporTs, then the STI-AS shall perform “div” authentication as specified in Clause 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 [Ref 8], History-Info [Ref 9], Referred-By [Ref 2]), 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 ATIS-1000074 [Ref 1] and as described in Clause 5.6.3.

If the criteria for performing “div” authentication as defined in the previous paragraph are met, but the canonicalized value of the TN of the retargeting entity is different than the "dest" claim of the PASSporT that was most recently added to the received INVITE request, then the STI-AS shall take no action (i.e., shall not perform "div" authentication).

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” PASSporT "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 ATIS-1000074 [Ref 1].

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 a SHAKEN Identity header, then the STI-AS may sign the request normally, performing base SHAKEN authentication as defined in ATIS-1000074 [Ref 1]. If the TN in the To header field value does not match the Request-URI TN (which would normally be the case when the INVITE is retargeted), and the STI-AS is able to assert that the end-user is has a verified association with the TN in the To header field value, then the STI-AS shall additionally perform “div” authentication to create an unbroken chain of valid TN claims from the “shaken” PASSporT “dest” claim to the Request-URI TN. If the STI-AS is not able to assert that the end-user has a verified association the TN in the To header field value, then it will be unable to generate a “div” PASSporT, which might result in a broken chain of valid TN claims from the To header field value to the Request-URI. If allowed by local policy, the STI-AS may resolve this by updating the To header TN to match the Request-URI TN before performing SHAKEN authentication, or take other measures to enable adding a “div” PASSporT that are left to future work.

If the information contained in an INVITE request received from an end-user device indicates that the request has been retargeted, and the retargeting entity indicates a TN that the end-user device is not authorized to use, then the STI-AS shall not perform a “div” authentication. Instead, the STI-AS shall remove any received Identity headers, and perform base SHAKEN authentication as defined in ATIS-1000074 [Ref 1].

5.6.3 Fully Attesting the Retargeting TN

Since the "div" PASSporT does not contain an "attest" claim, verifiers must assume that the signing entity is asserting the equivalent of the SHAKEN “full attestation” level for the "div" TN, and is in addition asserting that the retargeting customer entity was authorized to retarget the INVITE request. When applied to "div” authentication, the full attestation criteria defined in ATIS-1000074 [Ref 1] are modified as follows:

1) The signing provider must be responsible for the origination of the retargeted call leg onto the IP based service provider voice network.
2) The signing provider must have a direct authenticated relationship with the retargeting customer and can identify the customer.
3) The signing provider must have established a verified association with the retargeting telephone number.

The mechanisms used to satisfy criteria 2 and 3 when the OSP does not have a direct relationship with the retargeting entity, and/or when the OSP has no association with the retargeting TN, are outside the scope of this document.

5.6.4 Security Considerations

Armed with a valid SHAKEN Identity header received from a SHAKEN SP, an end-user device could attempt to maliciously spoof the “shaken” PASSporT “orig” claim TN by including the Identity header, plus a valid Diversion or History-Info header, in a new INVITE request addressed to a target victim. An OSP that supports the procedures defined in Clause 5.6.2 would authenticate the INVITE as if it had been legitimately retargeted, thus making the replayed “shaken” PASSporT appear valid to remote verifiers. Therefore, OSPs that provide this service must take measures to limit the customer’s ability to successfully launch such an attack. These measures could include the following:

- Provide the service only to customers that pass a vetting process; e.g., provide the service only to customers that have been authenticated via a direct UNI connection, and customers that have established a strong trust relationship with the OSP.
- Provide disincentives for bad behavior by negotiating Service Level Agreements with strong penalties if the customer abuses the service.
- Instead of providing a general authentication service for INVITE requests retargeted from any customer TN to any remote TN, provide the service to a limited set of retarget-to TNs, a limited set of customer retarget-from TNs, or a limited set of retarget-to/from TN pairs.
- Limit the replay interval by providing the service only for "shaken" PASSporTs that are within a shorter-than-usual freshness window. Selecting the freshness window in this case is a tradeoff between supporting the customer’s legitimate retargeting events and limiting the customer’s ability to launch a replay attack.
- Apply analytics to detect unusual call patterns that might indicate a replay attack is occurring; e.g., receiving the same SHAKEN Identity header multiple times, or detecting a dramatic increase in the rate of received retargeted INVITE requests.

Annex A – Authentication of End-user Device Retargeted Calls

Implementation of the normative procedures for authentication of in-network INVITE retargeting cases (Clause 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 (Clause 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 annex provides information that shows how the generic requirements in Clause 5.6.2 can be applied to different end-user device retargeting use cases.

The information in this annex is not normative. Also, this clause 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.

A.1 STI-AS Procedures

As shown in Figure A.1, 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 A.1 illustrates some of the scenarios that the STI-AS may need 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 conveys 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 simply perform “div” authentication because [4] INVITE does not contain a SHAKEN Identity header. Therefore, the STI-AS first performs SHAKEN authentication based on the information that it does have; i.e., that TN-a called TN-b, and TN-b retargeted the call to TN-c. In this example, since SP-b has no verified relationship with the originator of the call, it asserts an attestation level of Gateway in the “shaken” PASSporT. If SP-b is authoritative for the TN of the retargeting entity (TN-b), then it shall perform "div" authentication. The STI-AS includes two Identity headers, one containing the "shaken" PASSporT and one containing the "div" PASSporT in [5] INVITE to SP-c.

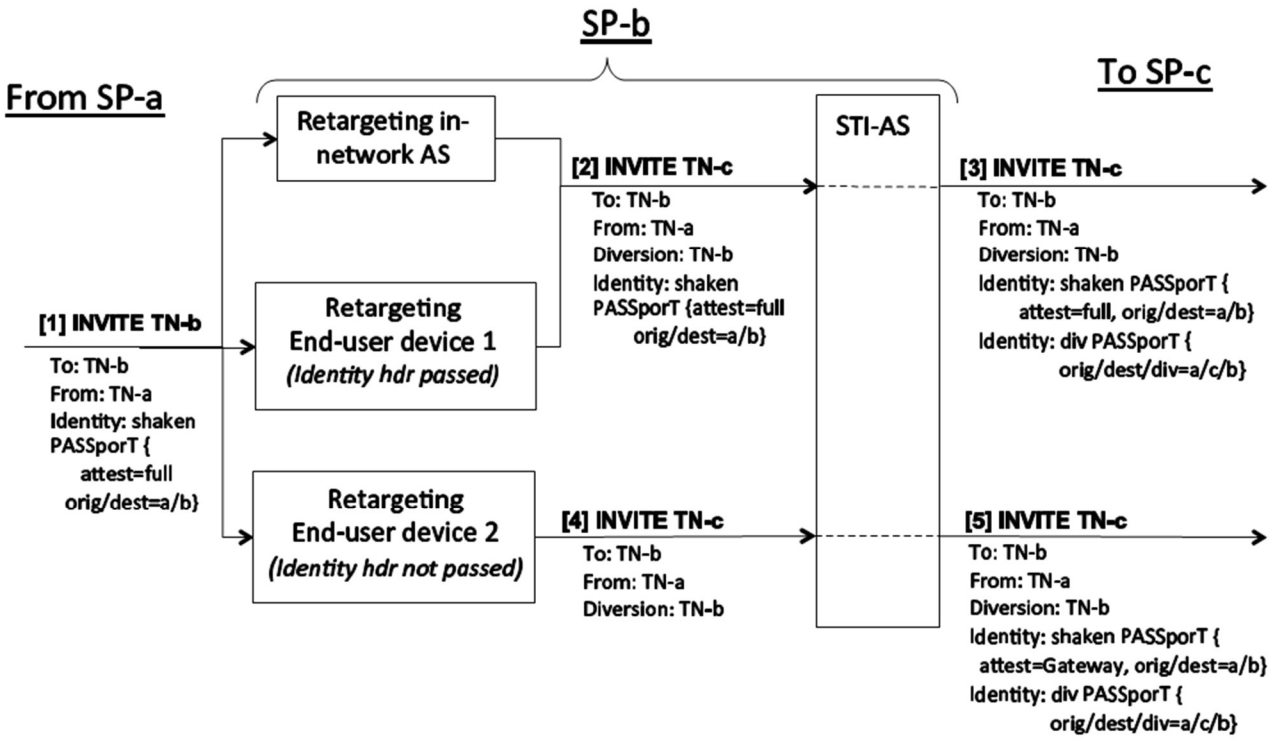

Figure A.1 – STI-AS Authentication Examples

Note: Figure A.1 shows the case where the To header field in the retargeted INVITE request (e.g., in [2] INVITE) contains the TN of the Request-URI before retargeting. There are also cases where the To header field in a retargeted INVITE does not contain the pre-retargeting Request-URI TN; e.g., when the retargeting Application Server or end-user device updates the To header field to match the post-retargeting Request-URI, or when retargeting occurs for a previously retargeted INVITE request. The “div” procedures described in this document can support all of these cases.

Figure A.2 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 the STI-AS performs “shaken” authentication followed by "div" authentication (else continue).
4) If the retargeted INVITE request contains an Identity header with a "shaken" PASSporT, then the STI-AS performs “div” authentication; otherwise it performs “shaken” authentication followed by "div" authentication.

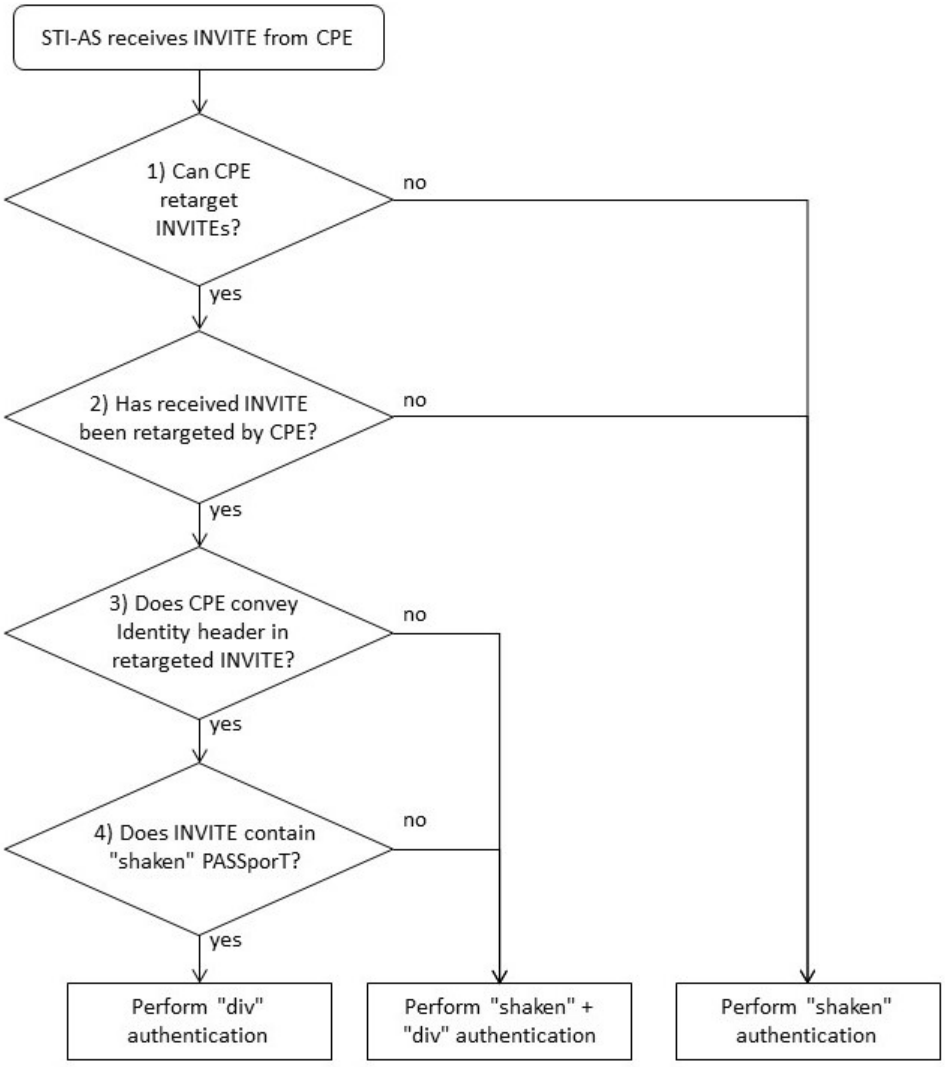

Figure A.2 – STI-AS logic to determine authentication procedures for INVITE from CPE

A.2 End-user Device Retargeting Examples

The message sequence diagrams in this clause use the template shown in Figure A.3, 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 assigned 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.

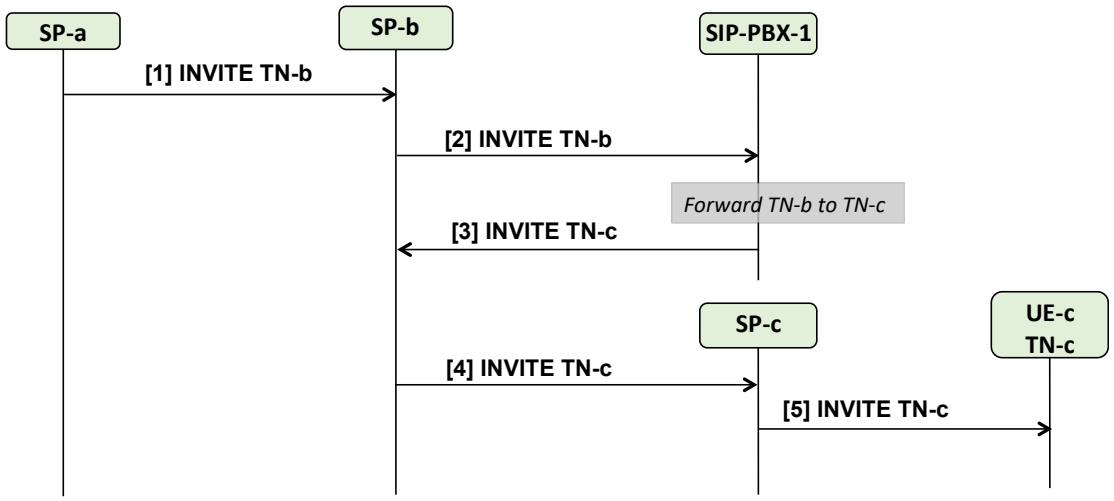

Figure A.3 – Message sequence diagram template

This clause 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 A.1.

> Note: The following sub-clauses use the term "PAID" to refer to the P-Asserted-Identity header, and "PPI" to refer to the P-Preferred-Identity header. Also, in the following message sequence diagrams, the presence of the Diversion header in an INVITE request indicates that the INVITE has been retargeted by the SIP-PBX. Retargeting could also be indicated by the presence of the History-Info header, or the Referred-By header.

Table A.1 – SIP-PBX cases

SIP-PBX case	Headers conveyed from INVITE [2] to [3]?	
	Identity	PAID/From
Case-1	yes	yes
Case-2	yes	no
Case-3	no	yes
Case-4	no	no

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:

a) INVITE contains a valid SHAKEN Identity header
b) INVITE contains no Identity header
c) INVITE contains an invalid Identity header

A.2.1 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, and a Diversion header identifying the retargeting entity

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

On receiving [1] INVITE in Figure A.4, SP-b STI-VS verifies that the received SHAKEN Identity header is valid. SP-b includes the Identity header and a "TN-Validation-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.

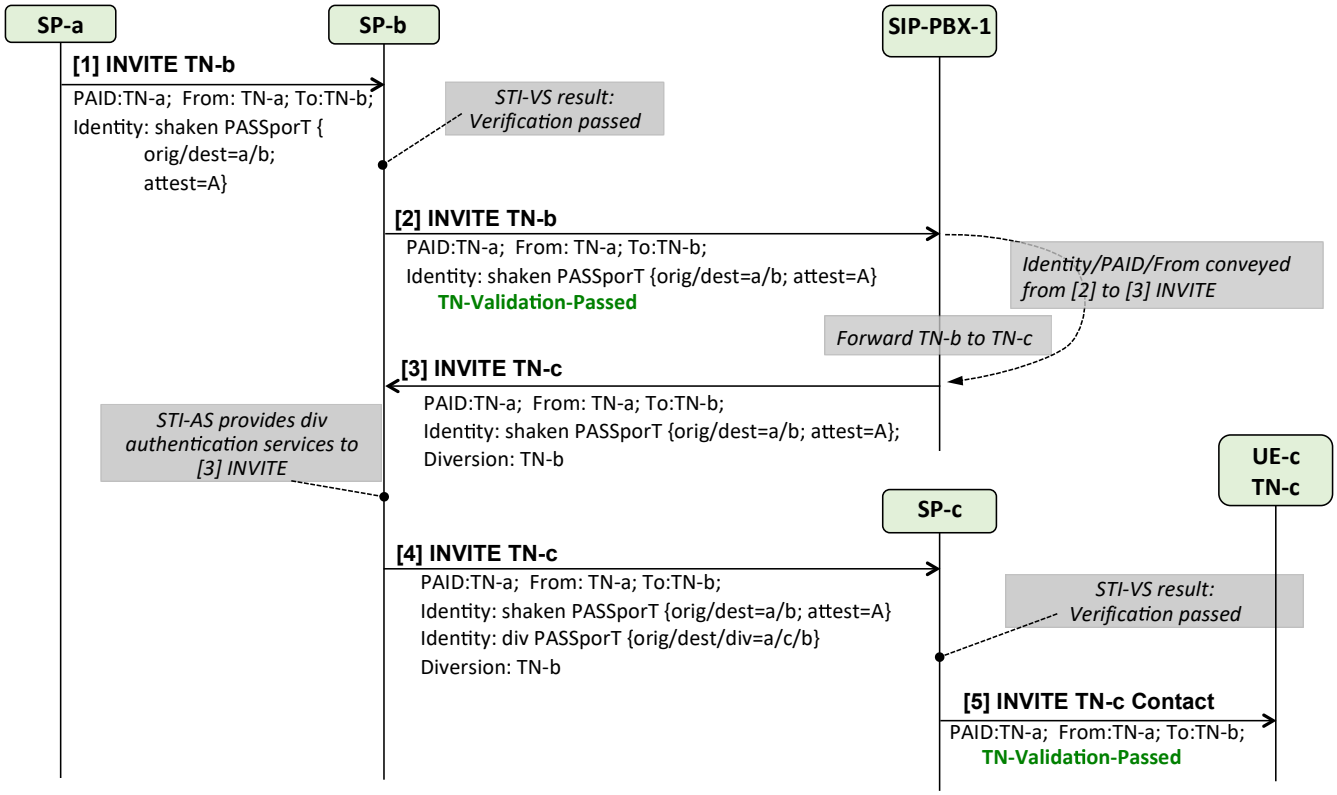

Figure A.4 – Case-1a– [1] INVITE contains valid Identity header

Note: SP-b will remove any "verstat" parameter received from the SIP-PBX in [3] INVITE PAID or From headers before including those headers in [4] INVITE to SP-c.

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

On receiving [1] INVITE in Figure A.5, 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 to 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 and “div” authentication on [3] INVITE (since it doesn’t contain a SHAKEN Identity header). [4] INVITE to SP-c contains a SHAKEN Identity header for calling TN-a with "Gateway" attestation and a “div” PASSporT.

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.

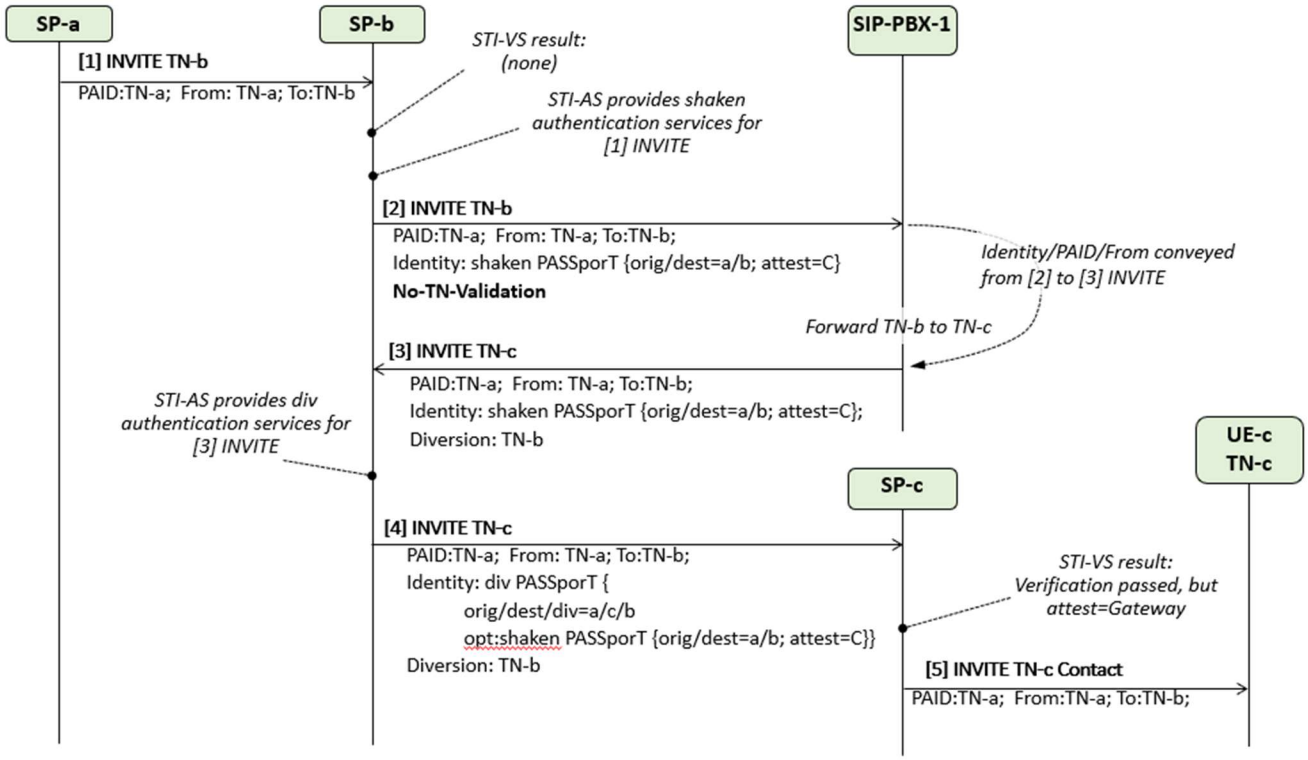

Figure A.5 – Case-1b – [1] INVITE contains no Identity header

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

On receiving [1] INVITE in Figure A.6, 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.

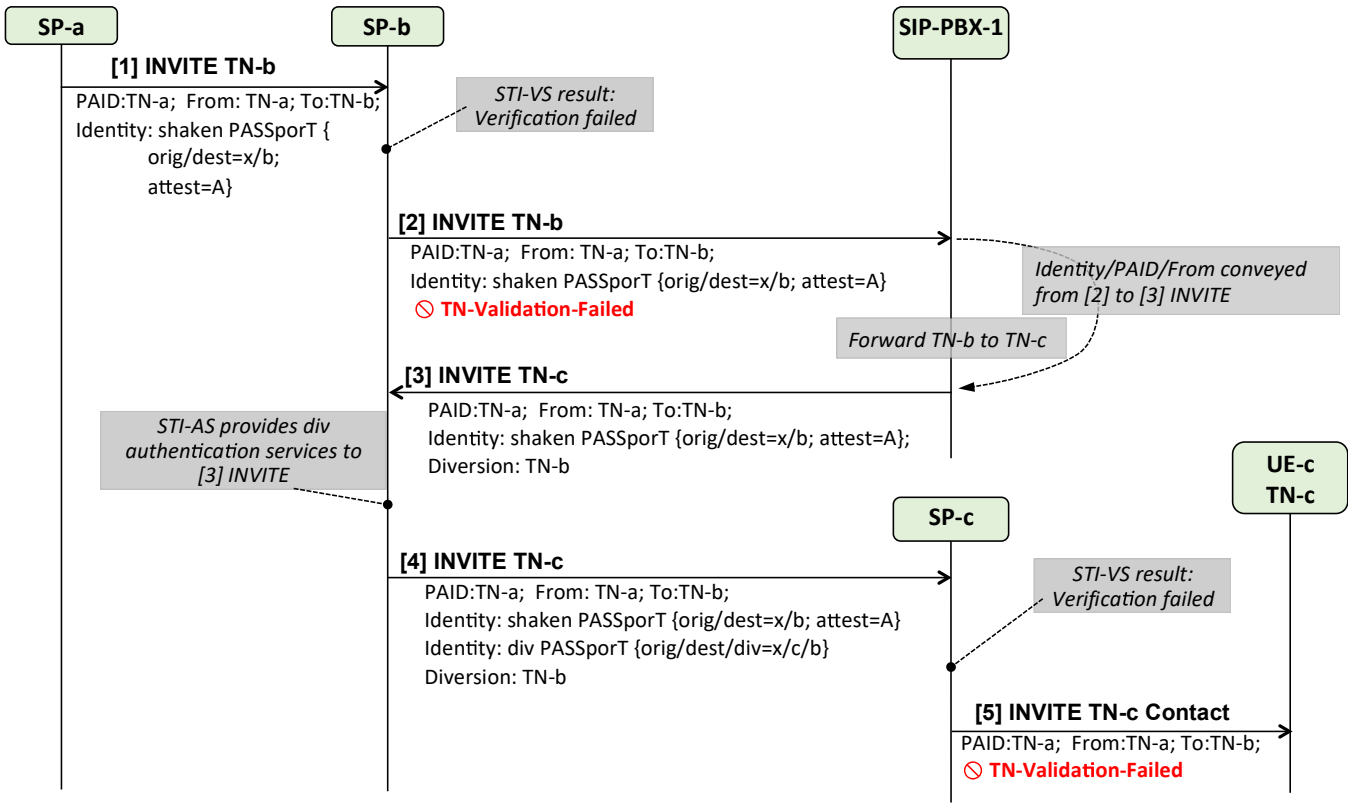

Figure A.6 – Case-1c – [1] INVITE contains invalid Identity header

A.2.2 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/From headers containing retargeting 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 A.7, SP-b STI-VS verifies that the received SHAKEN Identity header is valid and includes the Identity header and a "TN-Validation-Passed" indication in [2] INVITE to SIP-PBX-1. The SIP-PBX populates the P-Preferred-Identity header of [3] INVITE with the calling user identity (TN-b) that the SIP-PBX would like to deliver to the called user TN-c for this call leg. On receiving [3] INVITE, SP-b determines that the INVITE was not retargeted and therefore, the STI-AS removes the received SHAKEN Identity header, performs "shaken" authentication for calling TN-b, and includes the resulting SHAKEN Identity header in [4] INVITE to SP-c.

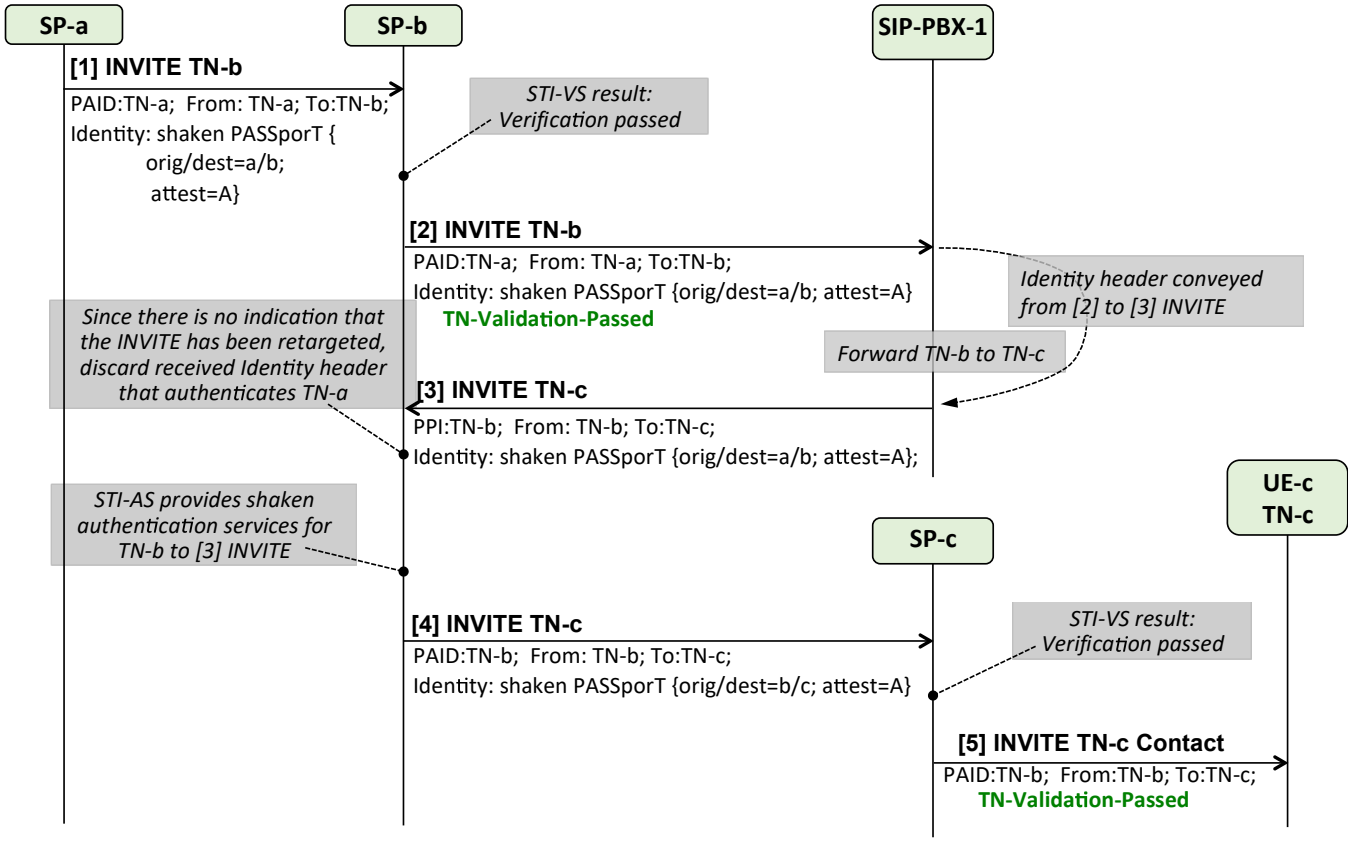

Figure A.7 – Case-2a – [1] INVITE contains valid Identity header

Case-2a demonstrates the fact that a SIP-PBX cannot deliver end-to-end SHAKEN by simply relaying the received Identity header in a retargeted INVITE. For call retargeting scenarios where the customer wants to deliver the original calling TN-a to the forward-to user, the SIP-PBX will need to convey calling TN-a in the P-Preferred-Identity or P-Asserted-Identity header of the retargeted INVITE, and explicitly indicate that the INVITE is being retargeted with a Diversion or History-Info header, similar to the Case-1 procedures shown in Annex A.2.1.

Case-2b/2c: Originating [1] INVITE contains no/invalid Identity header

The procedures for Case-2b/2c are generally the same as Case-2a. Independent of the SHAKEN authentication information received from SP-a in [1] INVITE, SP-b delivers a SHAKEN Identity header authenticating TN-b in [4] INVITE to SP-c.

A.2.3 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, and with a Diversion header identifying the retargeting entity.

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

On receiving [1] INVITE in Figure A.8, 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 followed by "div" authentication for retargeting TN-b, and adds two Identity headers containing the "shaken" and "div" PASSporTs 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 no verstat indication to UE-c.

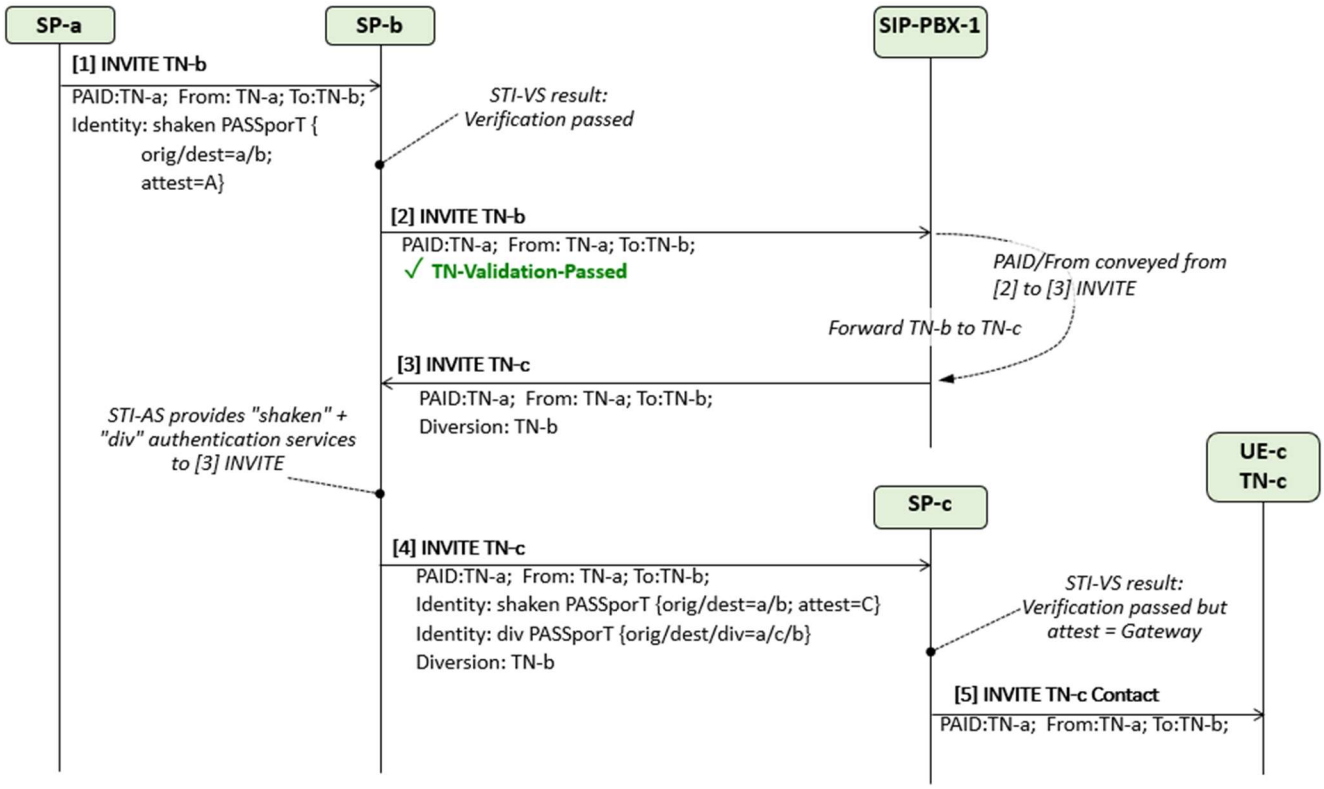

Figure A.8 – Case-3a – [1] INVITE contains valid Identity header

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". In both cases, SP-b provides a SHAKEN Identity header with Gateway Attestation for TN-a in [4] INVITE to SP-c.

A.2.4 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 does not 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 A.9, 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.

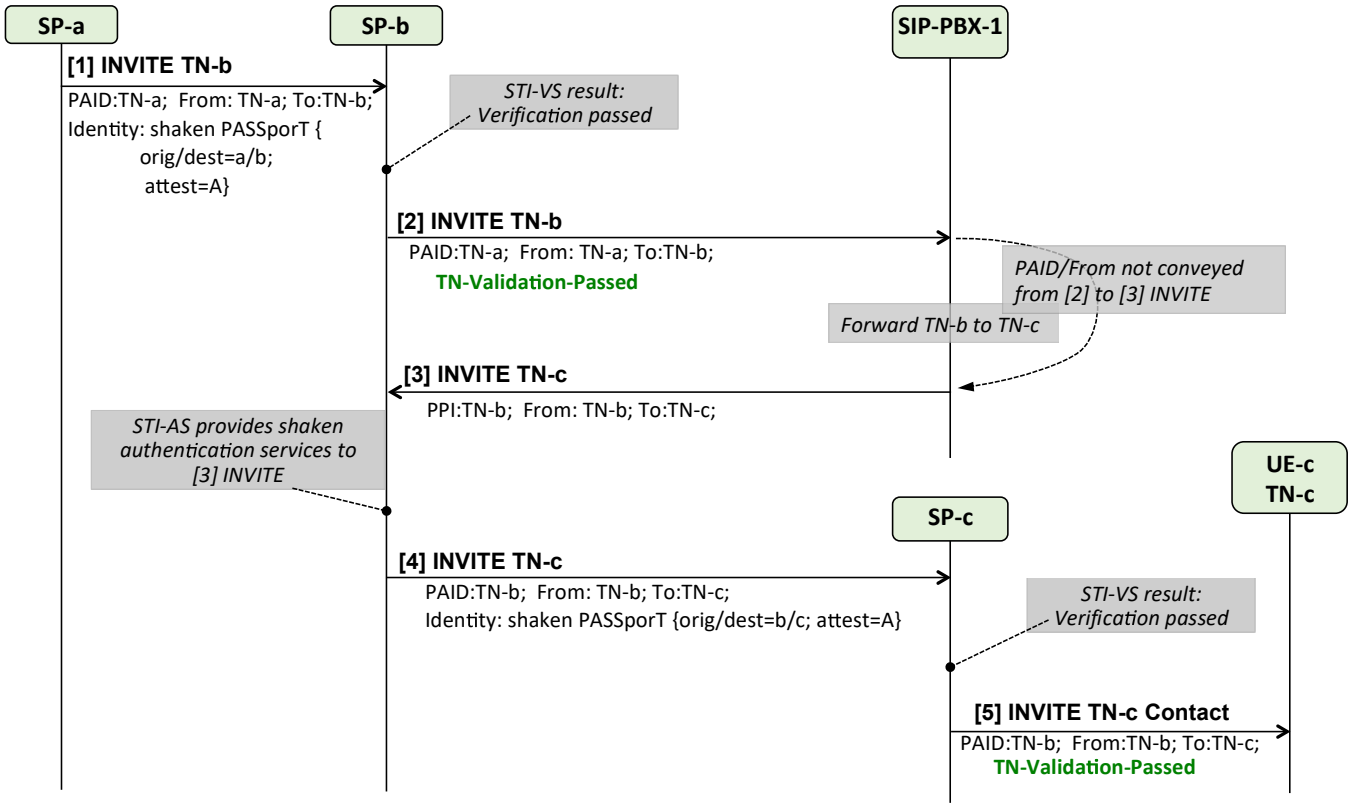

Figure A.9 – Case-4a – [1] INVITE contains valid Identity header

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

As shown in Figure A.10, 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”.

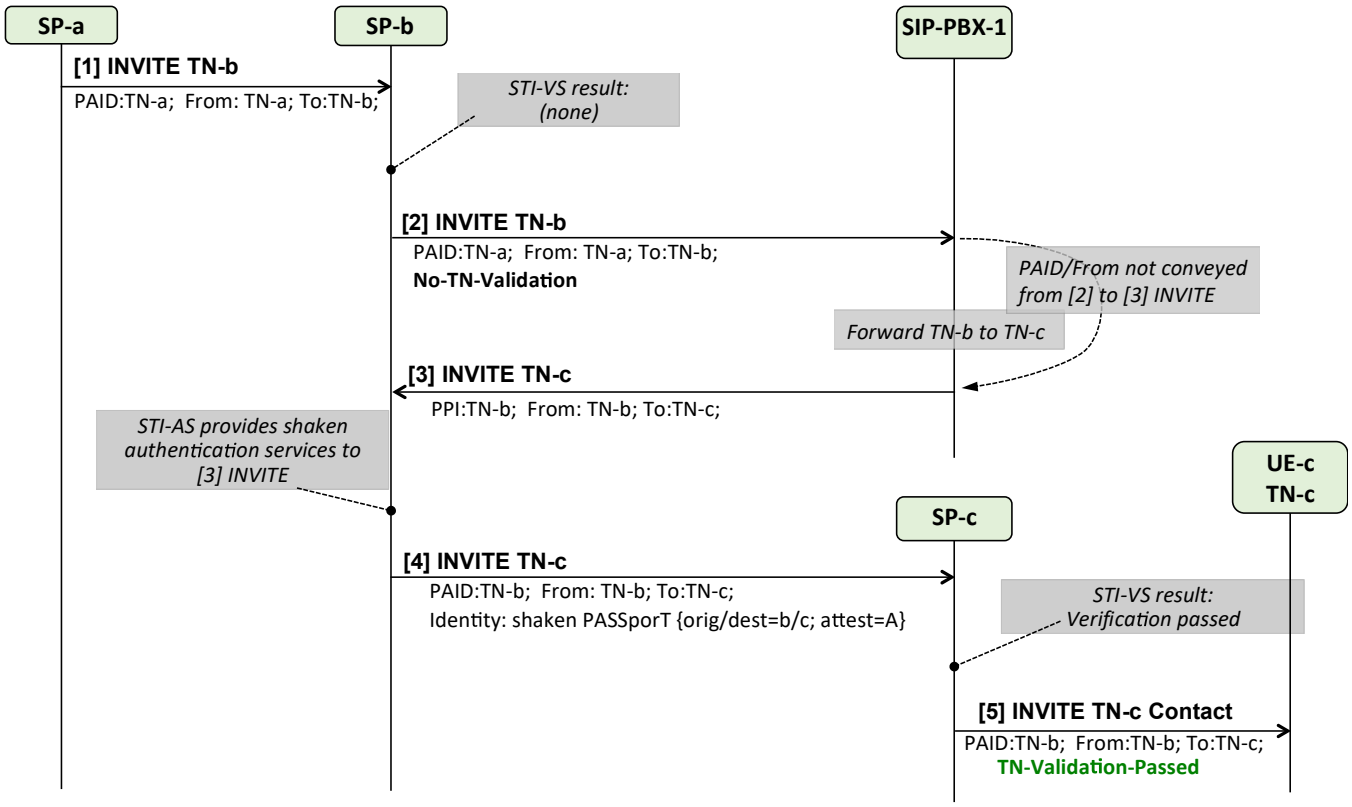

Figure A.10 – Case-4b – [1] INVITE contains no Identity header

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

As shown in Figure A.11, 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”.

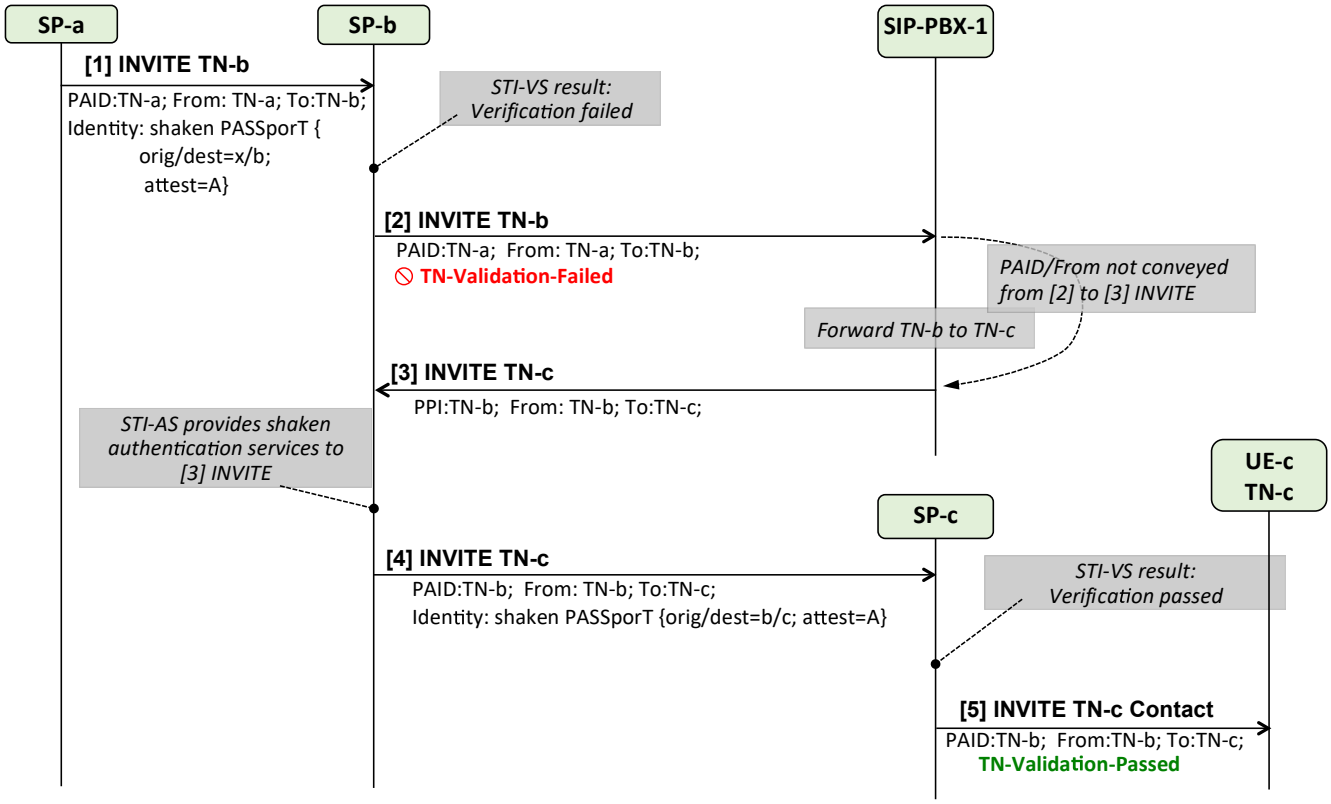

Figure A.11 – Case-4c – [1] INVITE contains invalid Identity header

Annex B – In-network Call Diversion Example for “div” PASSporT

This annex shows an example of a SIP Identity header containing a "div" PASSporT for the INVITE retargeting case where a call from TN-a to TN-b is forwarded to TN-c. The TN assignments used in the example are as follows:

- TN-a is 212-555-1212
- TN-b is 424-666-2323
- TN-c is 646-777-3434.

TN-a, TN-b, and TN-c are hosted by SP-a (example-1.net), SP-b (example2.net), and SP-c (example3.net) respectively.

During origination call processing, SP-a provides authentication services for calling TN-a by creating a “shaken” PASSporT containing a Protected header and Payload as specified in ATIS-1000074 [Ref 1]:

```
Protected Header
{
      "alg":"ES256",
      "ppt":"shaken",
      "typ":"passport",
      "x5u":"https://cert.example1.net/passport.cer"
}

Payload
{
      "attest":"A",
      "dest":{"tn":["14246662323"]},
      "iat":1538519401,
      "orig":{"tn":"12125551212"},
      "origid":"123e4567-e89b-12d3-a456-426655440000"
}
```

Per normal SHAKEN authentication procedures, SP-a adds an Identity header containing the resulting “shaken” PASSporT to the INVITE request sent to SP-b, as follows:

```
INVITE sip:+14246662323@tel.example2.net SIP/2.0
Via: SIP/2.0/UDP 10.36.78.177:60012;branch=z9hG4bK-524287-1---
77ba17085d60f141;rport
Max-Forwards: 69
Contact: <sip:+12125551212@69.241.19.12:50207;rinstance=9da3088f36cc528e>
To: <sip:+14246662323@tel.example2.net>
From: "Alice"<sip:+12125551212@tel.example1.net>;tag=614bdb40
Call-ID: 79048YzkxNDA5NTI1MzA0OWFjOTFkMmFlODhiNTI2OWQ1ZTI

P-Asserted-Identity: "Alice"<sip:+12125551212@tel.example1.net>,<tel:+12125551212>
CSeq: 2 INVITE
Allow: SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE, REFER, INFO, MESSAGE, OPTIONS
Content-Type: application/sdp
Date: Tue, 02 Oct 2018 16:30:01 GMT

Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9
jZXJ0LmV4YW1wbGUxLm5ldC9wYXNzcG9ydC5jZXIifQo=.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6W
yIxNDI0NjY2MjMyMyJdfSwiaWF0IjoxNTM4NTE5NDAxLCJvcmlnIjp7InRuIjoiMTIxMjU1NTEyMTIifSwi
b3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0K._28kAwRWnheXyA6nY4
MvmK5JKHZH9hSYkWI4g75mnq9Tj2lW4WPm0PlvudoGaj7wM5XujZUTb_3MA4modoDtCA;info=<https://
cert.example1.net/passport.cer>;alg=ES256;ppt="shaken"

Content-Length: 153
```

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

On receiving the above INVITE request, SP-b determines that the call is retargeted and then forwards the call to SP-c by retargeting the INVITE to forward-to TN TN-c. SP-b authenticates forwarding TN-b by creating a “div” PASSporT containing a Protected header and Payload as shown below. The Protected header “ppt” field is set to “div” to indicate that this PASSporT complies with draft-ietf-stir-passport-divert [Ref 4]. The “x5u” field references the SHAKEN certificate containing the public key that a remote terminating service can use to verify the "div" PASSporT signature.

```
Protected Header
{
      "alg":"ES256",
      "ppt":"div",
      "typ":"passport",
      "x5u":"https://cert.example2.net/passport.cer"
}
```

The PASSporT Payload “orig” claim is set to the “orig” claim of the received “shaken” PASSporT (TN-a), the “dest” claim is set to the new forward-to TN (TN-c), and the "div" claim is set to the forwarding TN (TN-b).

```
Payload
{
      "dest":{"tn":["16467773434"]},
      "div":{"tn":"14246662323"},
      "iat":1538519403,
      "orig":{"tn":"12125551212"}
}
```

SP-b adds a second Identity header containing the resulting “div” PASSporT to the retargeted INVITE request sent to SP-c, as follows:

```
INVITE sip:+16467773434@tel.example3.net SIP/2.0
Via: SIP/2.0/UDP 10.36.78.177:60012;branch=z9hG4bK-524287-1---
77ba17085d60f141;rport
Max-Forwards: 68
Contact: <sip:+12125551212@69.241.19.12:50207;rinstance=9da3088f36cc528e>
To: <sip:+14246662323@tel.example2.net>
From: "Alice"<sip:+12125551212@tel.example1.net>;tag=614bdb40
Call-ID: 79048YzkxNDA5NTI1MzA0OWFjOTFkMmFlODhiNTI2OWQ1ZTI
P-Asserted-Identity: "Alice"<sip:+12125551212@tel.example1.net>,<tel:+12125551212>
CSeq: 2 INVITE
Allow: SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE, REFER, INFO, MESSAGE, OPTIONS
Content-Type: application/sdp
Date: Tue, 02 Oct 2018 16:30:03 GMT
Diversion: <sip:+14246662323@tel.example2.net>;reason=unconditional
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9
jZXJ0LmV4YW1wbGUxLm5ldC9wYXNzcG9ydC5jZXIifQo=.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6W
```

```
yIxNDI0NjY2MjMyMyJdfSwiaWF0IjoxNTM4NTE5NDAxLCJvcmlnIjp7InRuIjoiMTIxMjU1NTEyMTIifSwi
b3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0K._28kAwRWnheXyA6nY4
MvmK5JKHZH9hSYkWI4g75mnq9Tj2lW4WPm0PlvudoGaj7wM5XujZUTb_3MA4modoDtCA;info=<https://
cert.example1.net/passport.cer>;alg=ES256;ppt="shaken"

Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6ImRpdiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ
0LmV4YW1wbGUyLm5ldC9wYXNzcG9ydC5jZXIifQo=.eyJkZXN0Ijp7InRuIjpbIjE2NDY3NzczNDM0Il19L
CJkaXYiOnsidG4iOiIxNDI0NjY2MjMyMyJ9LCJpYXQiOjE1Mzg1MTk0MDMsIm9yaWciOnsidG4iOiIxMjEy
NTU1MTIxMiJ9fQo=.rq3pjT1hoRwakEGjHCnWSwUnshd09zJ6F1VOgFWSjHBr8QjpjlkpcpFYpFYsojNCpT
zO3QfPOlckGaS6hEck7w;info=<https://cert.example2.net/passport.cer>;alg=ES256;ppt="d
iv"

Content-Length: 153


v=0
o=- 13103070023943130 1 IN IP4 10.36.78.177
s=-

c=IN IP4 10.36.78.177
t=0 0
m=audio 54242 RTP/AVP 0
a=sendrecv
```

On receiving the retargeted INVITE request, SP-c verifies the received "shaken" and “div” PASSporTs as specified in ATIS-1000074 [Ref 1] and in this specification, including verification that the “div” PASSporT provides an unbroken chain of authority between the Request-URI TN and the "shaken" PASSporT "dest" claim. In this example, the chain of authority is verified by checking that the canonicalized value of the received Request-URI TN “16467773434” matches the “div” PASSporT “dest” claim TN, and that the “div” PASSporT “div” claim TN “14246662323” matches the “shaken” PASSporT “dest” claim TN.