ATIS-1000095.v002

ATIS Standard on -

Extending STIR/SHAKEN over TDM

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.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF NOR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to https://www.atis.org/policy/patent-assurances/ to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Published by

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

ATIS-1000095.v002

ATIS Standard on

Extending STIR/SHAKEN over TDM

Alliance for Telecommunications Industry Solutions

Approved August 26, 2022

Abstract

The SHAKEN framework enables SHAKEN-authorized VoIP Service Providers to provide cryptographically protected attestation via SIP signaling that the calling user is authorized to use the calling telephone number. This specification extends the SHAKEN framework to enable conveyance of verified “shaken” attestation levels over TDM interconnects.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, 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 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.

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

The **Non-IP Call Authentication Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** was responsible for the development of this document.

At the time it approved this standard, the PTSC had the following leadership:

M. Dolly, PTSC Chair

V. Shaikh, PTSC Vice Chair

P. Linse, PTSC NIPCA TF Chair

Table of Contents

Table of Figures

Table of Tables

ATIS Standard on –

Extending STIR/SHAKEN over TDM

1 Scope, Purpose, & Application

1.1 Scope

The Signature-based Handling of Asserted information using toKENs (SHAKEN) framework enables a SHAKEN-authorized Voice over Internet Protocol (VoIP) Service Provider to deliver cryptographically protected attestation, via SIP signaling, that the calling user is authorized to use the calling telephone number. This specification extends the SHAKEN framework to enable conveyance of verified "shaken" attestation levels over Time Division Multiplexing (TDM) interconnects.

ATIS-1000097, *Technical Report on Alternatives for Caller Authentication for Non-IP Traffic*, which evaluates the viability of implementing this call authentication mechanism for TDM networks, should be considered along with this specification.

The mechanisms specified in this document are based on ITU Q.763 (12/1999), *Signalling System No. 7 – ISDN user part formats and codes*, rather than ATIS-1000113, *Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part*. However, a similar approach could be used for ATIS ISUP, taking into consideration that the parameters, code values, and procedures of ATIS ISUP are different from ITU-T ISUP and are not specified in this document.

1.2 Purpose

The current SHAKEN framework provides a set of tools that enable verification of the calling party's authorization to use a calling telephone number for a call. It assumes that the SIP Identity header can be carried end-to-end between Originating Service Providers (OSPs) and Terminating Service Providers (TSPs). Currently this is not always possible due to the use of TDM-based signaling at various segments of the end-to-end signaling path.

The mechanisms described in this document address this problem by carrying verified "shaken" attestation levels over TDM signaling.

2 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.

2.1 Normative References

[Ref 1] ATIS-1000073, *Technical Report on Use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information.*[1]

[Ref 2] ATIS-1000074, *ATIS Standard on Signature-based Handling of Asserted Information using toKENs (SHAKEN).*[1]

[Ref 3] ATIS-1000679, *Interworking Between Session Initiation Protocol (SIP) and ISDN User Part.*[1]

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

[Ref 4] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*[2]

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

[Ref 6] IETF RFC 4412, *Communications Resource Priority for the Session Initiation Protocol (SIP).*[2]

[Ref 7] IETF RFC 7135, *Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications.*[2]

[Ref 8] IETF RFC 7234, *Hypertext Transfer Protocol (HTTP/1.1): Caching.*[2]

[Ref 9] ITU Q.763 (12/1999), *Signalling System No. 7 – ISDN user part formats and codes.*[3]

[Ref 10] 3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3.*[4]

[Ref 11] 3GPP 29.163, *Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks 16.4.0.*[4]

[Ref 12] ITU Q.931, *ISDN user-network interface layer 3 specification for basic call control.*[3]

[Ref 13] ATIS-1000096, *Out-of-Band PASSporT Transmission Involving TDM Networks*.[5]

[Ref 14] ATIS-1000085, *Signature-based Handling of Asserted information using toKENs (SHAKEN): SHAKEN Support of "div" PASSporT.*[5]

2.2 Informative References

[Ref 100] ATIS-1000113, *Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part.*[5]

[Ref 101] ATIS-1000097, *Technical Report on Alternatives for Caller Authentication for Non-IP Traffic.*[5]

[Ref 102] IETF RFC 4904, *Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs).*[2]

3 Definitions, Acronyms, & Abbreviations

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

3.1 Definitions

The following provides some key definitions used in this document.

Private Key: In asymmetric cryptography, the private key is kept secret by the end-entity. The private key can be used for both encryption and decryption [IETF RFC 4949, *Internet Security Glossary, Version 2*].

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

3.2 Acronyms & Abbreviations

AIN	Advanced Intelligent Network

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

[3] Available from International Telecommunication Union (ITU) at: < https://www.itu.int/ >.

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

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

ASCII	American Standard Code for Information Exchange
ATIS	Alliance for Telecommunications Industry Solutions
CgPN	Calling Party Number
CDR	Call Detail Record
CVT	Call Validation Treatment
GW	Gateway
IETF	Internet Engineering Task Force
IAM	Initial Address Message
ISUP	Integrated Services Digital Network User Part
MLPP	Multilevel Precedence and Preemption
OCN	Operating Company Number
OSP	Originating Service Provider
PAI	P-Asserted-Identity
PASSporT	Personal Assertion Token
RPH	Resource Priority Header
SCP	Service Control Point
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SS7	Signaling System No. 7
STI	Secure Telephone Identity
STI-AS	Secure Telephone Identity Authentication Service
STI-VS	Secure Telephone Identity Verification Service
STIR	Secure Telephone Identity Revisited
TDM	Time Division Multiplexing
TG	Trunk Group
TSP	Terminating Service Provider
URI	Uniform Resource Identifier
UUI	User to User Information
VoIP	Voice over Internet Protocol

4 STIR/SHAKEN Extension over TDM Interconnect

4.1 Overview

Service provider and operator are used interchangeably throughout this document.

The ATIS SHAKEN framework [ATIS-1000074, *ATIS Standard on Signature-based Handling of Asserted Information using toKENs (SHAKEN)*] provides a set of tools that enable verification of the calling party's authorization to use a calling telephone number for a call. It assumes that the SIP Identity header [RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol*] can be carried end-to-end between OSPs and TSPs. Currently this is not always possible due to the use of TDM signaling in various network segments of the end-to-end signaling path. TDM network signaling is usually based on the Signaling System No. 7 (SS7) Integrated Services Digital Network User Part (ISUP) [Ref 9] protocol and the rest of this document assumes that this is the case.

The mechanisms described in this document address this problem by carrying verified attestation levels over TDM signaling.

The mechanisms rely on bilateral agreements and transitive trust between operators on each end of a TDM connection. The nature of the agreement, and whether there is an agreement at all is on a per-TDM-connection basis. Therefore, it is flexible in terms of its applicability. It covers all types of TDM connections as the agreement is only between directly connected operators. An operator may choose to have a different agreement or no agreement on each of its TDM interconnects. This allows partial upgrades and does not require any universal agreements. It also covers cases where several TDM connections need to be traversed in the signaling path of a call. In scenarios where a call traverses multiple TDM links and multiple service providers, bilateral agreements are required for every link and every service provider in the path. In the case of calls that traverse a TDM-to-TDM tandem/transit network that transparently passes signaling parameters between multiple peers, this may also require multi-lateral agreement between all service providers that may exchange traffic through the tandem/transit network. If even a single link is not covered by a bilateral agreement, or in some cases a multilateral agreement in a tandem/transit network, it will break the transitive trust and it will not be possible to convey the verified attestation levels end-to-end. As a result, the service providers must provision their network so that links covered by bilateral agreements are distinguished from links that are not covered by bilateral agreements to maintain the integrity of the transitive trust. In addition, service providers using this mechanism must monitor traffic incoming from ISUP links not covered by a bilateral agreement, and ensure that the ISUP parameters are set appropriately.

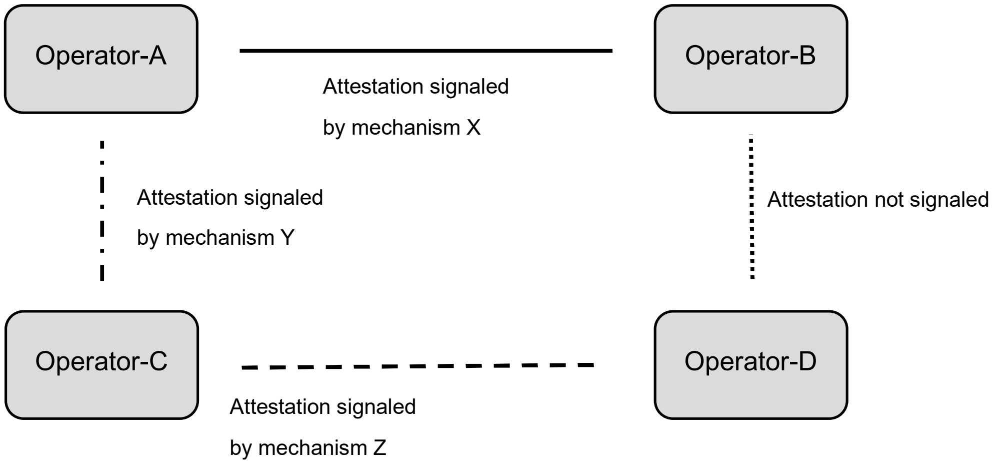


Figure 4-1: Use of different mechanisms among Operators

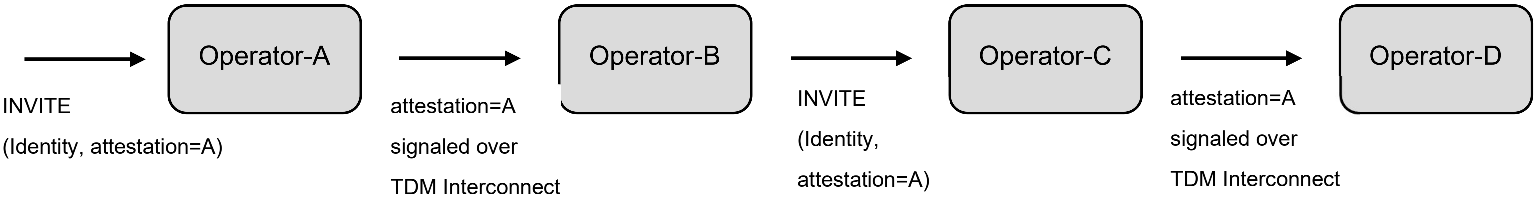


Figure 4-2: Carrying Attestation over multiple TDM Interconnects

This document identifies several possible ISUP parameters that could be used to signal SHAKEN attestation levels based on the bilateral agreements. If different approaches are used on different ISUP links, then ISUP nodes must modify the agreed ISUP parameters accordingly. It is also possible to use the same mechanism among several operators as long as they all agree to use the same mapping.

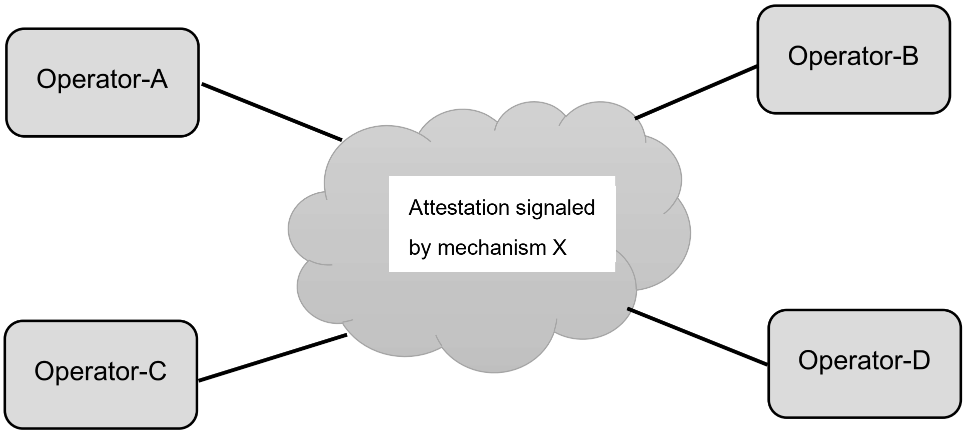


Figure 4-3: Carrying Attestation Among Multiple Operators

The STIR/SHAKEN relationship is terminated/re-generated on the two ends of the TDM interconnect. The terminating side of the STIR/SHAKEN relationship (i.e., the originating side of the TDM interconnect) signals the verified attestation level to the side re-generating the Personal Assertion Token (PASSporT) (i.e., the terminating side of the TDM interconnect). The terminating side of the TDM interconnect then re-generates the PASSporT by using the received attestation level and its own private key (i.e., Secure Telephone Identity (STI) certificate). This requires that each service provider generating a PASSporT be a member of the SHAKEN ecosystem and eligible to obtain STI certificates. Each STIR/SHAKEN relationship can be considered as a separate “STIR/SHAKEN leg”.

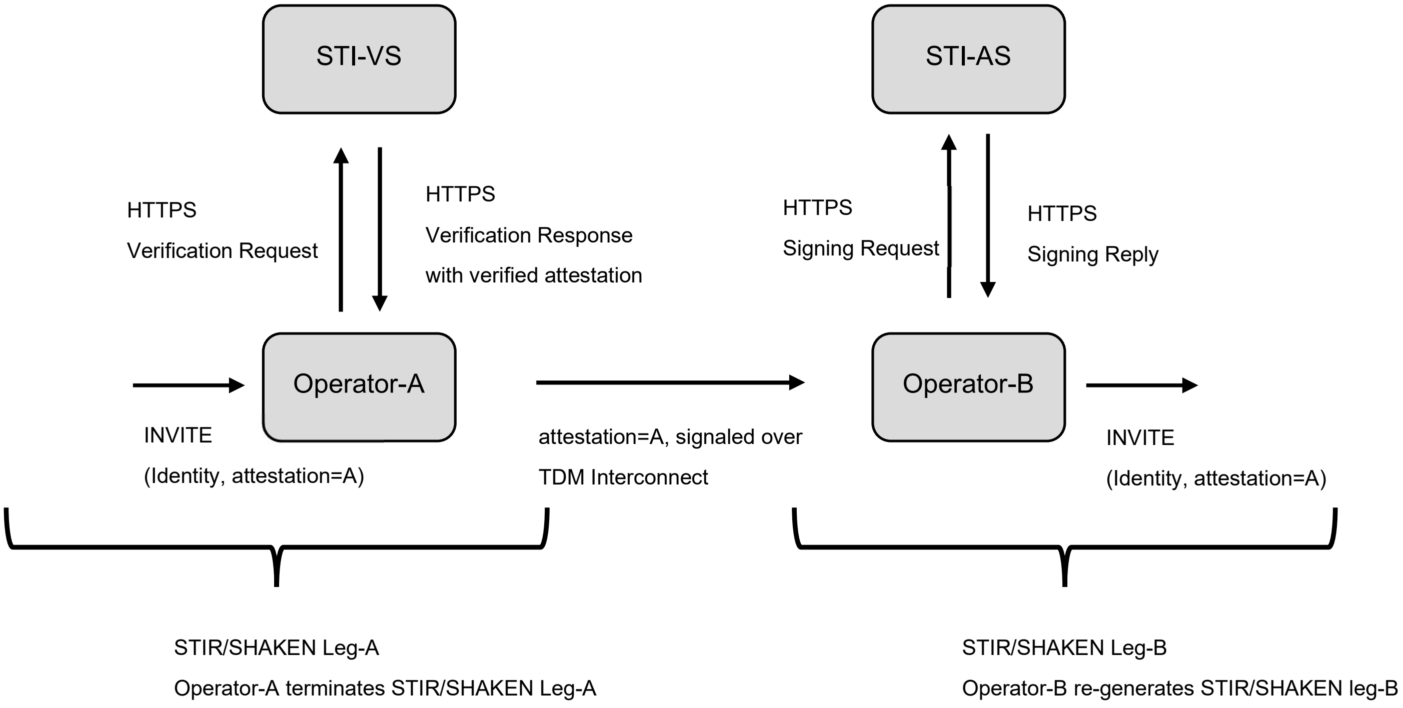

STI-VS
STI-AS
HTTPS
Verification Request
HTTPS
Verification Response
with verified attestation
HTTPS
Signing Request
HTTPS
Signing Reply
Operator-A
Operator-B
INVITE
(Identity, attestation=A)
attestation=A, signaled over
TDM Interconnect
INVITE
(Identity, attestation=A)
STIR/SHAKEN Leg-A
Operator-A terminates STIR/SHAKEN Leg-A
STIR/SHAKEN Leg-B
Operator-B re-generates STIR/SHAKEN leg-B

Figure 4-4: Extending STIR/SHAKEN over TDM Interconnect Architecture with Multiple STIR/SHAKEN Legs

4.2 Procedures

STIR/SHAKEN defines three attestation levels as “A”, “B”, and “C”. There is also the possibility of no Identity header, i.e., no attestation. The objective of the mechanism described in this standard is to signal the appropriate attestation value over a TDM interconnect. This document describes two high-level methods to achieve this objective:

- Use specific fields in the TDM signaling to encode the attestation level.
- Use a different Trunk Group (TG) for each attestation level.

- **TDM Signaling Based Model**

  In this model, different attestation levels need to be encoded using TDM signaling parameters. For example, this can be achieved by using the Screening Indicator in the ISUP Calling Party Number parameter.

  It should be noted that other parameters/bits could also be used for this purpose (e.g., spare bits in the second octet of Called Party Number parameter, spare bits of Call Reference, etc.) if the two ends of the TDM interconnect agree on their use and the attestation level they represent.

- **TG Based Model**

  In this model, all traffic within a TG would have the same verified attestation level. For example, TG-1 for “No Identity header received”, TG-2 for “A”, TG-3 for “B” and TG-4 for “C”.

Two operators may agree on signaling for only a subset of attestation levels (e.g., “No Identity received” and “A”) but this would need to be covered by the appropriate bilateral agreements.

To implement this specification, the following procedural steps are followed:

- The operator terminating the STIR/SHAKEN leg verifies the PASSporT in the INVITE Identity header.

- The operator terminating the STIR/SHAKEN leg signals the verified attestation value and the verification result over the TDM Interconnect based on the model agreed with the operator at the other end of the TDM Interconnect.
- If verification during STIR/SHAKEN leg termination was successful, the operator re-generating the STIR/SHAKEN leg generates a new “shaken” PASSporT with the attestation level it received over the TDM interconnect by using its own private key (i.e., STI certificate). It adds an Identity header including that PASSporT. Alternatively, a verstat parameter corresponding to the attestation level/verification result can be included. This is determined based on policy and deployment model.
- If verification during STIR/SHAKEN leg termination was not successful, the operator does not generate a new “shaken” PASSporT. It may apply Call Validation Treatment (CVT) or it may add a verstat parameter corresponding to the attestation level/verification result. Alternatively, CVT may be applied at the operator terminating the STIR/SHAKEN leg. This is determined by policy and deployment model.

4.2.1 Example Mappings with ISUP Screening Indicator

This clause and following sub-clauses explain the proposed solution by making use of the Screening Indicator in the ISUP Calling Party Number parameter.

- In total, the following values are all the possible combinations of attestation level and verification status that may be signaled over a TDM interconnect:
    - A: success
    - A: failure
    - B: success
    - B: failure
    - C: success
    - C: failure
    - No Identity header
- The 7 different outcomes above would require 3 bits, but there are only 2 bits available with the Screening Indicator. The next clause describes how attestation level can be passed using the 2 bits that are available.

4.2.1.1 TDM Interconnect

“TDM Interconnect” refers to the scenario where TDM is used to connect two SIP islands.

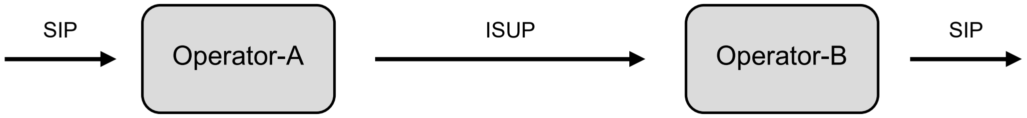


Figure 4-5: TDM Interconnect Topology

- Backtracing triggered by any verification failure should be performed by the egress leg (Operator-B).
    - Backtracing is performed by correlating Call Detail Records (CDRs) at each hop to find the previous hop until eventually the entity which has verified the PASSporT is reached. This would be the entity terminating the STIR/SHAKEN leg. The information present in a PASSporT can be used to deduce the operator/entity which created the PASSporT if relevant information from the PASSporT is saved in the CDR. Backtracing may also terminate in the TDM domain if it is detected that an entity did not properly follow the procedures described in this document and agreed upon between interconnecting operators, e.g., changing the ISUP Screening Indicator value inappropriately.
- CVT for any verification failure can/should be performed by the egress leg (Operator-B).
- It is not mandatory that Screening Indicator values be used consistent with their native ISUP meaning.
    - The goal is to map as much information as possible. The 2 bits are used mainly as placeholders.

  - Nonetheless, Screening Indicator values are used with their original meanings to provide consistent behavior with TDM Origination scenarios.

- Mapping from Identity verification to Screening Indicator:[6]

Table 4-1: Mapping from Identity verification to Screening Indicator

Attestation Level	Verification Status	Screening Indicator
A	Passed	11 – network provided
B	Passed	00 – user provided, not verified
C	Passed	00 - user provided, not verified
Any	Failed	10 - user provided, verified and failed
No Identity	<no verification>	00 - user provided, not verified

- Mapping from Screening Indicator to Identity header or to verstat (if Identity header is not to be further propagated):

Table 4-2: Mapping from Screening Indicator to Identity header or to verstat

Screening Indicator	Identity header generated with Attestation Level	verstat
01 - user provided, verified and passed (01 is not used for Identity to Screening Indicator mapping for interconnect scenarios per the mapping defined in this document. It may be used by an ATIS-1000679 [Ref 3] compliant entity or by an entity in TDM domain)	A	TN-Validation-Passed
10 - user provided, verified and failed	No Identity header	TN-Validation-Failed
11 - network provided	A	TN-Validation-Passed
00 - user provided, not verified	B/C or No Identity header based on policy	No-TN-Validation or not included based on policy

Within the TDM domain, the occurrence of certain conditions could break the transitive trust that is the basis for this mechanism. For example, if a call received from an untrusted entity may be redirected, but the Screening Indicator value is not adjusted accordingly, possibly due to limitations of existing TDM equipment. It is therefore important that the Screening Indicator in an ISUP Calling Party Number parameter be monitored at network ingress and changed to “user provided, not verified” if the call is coming from networks not adhering to this use of the indicator. Similarly, all elements that originate or redirect calls must assign the appropriate attestation level.

4.2.1.2 TDM Termination

“TDM Termination” refers to the scenario where TDM is used in the TSP’s network. The mapping described in this section is provided as an example. A TSP can decide how to make use of a received SIP Identity header with a PASSporT within TDM-based domains of its network. It is ultimately a local policy decision that may result in applying CVT, mapping it to an ISUP Screening Indicator, mapping it to another ISUP parameter, or ignoring it completely.

[6] Note that ATIS-1000113 [Ref 100] defines the Calling Party Number Screening Indicator value “01” as “user provided, screening passed”, value “00” as “user provided, not screened”, and value “10” as “user provided, screening failed”.

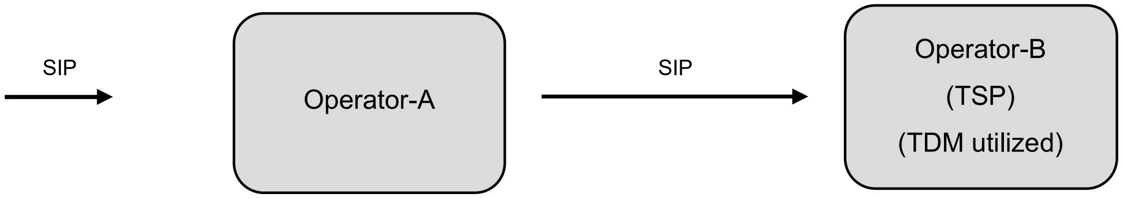


Figure 4-6: TDM Termination Topology

- Backtracing triggered by any verification failure can/should be performed by the egress leg (Operator-B/TSP)
- CVT for any verification failure can/should be performed by the egress leg (Operator-B/TSP)
- Screening Indicator values should be used consistently with their native ISUP meaning
  - They could be consumed by downstream ISUP entities
- Mapping from Identity verification status to Screening Indicator

Table 4-3: Mapping from Identity verification status to Screening Indicator

Attestation Level	Verification Status	Screening Indicator
A	Passed	11 – network provided
B	Passed	00 – user provided, not verified
C	Passed	00 - user provided, not verified
Any	Failed	10 - user provided, verified and failed
No Identity	<no verification>	00 - user provided, not verified

- No mapping is needed from Screening Indicator to Identity header or to verstat.
- CVT for TDM Termination can be provided by taking action (e.g., continue call, release call, play announcement) on the element performing SIP/ISUP STIR/SHAKEN conversion, or through an Advanced Intelligent Network (AIN) query to a Service Control Point (SCP) where the SCP can provide instructions about the action to be taken.

4.2.1.3 TDM Origination

“TDM Origination” refers to the scenario where TDM is used in the Originating Service Provider’s (OSP’s) network. Mapping in this section is provided as an example. An OSP can decide whether and how to make use of the ISUP Screening Indicator or some other ISUP parameter for STIR/SHAKEN authentication purposes, and generate a STIR/SHAKEN PASSporT accordingly.

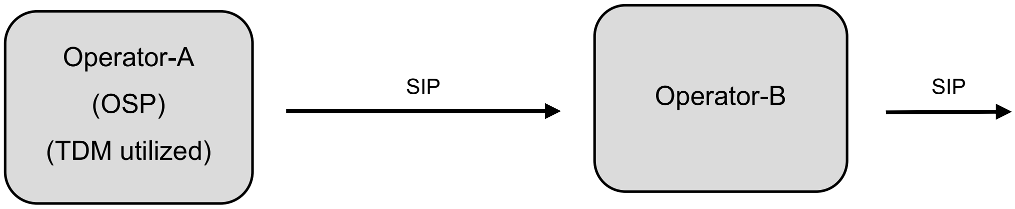


Figure 4-7: TDM Origination Topology

- Mapping from Screening Indicator to attestation level or to verstat (if Identity header is not to be further propagated) if TDM is using ISUP.

Table 4-4: Mapping from Screening Indicator to attestation level or to verstat

Screening Indicator	Attestation Level	Verstat
01 - user provided, verified and passed	A	TN-Validation-Passed
10 - user provided, verified and failed	No Identity header	TN-Validation-Failed
11 - network provided	A	TN-Validation-Passed
00 - user provided, not verified	B/C or No Identity header based on policy	No-TN-Validation or not included based on policy

- It is also possible to use ingress TG information or any other suitable factor to populate the SIP Identity header or to set the ISUP Screening Indicator for conversion to a SIP Identity header by a downstream element. This is essentially the authentication functionality, which is a matter of local policy and therefore is not specified by STIR/SHAKEN and can be done by any acceptable manner.
- For PBX connections, use of the Screening Indicator will depend on the deployment model and local policy. For example:
  - If no screening is provided, “00 – user provided, not verified” may always be used.
  - If screening is provided and the TN is assigned to the PBX, “10 – user provided, verified and passed” may be used.
  - If screening is provided and the TN is not assigned to the PBX, “00 – user provided, not verified” may be used.

Within the TDM domain, the occurrence of certain conditions could break the transitive trust that is the basis for this mechanism. For example, a call may be received from an untrusted entity and redirected, but the Screening Indicator value is not adjusted accordingly, possibly due to limitations of existing TDM equipment. It is therefore important that the Screening Indicator within the Calling Party Number parameter be monitored at network ingress and changed to “user provided, not verified” if the call is coming from networks not adhering to this use of the indicator. Similarly, all network elements that originate or redirect calls must assign the appropriate attestation level.

4.3 Backward Traceability

This mechanism terminates and re-generates the STIR/SHAKEN relationship but still allows for full backward traceability. On each STIR/SHAKEN leg, STIR/SHAKEN backward traceability procedures are applicable. The two STIR/SHAKEN legs would be tied to each other through Call Detail Record (CDR) backtracing. It should be noted that there are also attack/error scenarios applicable in an end-to-end STIR/SHAKEN model which still require CDR-based backtracing, e.g., corrupted origination-id in the PASSporT claim.

4.4 Diversion Impact

Verification of STIR/SHAKEN Identity header(s) applies to all claims/extensions at the STIR/SHAKEN termination. Therefore, "div" extension claims will be verified as well.

Bilateral agreement will determine whether only Identity("shaken") or both Identity("shaken") and Identity("div") headers will be generated based on TDM signaling diversion information. If the Request-URI and To header values of the INVITE generated at the egress STIR/SHAKEN leg are different, then "div" claim(s) must be generated.

If a verified diversion chain is used to populate TDM signaling diversion information during STIR/SHAKEN termination, then Identity(div) may be generated during STIR/SHAKEN re-generation.

ISUP Initial Address Message (IAM) Calling Party Number, Called Party Number, Redirecting Number and Original Called Party Number can be used to generate the PASSporT for "shaken" and "div" claims.

4.5 Support for Simultaneous Calls

Semi-simultaneous calls are multiple calls for which corresponding call signaling is received within a time period less than the STIR/SHAKEN freshness-check value in use.

Semi-simultaneous calls for the same calling/called party pair can happen for various reasons. For example, a single call may be forked upstream or there could be indeed multiple distinct calls originated, e.g., between a hospital and insurance company.

The mechanism described in this document fully supports such scenarios without any ambiguity regarding attestation level corresponding to each call because attestation level is carried as a component of the call signaling itself.

4.6 Support for Other Claim Types

Verification of STIR/SHAKEN Identity header(s) applies to all claims/extensions at the STIR/SHAKEN termination.

The hop-by-hop agreement characteristic of the mechanism makes it possible to utilize ISUP parameters for supporting additional claim types in a flexible way.

4.6.1 Support for “rph” Claim

"rph" claims for some services can be supported by using the ISUP “Calling Party’s Category” parameter[7] and ISUP “MLPP Precedence” parameter to convey an "rph" claim for a particular SIP “Resource Priority Header” (RPH) namespace and to set the appropriate SIP namespace priority value (i.e., the “r-priority” value). Similarly multiple TGs can be used where each of them corresponds to a different SIP RPH namespace and namespace priority value.

Whether to convey an “rph” claim by using the mechanisms defined in this document and if so, how, will be based on agreements among operators and outside of the scope of this document.

4.6.2 Support for “rcd” and “crn” Claims

The "nam" key of an "rcd" claim can be supported by using the Display Information parameter or Generic Name parameter.[8]

A "crn" claim, if used to provide information about the type of call (e.g., telemarketing, political, survey, or public-service) can be supported by making use of a parameter conveying information about the purpose of the call, e.g., the ISUP Originating Line Information parameter.[9] Any categories that do not correspond to an already defined value may be supported by using spare values based on bilateral agreement between the operators or in some cases multiple operators in a TDM-TDM switching network that passes signaling values transparently across TDM call legs.

In general, the ISUP User-to-User Information parameter may be used for any claim type as long as the required size does not exceed limits, and it is not being used by the end user.

[7] For example, an ISUP “Calling Party’s Category” parameter with a value of “high priority emergency service call” or "national security and emergency preparedness call" as specified in ATIS-1000113, Clause 3.8 [Ref 100] may be used to convey an "rph" claim for the “esnet” or “ets” SIP “Resource Priority Header” (RPH) namespace, respectively.

[8] See Chapter 3, Clause 3.20C of ATIS-1000113 [Ref 100] for details regarding the Generic Name parameter.

[9] See Chapter 3, Clause 3.26A of ATIS-1000113 [Ref 100] for details regarding the Originating Line Information parameter.

4.7 Security Concerns

The mechanism described in this standard relies on STIR/SHAKEN security principles on each STIR/SHAKEN leg and transitive trust on direct TDM connections between two operators.

Original STIR/SHAKEN authentication is verified at the STIR/SHAKEN Leg-A (see Figure 4-4). The result of this verification is signaled over a trusted TDM interconnect. The signaled value is used to re-construct the verified authentication level at the STIR/SHAKEN Leg-B (see Figure 4-4). As such, the original attestation level is not lost and is used verbatim; however, the origid and originating service provider information in the original PASSporT are not present in the newly generated PASSporT. That information can be retrieved as follows:

- On the terminating STIR/SHAKEN leg, "origid" is used to determine the entity which generated the new PASSporT;
- Backtracing based on stored CDRs is used to determine the entity which verified the original PASSporT on the originating STIR/SHAKEN leg;
- "origid" of the original PASSporT as stored in the CDR of the entity which verified the original PASSporT on the originating STIR/SHAKEN leg is used to determine the entity which created the original PASSporT.

TDM networks are generally interconnected in complicated ways with multiple paths between the ingress and egress points from and to a TDM network. There also are many types of trunks connected to the same network. It is imperative that all calls arriving at a TDM egress point, which will use this specification to recreate STIR/SHAKEN attestation or to directly inform a TDM connected user, must be received by a TDM network via a TDM trunk where there is a bilateral agreement to follow the specification. Calling number screening procedures are not widely used in North America and so existing service provider networks may not set Screening Indicator values in accordance with this usage. If existing TDM trunks with no prior design review deliver calls to a TDM egress point using this specification, it may be possible that spoofed calls in the TDM network will be signed with the transit carrier’s certificate at attestation level A. This will effectively launder the spoofed calls, much like dirty money can be unknowingly laundered through legitimate businesses. One way to mitigate this risk is to reconfigure all TDM trunks not using this specification to populate the Screening Indicator parameter as “00 – user provided, not verified”. In any case, correct provisioning of all portions of the call path using this specification is required, along with screening of TDM trunks from outside the trust domain defined by this specification.

4.8 Deployment Models

Existing gateway (GW) equipment at TDM interconnects may or may not have the capability or flexibility to apply the procedures associated with this mechanism. Lack of functionality support in GWs may be overcome by performing the necessary procedures in front-end/back-end entities. For example, a front-ending SIP entity may verify the Identity(“shaken”) signature, remove it, and populate the ISUP MIME body with corresponding parameter values. Similarly, at the other end of the TDM interconnect, a back-end entity may receive the INVITE with the ISUP MIME, which has the verified attestation level encoded in a parameter, and generate an Identity(“shaken”) header based on it.

Similarly, a front-end entity may insert SIP “trunk-context” and SIP ”tgrp” parameters specified in IETF RFC 4904, *Representing Trunk Groups in tel/sip Uniform Resource Identifiers*, into an INVITE to guide the GW in its selection of the TG on the TDM interconnect. Such a front-end entity would populate SIP “trunk-context”/”tgrp” parameters based on the verified attestation value.

The decision of if and how to use front-end/back-end entities to support these procedures does not require any coordination among operators. It is a decision to be made and applied solely within an operator’s own domain.

The concept of front-end/back-end entities can be applied in the TDM domain as well to provide the necessary SIP/ISUP STIR/SHAKEN conversion functionality if not supported by existing equipment.

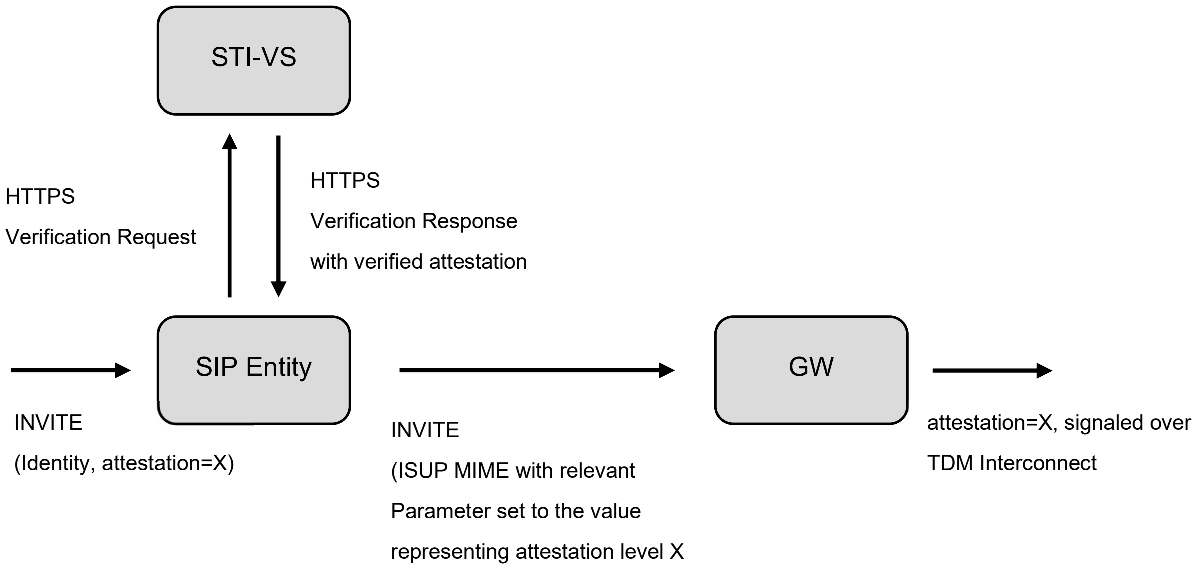
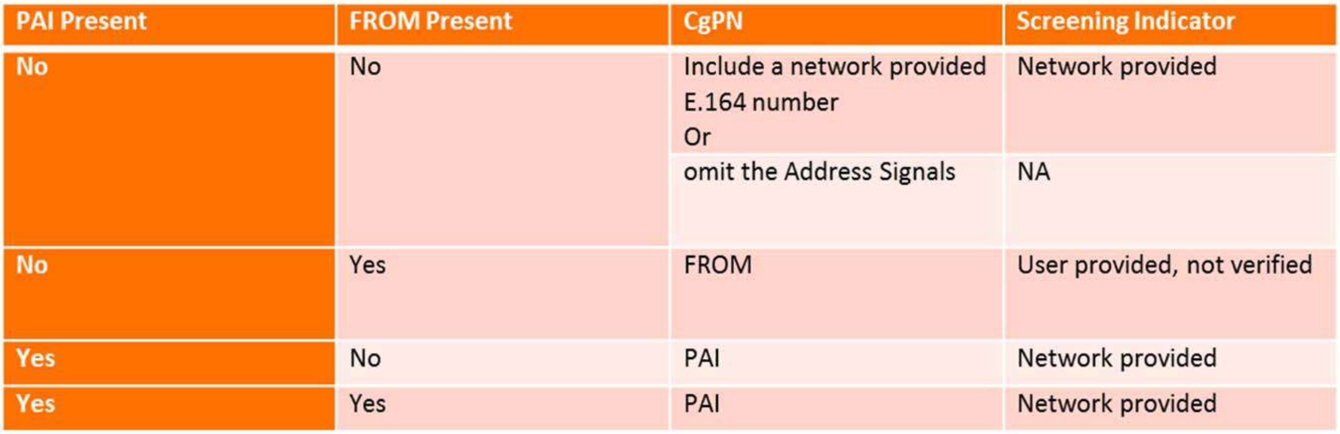

STI-VS
HTTPS
Verification Request
HTTPS
Verification Response
with verified attestation
SIP Entity
GW
INVITE
(Identity, attestation=X)
INVITE
(ISUP MIME with relevant
Parameter set to the value
representing attestation level X
attestation=X, signaled over
TDM Interconnect

Figure 4-8: SIP Front-End Entity Populating ISUP MIME Parameter for Attestation

4.9 Interworking with "ATIS-1000679, Interworking Between Session Initiation Protocol (SIP) And ISDN User Part"

ATIS-1000679, *Interworking Between Session Initiation Protocol (SIP) and ISDN User Part*, SIP/ISUP interworking is defined in the following table[10]:

Table 4-5: SIP/ISUP interworking



PAI Present	FROM Present	CgPN	Screening Indicator
No	No	Include a network provided E.164 number Or	Network provided
		omit the Address Signals	NA
No	Yes	FROM	User provided, not verified
Yes	No	PAI	Network provided
Yes	Yes	PAI	Network provided

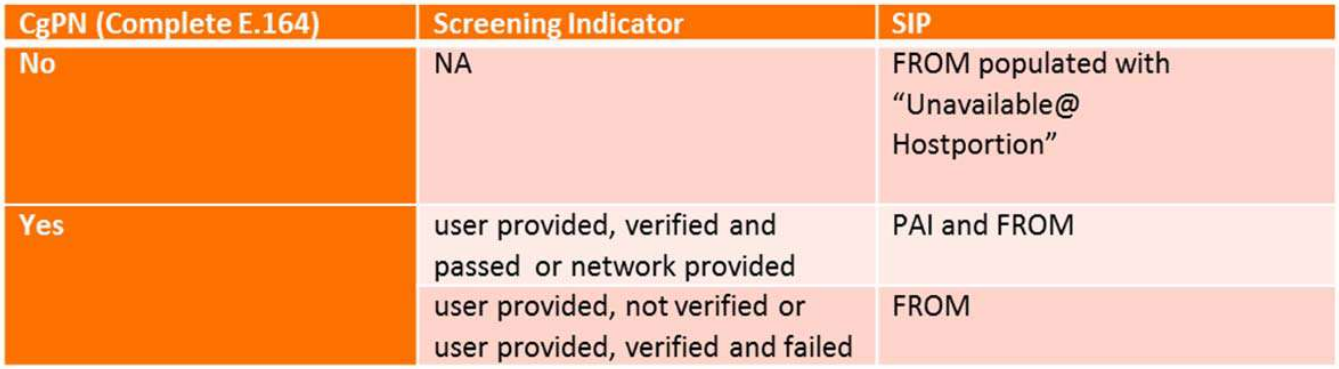
- The mechanism defined in this document uses a "network provided" Screening Indicator value when the verification result for a call is "A/Passed".

[10] This table is taken from ATIS-1000073, *Technical Report on Use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information*.

  - This semantically means “caller authenticated and corresponding attestation verified successfully”.
- ATIS-1000679 [Ref 3] SIP/ISUP mapping uses a “network provided” Screening Indicator when the calling party identifier can be trusted.
  - In P-Asserted-Identity (PAI) if user provided and authenticated.
  - In Calling Party Number (CgPN) if populated by the network.
- During SIP/ISUP interworking, the “network provided” value populated by equipment compliant with this document would be interpreted properly by network equipment compliant with ATIS-1000679 [Ref 3]. It would indicate that the received CgPN value is trusted.
- Similarly, a “network provided” value populated by equipment compliant with ATIS-10000679 [Ref 3] would be interpreted properly by equipment compliant with this document. It would indicate that the received CgPN value is trusted.

ATIS-1000679 [Ref 3] ISUP/SIP interworking is defined in the following table[11]:

Table 4-6: ISUP/SIP interworking



CgPN (Complete E.164)	Screening Indicator	SIP
No	NA	FROM populated with "Unavailable@ Hostportion"
Yes	user provided, verified and passed or network provided	PAI and FROM
	user provided, not verified or user provided, verified and failed	FROM

- The mechanism defined in this document maps a Screening Indicator value "network provided" or "user provided, verified and passed" to an Identity header with a PASSporT with attestation level (A).
- ATIS-1000679 [Ref 3] ISUP/SIP mapping populates a PAI with the CgPN if a "network provided" or "user provided, verified and passed" Screening Indicator value is received.
- During ISUP/SIP interworking, the "network provided" value populated by equipment compliant with this specification would be interpreted correctly by equipment compliant with ATIS-10000679 [Ref 3]. It would use CgPN as a trusted identity to populate relevant SIP header fields.
- Similarly, during ISUP/SIP interworking, the "network provided" or "user provided, verified and passed" values populated by equipment compliant with ATIS-10000679 [Ref 3] would be interpreted properly by equipment compliant with this document. It would add an Identity header with a PASSporT with attestation level (A).

4.10 Interworking with "3GPP 29.163 Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks"

- 3GPP 29.163, *Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks 16.4.0,* SIP/ISUP mapping rules are as follows:
  - The value "No-TN-Validation" to the value "user provided, not verified";
  - The value "TN-Validation-Passed" to the value "user provided, verified and passed"; and
  - The value "TN-Validation-Failed" to the value "user provided, verified and failed".
  - "Extending STIR/SHAKEN for TDM" specification maps "user provided, verified and passed" to TN-Validation-Passed.
    - A screening indicator parameter received from a 3GPP 29.163 [Ref 11] compliant sender would be interpreted properly by equipment in compliance with this document.

- 3GPP 29.163 [Ref 11] ISUP/SIP mapping rules are as follows:
  - If the MGCF performed mapping of the Calling party number parameter to the P-Asserted-Identity header field as defined in Table 14 [Ref 10] and the MGCF received the Calling party number with the Screening indicator set to value "user provided, verified and passed":

[11] This table is taken from ATIS-1000073 [Ref 1].

a) Set the value of the Attestation-Info header field to "B" (Partial Attestation) as described in 3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*; and

b) Use own address or identifier for creation of the Origination-Id header field as described in 3GPP TS 24.229 [9] [Ref 10]; or

- Otherwise, for all other mapping cases defined in Table 12 [Ref 10]:

a) Set the value of the Attestation-Info header field to "C" (Gateway Attestation) as described in 3GPP TS 24.229 [9] [Ref 10]; and

b) Use the received Circuit identification field (i.e., Circuit identification code) for creation of the Origination-Id header field as described in 3GPP TS 24.229 [9] [Ref 10].

- “Extending STIR/SHAKEN for TDM” specification never uses the “user provided, verified and passed” Screening Indicator value:
    - This will prevent a successful mapping for the Screening Indicator for a call sent by equipment compliant with this document and received by equipment compliant with 3GPP 29.163 [Ref 11]. It will not cause an improper escalation of attestation level and therefore is not harmful.
    - A change to 3GPP 29.163 [Ref 11] ISUP/SIP mapping rules so that “A” full attestation is used for the mapping of “user provided, verified and passed” would result in alignment.

4.11 PASSporT encoded in ISUP User-to-User Information (UUI) Parameter

This clause defines procedures to encode an STI PASSporT in the ISUP UUI parameter. This may allow interconnected TDM networks to preserve the original “shaken” PASSporT across a TDM domain under certain circumstances.

An OSP network can encode an STI PASSporT in an ISUP UUI parameter during call origination. Similarly, a transit provider network can encode an STI PASSporT in an ISUP UUI parameter during SIP-to-ISUP conversion. The TSP network can use the resulting ISUP UUI content to reconstruct an STI PASSporT during call termination processing. A transit provider can reconstruct the STI PASSporT from the ISUP UUI content during ISUP-to-SIP conversion. This PASSporT is used for verification in the TSP network or in a SIP Identity header as needed for signaling to downstream networks and elements.

This mechanism shall be used only if all the following criteria are met:

- The ISUP UUI parameter is not used for any other purpose;

  For example, to transfer user-network call control messages as defined in ITU Q.931, *ISDN user-network interface layer 3 specification for basic call control*,
- The encoded PASSporT size is less than 129 bytes;
- The encoded PASSporT size does not cause the ISUP IAM message size to exceed 232 bytes;
- Any PASSporT claims that are conveyed only in ISUP parameters and not encoded in an ISUP UUI parameter are aligned (e.g., “orig” claim and Calling Party Number parameter are aligned). Otherwise, the claims in the PASSporT won’t match the SIP headers after TDM-to-SIP interworking is applied.
- One of the following conditions is met:
    - the encoded PASSporT does not include a non-null “nam” claim, or
    - the call does not have Privacy (i.e., the ISUP Address presentation restricted indicator is not set to “presentation restricted”), or
    - it is known that another entity (e.g., the TSP) shall enforce the privacy procedures for the UUI parameter (i.e., prevent a UUI parameter with a “nam” claim from being sent to a user for a call with Privacy).

This mechanism may also be used if STIR/SHAKEN attestation information is received/derived by the TDM domain by first constructing a STIR/SHAKEN PASSporT based on it and then encoding that PASSporT in an ISUP UUI parameter.

This mechanism may also be used if STIR/SHAKEN attestation information is to be conveyed to the TDM domain by first constructing a STIR/SHAKEN PASSporT based on ISUP UUI content and then using relevant mechanisms to interwork it to TDM.

If an ISUP trunk terminates on a TDM end office that does not support the optional UUI parameter-based functionality specified in this document, there is a risk that STIR/SHAKEN PASSporT claims and signatures could be passed across a PRI interface to the terminating subscriber. The UUI parameter-based mechanism uses a dedicated UUI Protocol Discriminator value which may be used to distinguish this use case from other UUI use cases.

If the OSP does not support this optional UUI parameter-based functionality specified in this document, and if the ISUP UUI parameter in the PRI from an originating enterprise contains encoded STIR/SHAKEN PASSporT claims and signatures, as described in this document, then it is possible that the STIR/SHAKEN PASSporT claims and signatures could be passed into the network in the UUI parameter in ISUP signaling.

ISUP UUI encoding for “shaken” PASSporT information shall be encoded as in the following table:

Table 4-7: ISUP UUI encoding of “shaken” PASSporT information

Field	Bit Positions	Value	Definition
UUI protocol discriminator	0 – 7	0b01001010	ITU Q.931 [Ref 12], defines the use of the first byte of the ISUP UUI parameter to identify its intended use. This value specifies that it is used for an encoded STI PASSporT.
ppt/alg	8 – 13	0b000000	Defines the PASSporT type and algorithm used to generate the signature. This value represents a “shaken” PASSporT with “ES256” signature algorithm.
attest	14 – 15	0b00 = “A” 0b01 = “B” 0b10 = “C”	Attestation level
x5u	16 – 103		ASCII encoded URL without protocol (assumes HTTPS) . Most significant bytes are padded with NULL characters (“00000000”). Allows up to 11 characters.
iat	104 – 135		32-bit unsigned integer. Number of seconds since UNIX epoch
origid	136 – 263		128-bit UUID
Signature	264 – 775		PASSporT signature The provided length is for ES256. The length will vary depending on signature algorithm used.

An example of how a “shaken” PASSporT is encoded in ISUP UUI:

PASSporT to be encoded:

```
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ0LmV4YW
1wbGUub3JnL3Bhc3Nwb3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyIxMjEyNTU1MTIxMyJdfSwia
WF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1NTEyMTIifSwib3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQ
zLWE0NTYtNDI2NjU1NDQwMDAwIn0._V41ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUT
RTpQ5X0relYset-EScb9otFNDxOCTjerg
```

Protected Header:

```
    {
        "alg":"ES256",
        "typ":"passport",
        "ppt":"shaken",
            "x5u":"https://cert.example.org/passport.pem"
    }
```

Payload:

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

Signature (base64url):

V41ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-EScb9otFNDxOCTjerg

URL shortener:

https://bit.ly/3odj5jb

HTTP 301 response Location header:

Location: https://cert.example.org/passport.pem

“bit<"NULL”>ly3odj5” is encoded.

Table 4-8: ISUP UUI content for the “shaken” PASSporT to be encoded

Field	Value
UUI protocol discriminator	01001010
ppt/alg	000000
attest	00
x5u	01100010 01101001 01110100 0000000001101100 01111001 00110011 01101111 01100100 01101010 00110101
iat	01100000 01110000 11001011 01110000
origid	00010010 00111110 01000101 01100111 11101000 10011011 00010010 11010011 10100100 01010110 01000010 01100110 01010101 01000100 00000000 00000000
Signature	11111101 01011110 00110101 01001110 00010100 01001001 11101111 10000011 00100100 10110111 00010111 10001011 00011001 10100110 01010000 00011000 00001000 10101011 11110010 10010111 00001000 10111110 01100000 01111010 00111001 00000001 00001100 10000001 00101110 00011000 10011011 10110001 01001111 11000000 01101100 01100110 11011110 11010000 11010100 01001101 00010100 11101001 01000011 10010101 11110100 10101101 11101001 01011000

	10110001 11101011 01111110 00010001 00100111 00011011 11110110 10001011 01000101 00110100 00111100 01001110 00001001 00111000 11011110 10101110

4.11.1 OSP Procedures During ISUP Origination

The OSP network shall perform the following actions when originating a call via an ISUP interface:

- Check whether the criteria for using the ISUP UUI parameter to encode the PASSporT are met.
    - Execute the following steps only if criteria are met.
- Generate a shortened URL for the x5u field of the PASSporT as described in Clause 4.11.7 below.
- Encode the STI PASSporT in the ISUP UUI parameter as described in Clause 4.11 and subsequent clauses.

4.11.2 Procedures During SIP-to-ISUP Interworking

The SIP-to-ISUP interworking entity shall perform the following actions:

- Populate the ISUP Screening Indicator in the Calling Party Number parameter as specified in previous clauses, if there is an appropriate bilateral or multilateral agreement to use it for conveyance of SHAKEN attestation level.
- Check whether the criteria for using the ISUP UUI parameter to encode the PASSporT are met.
    - Execute the following steps only if criteria are met.
- Generate a shortened URL for the x5u field of the PASSporT as described in Clause 4.11.7 below.
- Encode the STI PASSporT in an ISUP UUI parameter as described in Clause 4.11 and subsequent clauses.

4.11.3 Procedures During ISUP-to-SIP Interworking

The ISUP-to-SIP interworking entity shall perform the following actions:

- Verify whether the ISUP UUI parameter includes an encoded PASSporT.
    - Check whether the first byte of the UUI parameter is “01001010”.
    - Check that “iat” value is not earlier than two days before the interworking entity’s current clock time.
    - Check that “iat” value is not later than two days after the interworking entity’s current clock time.
    - Check that the ISUP UUI parameter size is consistent with the expected value based on the ppt/alg value in the UUI parameter.
        - For “shaken”/ES256, expected UUI size is 97 bytes.
    - Execute the following steps only if verification succeeds.

- Send an HTTPS request the URL encoded in the ISUP UUI parameter x5u field.
    - If a 301/302/307/308 response is received, use the Location header value from the response as the “x5u” value for the PASSporT that is reconstructed.
        - The Location header is expected to contain the long-form URL corresponding to the short-form URL provided in the GET Request-URI to the URL shortener.
        - The ISUP-to-SIP interworking entity does not need to retrieve the certificate to encode the PASSporT. For efficiency, it should not generate an HTTPS GET request to the redirected location.
    - If a non-3xx response (e.g., 404, 498) is received then do not reconstruct an STI PASSporT.
        - This could correspond to the case where the URL is shortened but the URL shortener was not able to provide the long-form URL due to a failure.

- Reconstruct the STI PASSporT based on ISUP UUI parameter content, other relevant ISUP parameters, and the URL shortener response.
- Add a SIP Identity header which includes the reconstructed PASSporT to the next-hop SIP INVITE.

4.11.4 TSP Procedures During ISUP Termination

The TSP ISUP UUI verification function shall perform the following actions upon receiving an ISUP IAM containing an ISUP UUI parameter:

- Verify whether the ISUP UUI parameter includes an encoded PASSporT.
    - Check whether the first byte of the UUI parameter is "01001010".
    - Check that "iat" value is not earlier than two days before the interworking entity's current clock time.
    - Check that "iat" value is not later than two days after the interworking entity's current clock time.
    - Check that the ISUP UUI parameter size is consistent with the expected value based on the ppt/alg value in the UUI parameter.
        - For "shaken"/ES256, expected UUI size is 97 bytes.
    - Execute the following steps only if verification succeeds.

- Send an HTTPS request to the URL encoded in the ISUP UUI parameter x5u field.
    - If a 301/302/307/308 response is received, use the Location header value from the response as the "x5u" value for the PASSporT that is reconstructed.
        - The Location header is expected to contain the long-form URL corresponding to the short-form URL provided in the GET Request-URI to the URL shortener.
        - The TSP PASSporT reconstruction logic does not need to retrieve the certificate to encode an STI PASSporT. For efficiency, it should not generate an HTTPS GET request to the redirected location.
    - If a non-3xx response (e.g., 404, 498) is received then do not reconstruct an STI PASSporT.
        - This corresponds to the case where the URL is shortened but the URL shortener was not able to provide the long-form URL due to a failure.
- Reconstruct the STI PASSporT based on ISUP UUI parameter content, other relevant ISUP parameters, and the URL shortener response.
- Send the STI PASSporT and related call processing parameters to the TSP's STI-VS via SIP or other application-specific means for verification per the rules of the PASSporT type.

4.11.5 Procedures for TDM Domain Entities Transiting ISUP

Entities in the TDM domain transiting ISUP shall transparently pass the ISUP UUI parameter, unless discarding the UUI parameter is required due to size limits.

4.11.6 Procedures for TDM Domain Entities Manipulating ISUP IAM Content

Some entities that both receive and send signaling within the TDM domain may manipulate ISUP IAM parameters which pertain to STIR/SHAKEN claims, e.g., calling party number, called party number. This, for example, could happen due to call forwarding performed by the entity. Such entities that also implement STI PASSporT encoding and decoding in the ISUP UUI parameter shall perform the following actions to generate a new PASSporT with modified claims and encode it in the ISUP UUI parameter.

- Verify the ISUP UUI contents per the procedures of Clause 4.11.4 above and re-create the associated STI PASSporT.
- Verify the STI PASSporT utilizing the call processing parameters received in the IAM before manipulation. Execute the following steps only if verification succeeds:

- Generate a new STI PASSporT including the modified ISUP parameters/claims
- Strip the previous ISUP UUI parameter, Encode the new generated PASSporT in an ISUP UUI parameter by following the procedures applicable for SIP-to-TDM interworking entities
- Include the new ISUP UUI parameter in the next-hop ISUP IAM.

TDM-domain entities that modify call processing procedures but that do not implement STI PASSporT encoding, decoding, verification, and PASSporT creation in ISUP UUI are expected to transit the original PASSporT encoded in ISUP UUI, in which case verification at the TSP is expected to fail.

4.11.7 x5u URL Procedures

ISUP UUI PASSporT encoding uses an 11-byte field to encode the x5u. The value in this field points to a shortened URL. The x5u present in a PASSporT to be encoded in a UUI parameter is always shortened.

Encoding of the shortened URL shall follow the following rules:

- The URL protocol is not included in the encoding.
- The second level domain is 4 characters long.
    - The second level domain is padded with NULL characters if it is shorter than 4 characters.
- The top level domain is 2 characters long.
- A "." is not included between the second level domain and the top level domain.
- The path is 5 characters long.
- The path does not include any file extension.
- The path does not contain any query/fragment components.

Examples:

"https://rome.is/spqr" is encoded as "<romeisspqrNULL>"

"https://ro.me/spqr" is encoded as "ro<NULL><NULL>mespqr<NULL>"

When reconstructing the x5u URL from the encoded UUI PASSporT, it shall be prefixed with "https://".

A SIP-to-TDM interworking entity may use the same long form URL/shortened URL mapping for an amount of time determined by local policy.

A TDM-to-SIP interworking entity may cache a shortened URL based on the expiry duration as specified in the response from the URL shortener.

The full form of the URL shall be used by the TDM-to-SIP interworking entity when reconstructing a PASSporT to populate the "x5u" parameter of the PASSporT header.

The URL shortener shall only accept HTTPS requests. The URL shortener shall listen for requests on port 443. The URL shall implement the cache control behavior described in IETF RFC 7234, *Hypertext Transfer Protocol (HTTP/1.1): Caching*. The URL shortener HTTP response shall include the "Cache-Control" header with a "public" cache directive and "max-age" cache directive. The "max-age" cache directive shall contain a value of at least 86,400 seconds (24 hours). Additional non-conflicting cache directives may be included.

4.11.8 Support for "shaken" PASSporT Optional Claims and Other PASSporT Types

A SIP INVITE request may contain a "shaken" PASSporT with optional claims, e.g., "rcd" claims, and PASSporTs of a type other than "shaken", e.g., "div", "rph", "rcd" instead of or in addition to the "shaken" PASSporT. Optionally, the following procedures may be followed to transfer the protected claim information associated with these PASSporTs over the TDM domain in a cryptographically secure manner.

If multiple PASSporTs of different types are present and only if some of them are supported by the SIP-to-TDM interworking entity, then procedures shall only be applied to the supported PASSporT(s).

If multiple PASSporT(s) of different types are present and if verification succeeds for only some of them, then the PASSporT(s) for which verification failed shall not be interworked. PASSporT(s) for which verification succeeds may/or may not be interworked depending on policy.

The term "PASSporT generation" means preparing a new PASSporT based on claims received in multiple PASSporTs or in ISUP IAM parameters. A new signature is generated and used with the private key of the entity performing this operation. This operation is performed in two steps:

- First, a new "shaken" PASSporT is created including all claims. This "shaken" PASSporT is identical to a "shaken" PASSporT which would be prepared to be used for end-to-end SIP STIR/SHAKEN deployment model.
- Then, the new "shaken" PASSporT is encoded in ISUP UUI parameter by following procedures specified in this document.

The term "PASSporT reconstruction" means preparing an STI PASSporT which is equivalent to the PASSporT encoded in the ISUP UUI parameter. All information for this reconstructed PASSporT, including the signature, is equivalent to the PASSporT information encoded in the ISUP UUI parameter. The procedure is just syntactical.

If a SIP-to-TDM interworking entity receives all claims in a single PASSporT, then the original PASSporT shall be encoded in ISUP UUI parameter. If SIP-to-TDM entity receives claims in multiple PASSporTs of different types, then it shall generate a new PASSporT including all claims and encode this new PASSporT in ISUP UUI parameter. Note that any of the following procedures that involve generating new PASSporTs do not maintain the identity of the entity or entities that populated and signed the PASSporTs received in the incoming SIP signaling.

A “shaken” claim is encoded in ISUP UUI as follows:

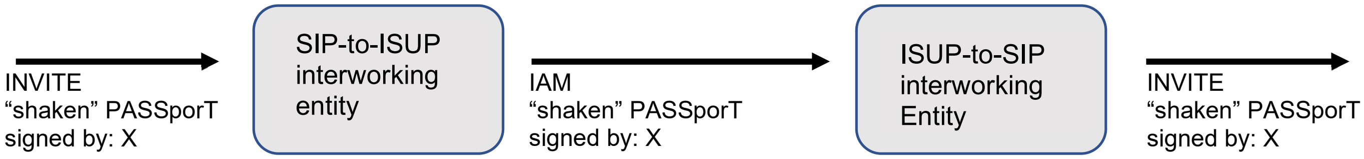


Figure 4-9: PASSporT(“shaken”) transferred via ISUP UUI

4.11.8.1 Summary of “ppt/alg” Field Usage

Table 4-9: Summary of “ppt/alg” Field Usage

Use Case	ppt/alg value (for ES256 signature algorithm)
“shaken” PASSporT	0b000000
“shaken” / “div” PASSporT	0b000100
“shaken PASSporT/ “nam” “crn” claim	0b001000
“shaken” / “div” PASSporT/ ”nam” “crn” claim	0b001100
“rph” PASSporT	0b010000
“shaken” / ”rph” PASSporT	0b010100
“shaken” / “div” / ”rph” PASSporT	0b011000
“shaken” / “rph” PASSporT / “nam” “crn” claim	0b011100
“shaken” / “div” / “rph” PASSporT / “nam” “crn” claim	0b100000

When an OSP supports this procedure and receives a UUI parameter over the PRI with the UUI PASSporT discriminator, then it should treat it as a PASSporT and not merely transport it transparently.

4.11.8.2 Support For “div” Claim

ISUP IAM message size limits and ISUP UUI parameter size limits will not allow for the encoding of more than one PASSporT in a UUI parameter. Therefore, entities supporting “div” claim interworking with PASSporTs encoded in the ISUP UUI parameter shall execute the following procedure upon receiving a SIP INVITE containing a “shaken” PASSporT and one or more “div” PASSporT(s).

A SIP-to-TDM interworking entity that supports “div” claim interworking with PASSporTs encoded in ISUP UUI shall execute the following procedure upon receiving a SIP INVITE containing a "shaken” PASSporT and one or more “div” PASSporTs:

- Verify the “shaken” and “div” PASSporTs using the procedures defined in ATIS-1000085, *Signature-based Handling of Asserted information using toKENs (SHAKEN): SHAKEN Support of "div" PASSporT* . Execute the following steps only if verification succeeds:
- Generate a “shaken” PASSporT based on the following rules:
  - The “ppt/alg” field is set as defined in the “Summary of “ppt/alg” field usage” table.
  - The “attest” field is populated with the “attest” claim value of the received “shaken” PASSporT.

    - The “x5u” field of the UUI parameter is populated with the shortened URL information for the public key of the interworking organization.
    - The “iat” field is populated based on current time.
    - The “origid” field is populated with a value based on the local policy of the SIP-to-TDM interworking entity.
    - The “orig” field is populated with “orig” claim of the received “shaken” PASSporT.
    - The “dest” field is populated with the “dest” claim of the received “div” PASSporT. If there are more than one “div” PASSporTs then the last one in the chain is used.
    - A signature is generated by using the private key of the SIP-to-TDM interworking entity.
- The “shaken” PASSporT is encoded in the ISUP UUI parameter.

A TDM-to-SIP interworking entity supporting “div” claim interworking that receives an ISUP IAM containing a UUI parameter indicating an encoded PASSporT shall execute the following procedure:

- Check the “ppt/alg” field. Execute the following steps only if its value indicates that “div” PASSporT was interworked as defined in “Summary of “ppt/alg” field usage” table.
- Reconstruct a “shaken” PASSporT based on the PASSporT encoded in ISUP UUI using the procedures defined in Clause 4.11.3.
- Populate the To header and Request-URI of the next-hope SIP INVITE with the destination value from the IAM representing the last retarget-to user.

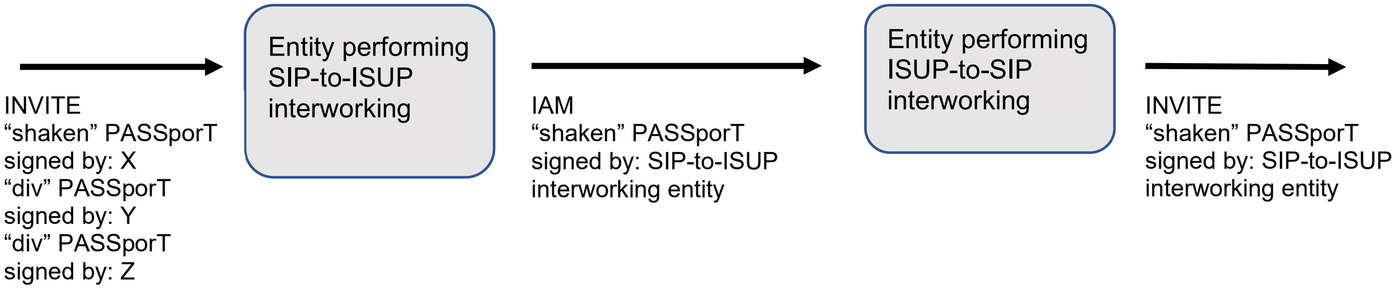

INVITE
“shaken” PASSporT
signed by: X
“div” PASSporT
signed by: Y
“div” PASSporT
signed by: Z
Entity performing SIP-to-ISUP interworking
IAM
“shaken” PASSporT
signed by: SIP-to-ISUP interworking entity
Entity performing ISUP-to-SIP interworking
INVITE
“shaken” PASSporT
signed by: SIP-to-ISUP interworking entity

Figure 4-10: “shaken” PASSporT/”div” PASSporT transferred via ISUP UUI

4.11.8.3 Support For “rph” and “sph” Claims

The use case combinations for “rph” described in Table 4-10 can be generalized as follows:

- An “rph” PASSporT without any other PASSporT, and
- An “rph” PASSporT together with a “shaken” PASSporT (including other claims) and other PASSporTs (e.g., “div”).

If an “rph” PASSporT is received without any other PASSporT, then the SIP-to-TDM interworking entity shall directly encode the “rph” PASSporT in the ISUP UUI with its original signature, following the procedures as described below. The SIP-to-TDM interworking entity does not generate a new PASSporT in this instance.

There is no standardized approach to interwork “rph” claims into ISUP parameters and then back to “rph” claims. Any such interworking requires bilateral agreement between the SIP-to-ISUP interworking entity and ISUP-to-SIP interworking entity to ensure that they follow the same semantics regarding SIP headers and ISUP parameters and their values used for this purpose. Therefore, “rph” claims shall be encoded in dedicated fields in ISUP UUI parameter.

ISUP IAM/ISUP UUI parameter size limitations do not allow encoding more than one PASSporT. Therefore, if an “rph” PASSporT is received together with a “shaken” PASSporT, the SIP-to-ISUP interworking entity shall generate a new “shaken” PASSporT with “rph” claims and sign it when allowed by regulatory rules and policy agreements to convey it in the ISUP IAM/ISUP UUI parameter.

“rph” claims present in an ISUP UUI shall not be used to generate “rph” claims in a “rph” PASSporT if the corresponding regulatory rules do not allow it. For example, regulation may require that this interworking shall be performed only if the ISUP-to-SIP interworking entity has authority over the relevant namespaces. Some other regulation may allow this interworking to be performed by any ISUP-to-SIP interworking entity in possession of an STI signing key by assuming that proper use of namespace values is already asserted by an upstream entity with authority to do so and the interworking entity merely is extending this assertion.

Because of the unique characteristics of emergency services (911) architectures, use of the ISUP UUI parameter for encoding “rph” claim with “esnet.1” resource priority value is out of scope.

SIP-to-ISUP interworking entities that support interworking of “rph” PASSporT claims with PASSporTs encoded in ISUP UUI shall execute the following procedure upon receiving a SIP INVITE containing an “rph” PASSporT:

- Verify the received “rph” PASSporT. Execute the following steps only if verification succeeds and if the namespace value(s) in the “rph” claim are in the set of namespaces supported by the encoding rules. If multiple namespaces are present in the “rph” claim and if they have different values, then at most two namespaces are supported.
    - Supported namespaces are “drn”, “drsn”, “q.735”, “ets”, “wps” as defined in IETF RFC 4412, *Communications Resource Priority for the Session Initiation Protocol (SIP)*, and “esnet” as defined in IETF RFC 7135, *Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications*.
- The ISUP UUI PASSporT encoding fields are populated as follows:
    - The “protocol discriminator” is populated as defined in “Summary of “ppt/alg” field usage” table.
    - The “ppt/alg” field is populated as follows:
        - 0b010000 if only an “rph” PASSporT is to be interworked.
        - 0b010100 if “shaken” and “rph” PASSporTs are to be interworked.
        - 0b011000 if “shaken” PASSporT, “div” PASSporT and “rph” PASSporT are to be interworked.
        - 0b011100 if “shaken” PASSporT with “nam” claim and “rph” PASSporT are to be interworked.
        - 0b100000 if “shaken” PASSporT with “nam” and “div” claims and “rph” PASSporT are to be interworked.
        - These values assume use of ES256 as the signature algorithm.
    - The “attest” field is populated with the value corresponding to the “attest” claim value of the received “shaken” PASSporT if a “shaken” PASSporT is to be interworked, otherwise any value can be populated.
    - The “x5u” field of the UUI parameter is populated with the URL information for the public key of the interworking organization.
        - URL shortening procedures are followed as applicable.
    - The “iat” field is populated based on current time.
    - The “origid” field is populated with a value representing the SIP-to-TDM interworking entity.
    - The “rph namespace” field is populated as follows:
        - The most significant bit is populated as 0b1 if the “dsn” namespace is present in the “rph” claim. It is populated as 0b0 otherwise.
        - The second most significant bit is populated as 0b1 if the “drsn” namespace is present in the “rph” claim. It is populated as 0b0 otherwise.
        - The third most significant bit is populated as 0b1 if the “q735” namespace is present in the “rph” claim. It is populated as 0b0 otherwise.
        - The fourth most significant bit is populated as 0b1 if the “ets” namespace is present in the “rph” claim. It is populated as 0b0 otherwise.

        - The fifth most significant bit is populated as 0b1 if the “wps” namespace is present in the “rph” claim. It is populated as 0b0 otherwise.
        - The sixth most significant bit is populated as 0b1 if the “esnet” namespace is present in the “rph” claim. It is populated as 0b0 otherwise.
    - The “rph namespace value-1” field is populated with the binary representation of the first namespace present in the “rph” claim. Ordering is based on the list as specified in the previous rule, e.g., if both “wps” and “ets” namespaces are present in the “rph” claim then the value of “ets” namespace shall be used.
    - The “rph namespace value-2” field is populated with the binary representation of the second namespace present in the “rph” claim if the namespaces have different values. Otherwise, it is populated with the binary representation of the first namespace present in the “rph” claim.
    - “rph” namespace priority values are encoded as using the field values in ascending order.
        - e.g., lowest priority as 0b000, second lowest priority as 0b001, etc.
    - The “sph indicator” field is populated as 0b1 if the “sph” claim was present in the “rph” PASSporT. Otherwise, it is populated as 0b0.

TDM-to-SIP interworking entities that implement interworking of “rph” claims in PASSporTs encoded in an ISUP UUI parameter to “rph” PASSporTs shall execute the following procedure upon receiving an IAM with a PASSporT encoded in ISUP UUI:

- Check the “ppt/alg” field value for a value indicating that the “rph” PASSporT was interworked as defined in the “Summary of “ppt/alg” field usage” table. If one of the indicated values is present, reconstruct the indicated STI PASSporT type (e.g., “rph” PASSporT or “shaken” PASSporT with “rph” claims).
- Verify the reconstructed STI PASSporT signature received in the ISUP UUI. Execute the following steps only if verification is successful.
- If the “ppt/alg” field value contains a value indicating a “shaken” PASSporT has been interworked, generate an Identity header with a “shaken” PASSporT based on the ISUP UUI parameter content, not including the “rph” claim.
- In addition, depending on regulatory status of the entity performing the TDM-SIP interworking, a separate Identity header with an “rph” PASSporT may be generated based on the ISUP UUI parameter content. In that instance, “rph namespace”, “rph value-1”, “rph value-2”, and “sph” field values are used when generating the “rph” PASSporT.

ISUP UUI “rph” PASSporT information shall be encoded as in the following table:

Table 4-10: ISUP UUI encoding of “rph” and "shaken" PASSporT information

Field	Bit Positions	Value	Definition
UUI protocol discriminator	0 - 7	0b01001010	ITU Q.931 [Ref 12], defines use of the first byte of ISUP UUI to identify its intended use. This value specifies that it is used for the encoded STI PASSporT.
ppt/alg	8 - 13	0b010000/ 0b010100/ 0b011000	Defines the PASSporT type and algorithm used to generate the signature. This value represents an “rph” PASSporT with “ES256” signature algorithm. Interworking of “rph” PASSporT when “crn”/”nam” claims are present is covered in Clause 4.11.8.5.
attest	14 - 15	0b00 = “A” 0b01 = “B” 0b10 = “C”	Attestation level
x5u	16 - 103		ASCII encoded URL without protocol (assumes HTTPS). Most significant bytes are padded with NULL characters (“00000000”). Allows up to 11 characters.

iat	104 - 135		32-bit unsigned integer. Number of seconds since UNIX epoch
origid	136 - 263		128-bit UUID
rph namespace	264 - 269		A bitmap of namespaces present in the “rph” claim. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
Spare	270 - 271		Reserved for future use. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
rph namespace value-1	272 - 274		The first rph namespace value to be used for “rph” claim interworking Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
rph namespace value-2	275 - 277		The second rph namespace value to be used for “rph” claim interworking Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
sph indicator	278		A flag indicating whether “sph” claim is present. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
Spare	279		Reserved for future use. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
Signature	280 - 791		PASSporT signature The provided length is for ES256. The length would vary depending on signature algorithm used.

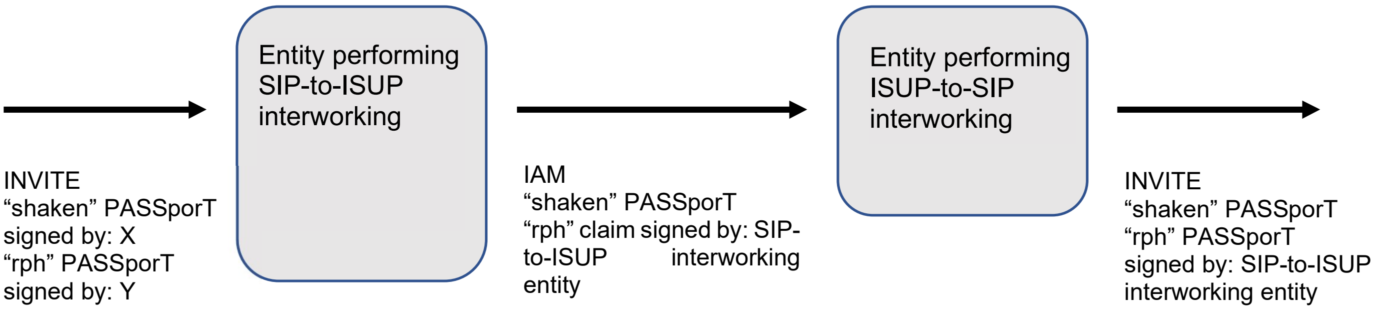

Entity performing SIP-to-ISUP interworking
Entity performing ISUP-to-SIP interworking
INVITE
“shaken” PASSporT
signed by: X
“rph” PASSporT
signed by: Y
IAM
“shaken” PASSporT
“rph” claim signed by: SIP-to-ISUP interworking entity
INVITE
“shaken” PASSporT
“rph” PASSporT
signed by: SIP-to-ISUP interworking entity

Figure 4-11: “shaken” PASSporT/“rph” PASSporT related parameters transferred via ISUP UUI

4.11.8.4 Support For “rcd” Claim

There are different ways to present an “rcd” claim in a PASSporT. Use of the ISUP UUI parameter to transfer “rcd”-related information is different for each and is defined in the following sub-clauses.

Two different mechanisms are defined to transfer “rcd” claims:

- The first mechanism relies on use of ISUP Display Information/Generic Name parameters. It can carry only “nam” claims. The SIP-to-TDM interworking entity may combine “nam” and “crn” claims into a single “nam” claim. This may be done, for example, by concatenating the two claim values, e.g., “nam” claim value “Bank-A” and “crn” claim value “Fraud Alert”, resulting in a new “nam” claim with the value “Bank-A Fraud Alert”. It should be noted that combining “nam” and “crn” claim values would increase the ISUP IAM message size. One or both claim values may be abbreviated to address size concerns.
    - This mechanism shall be followed only if ISUP parameters relevant for transferring “nam” claim can pass through the TDM domain. It never shall be used if the “nam” claim to be transferred is blank/empty string.
- The second mechanism encodes “nam” and “crn” claims in a new variable length field after the “signature” field. There is no explicit “nam/crn size” field as all the other fields have fixed lengths and ISUP UUI parameter size can be used to deduce the size of “nam/crn field”. The claim values are encoded as ASCII. 0b00011110 (ASCII Record Separator) is used as delimiter between “nam” and “crn” claims.
    - If ISUP UUI parameter size exceeds the combined length of all defined fields up to and including the “signature” field, then “nam” and/or “crn” claims are encoded in ISUP UUI.
    - If ISUP UUI parameters size matches the combined length of all defined fields up to and including the “signature” field, then it indicates that “nam” claim is used to populate ISUP Display Information/Generic Name parameter.
    - Empty “nam”/”crn” claims are encoded in ISUP UUI “nam crn claim field” as follows:

Table 4-11: “nam”, “crn” claim encoding in ISUP UUI “nam crn field”

nam	crn	nam crn claim field
“”	not present	
“”	“”	0b00011110
“”	“foo”	0b00011110“foo”
“foo”	not present	“foo”
“foo”	“”	“foo”0b00011110
“foo”	“bar”	“foo”0b00011110“bar”

ISUP UUI encoding for “shaken” PASSporT information with “nam”, and “crn” claims (“nam” and “crn” claims encoded in ISUP UUI) [Table 4-12]:

Table 4-12: ISUP UUI encoding for “shaken” PASSporT information with “nam” & “crn” claims

Field	Bit Positions	Value	Definition
UUI protocol discriminator	0 – 7	0b01001010	ITU Q.931 [Ref 12], defines use of the first byte of ISUP UUI to identify its intended use. This value specifies that it is used for encoded STI PASSporT.
ppt/alg	8 – 13	0b001000/ 0b001100	Defines the PASSporT type and algorithm used to generate the signature.
attest	14 – 15	0b00 = “A” 0b01 = “B” 0b10 = “C”	Attestation level
x5u	16 – 103		ASCII encoded URL without protocol (assumes HTTPS). Most significant bytes are padded with NULL characters (0b00000000). Allows up to 11 characters.
iat	104 – 135		32-bit unsigned integer. Number of seconds since UNIX epoch
origid	136 – 263		128-bit UUID
Signature	264 – 775		PASSporT signature The provided length is for ES256. The length would vary depending on signature algorithm used.
nam crn	776 – end of UUI		ASCII encoded nam and crn claims. Record separator character (0b00011110) used to separate nam and crn. The separator is not included if no crn is included. Allows up to 29 characters combined between nam and crn or 30 characters for nam if only nam is included.

ISUP UUI “shaken”, “nam”, and “crn” claims (“nam” and “crn” claims used to populate ISUP Display Information/Generic Name parameter) shall be encoded as in the following table [Table 4-13]:

Table 4-13: ISUP UUI encoding for “shaken” PASSporT information with “nam” & "crn” claims in other ISUP parameters

Field	Bit Positions	Value	Definition

UUI protocol discriminator	0 – 7	0b01001010	ITU Q.931 [Ref 12], defines use of the first byte of ISUP UUI to identify its intended use. This value specifies that it is used for encoded STI PASSporT.
ppt/alg	8 – 13	0b001000/ 0b001100	Defines the PASSporT type and algorithm used to generate the signature.
attest	14 – 15	0b00 = "A" 0b01 = "B" 0b10 = "C"	Attestation level
x5u	16 – 103		ASCII encoded URL without protocol (assumes HTTPS). Most significant bytes are padded with NULL characters (0b00000000). Allows up to 11 characters.
iat	104 – 135		32-bit unsigned integer. Number of seconds since UNIX epoch
origid	136 – 263		128-bit UUID
Signature	264 – 775		PASSporT signature The provided length is for ES256. The length would vary depending on signature algorithm used.

4.11.8.4.1 Only "nam" & "crn" claim(s) present as part of the PASSporT("shaken")

If only a "nam" claim is included in "shaken" PASSporT in addition to standard "shaken" claims, then the "shaken" PASSporT can be transferred via ISUP UUI as already defined.

SIP-to-TDM interworking entities that implement interworking of "rph" claims in PASSporTs encoded in an ISUP UUI parameter to "rph" PASSporTs shall execute the following procedure upon receiving an IAM with a PASSporT encoded in ISUP UUI:

- "ppt/alg" field is populated as defined in the "Summary of "ppt/alg" field usage" table.
- All the other steps for encoding a "shaken" PASSporT in the ISUP UUI are followed.
- If "nam"/"crn" claim(s) are encoded in the ISUP UUI, the "rcd nam crn" field is populated. Otherwise, the "nam" claim is used to populate the ISUP Display Information/Generic Name parameter.

TDM-to-SIP interworking entities that implement interworking of "rph" claims in PASSporTs encoded in an ISUP UUI parameter to "rph" PASSporTs shall execute the following procedure upon receiving an IAM with a PASSporT encoded in ISUP UUI:

- The "ppt/alg" field value is checked. Subsequent steps are followed only if its value matches one of the values for "nam/crn" as defined in the "Summary of "ppt/alg" field usage" table.
- A "shaken" PASSporT with a "nam"/"crn" claim(s) is reconstructed based on ISUP UUI content. If the ISUP UUI parameter size indicates that the "rcd nam crn" field is not included, then the ISUP Display Information/Generic Name parameter is used to populate the "nam" claim in the reconstructed PASSporT.

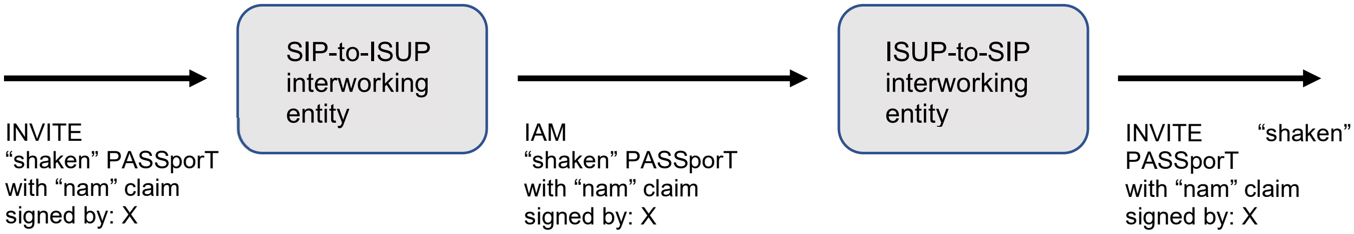


Figure 4-12: "shaken" PASSporT with "nam" claim transferred via ISUP UUI

4.11.8.4.2 "nam"/"crn" claim together with some other "rcd" claims present as part of the "shaken" PASSporT

If the "nam" claim together with some other "rcd" claims is present as part of the "shaken" PASSporT, then the SIP-to-TDM interworking entity validates the PASSporT and generates a new "shaken" PASSporT with a "nam"/"crn" claim(s) based on the received PASSporT.

SIP-to-TDM interworking entities that implement interworking of "rph" claims in PASSporTs encoded in an ISUP UUI parameter to "rph" PASSporTs shall execute the following procedure upon receiving an IAM with a PASSporT encoded in ISUP UUI:

- The received "shaken" PASSporT with "rcd" claims is verified. Execute the following steps only if verification succeeds.
- A new "shaken" PASSporT with "nam"/"crn" claim(s) is generated based on the claims present in the received "shaken" PASSporT. This new PASSporT is signed with the private key of the SIP-to-TDM interworking entity.
- The newly generated "shaken" PASSporT is transferred via the ISUP UUI parameter in the same way as in the "Only "nam"/"crn" claim(s) are present as part of the "shaken" PASSporT" case.

TDM-to-SIP interworking entities that implement interworking of "rph" claims in PASSporTs encoded in an ISUP UUI parameter to "rph" PASSporTs shall execute the following procedure upon receiving an IAM with a PASSporT encoded in ISUP UUI:

- The same procedures as "Only "nam"/"crn" claim(s) present as part of "shaken" PASSporT case" are followed.

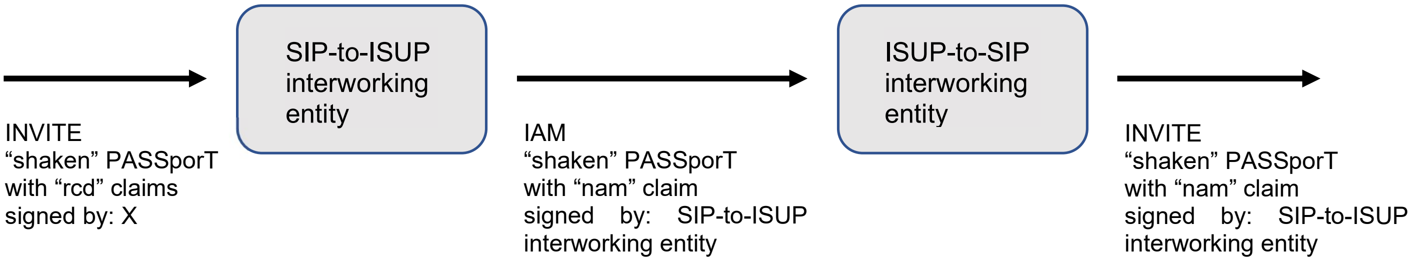

SIP-to-ISUP interworking entity
ISUP-to-SIP interworking entity
INVITE
"shaken" PASSporT
with "rcd" claims
signed by: X
IAM
"shaken" PASSporT
with "nam" claim
signed by: SIP-to-ISUP interworking entity
INVITE
"shaken" PASSporT
with "nam" claim
signed by: SIP-to-ISUP interworking entity

Figure 4-13: "shaken" PASSporT with "rcd" claims transferred via ISUP UUI

4.11.8.4.3 "nam"/"crn" claim(s) alone or together with some other "rcd" claims present in "rcd" PASSporT

If "nam"/"crn" claim(s) alone or together with other "rcd" claims are received in a dedicated "rcd" PASSporT, both the "shaken" PASSporT and the "rcd" PASSporT shall be verified. A new "shaken" PASSporT with a "nam"/"crn" claim(s) shall be generated by the SIP-to-TDM interworking entity. This new "shaken" PASSporT shall be transferred via the ISUP UUI parameter.

SIP-to-TDM interworking entities that implement interworking of “rph” claims in PASSporTs encoded in an ISUP UUI parameter to “rph” PASSporTs shall execute the following procedure upon receiving an IAM with a PASSporT encoded in ISUP UUI:

- The received “shaken” PASSporT and “rcd” PASSporT are verified. Execute the following steps only if verification succeeds.
    - Behavior when both or only one of the PASSporTs fails verification is policy driven. For example, the SIP-to-TDM interworking entity could pass only the “shaken” PASSporT if the “shaken” PASSporT verification succeeds and the “rcd” PASSporT verification fails.
- A new “shaken” PASSporT with a “nam”/“crn” claim(s) is generated based on the claims present in the received “shaken” PASSporT and “rcd” PASSporT. This new PASSporT is signed with the private key of the SIP-to-TDM interworking entity.
    - If all the received PASSporTs have the same “origid” value then that value is used to populate “origid”. Otherwise, the “origid” field is populated with a value representing the SIP-to-TDM interworking entity.
- The newly generated “shaken” PASSporT is transferred via the ISUP UUI parameter in the same way as in the “Only “nam”/“crn” claim(s) present are part of the “shaken” PASSporT” case.

TDM-to-SIP interworking entities that implement interworking of “rph” claims in PASSporTs encoded in an ISUP UUI parameter to “rph” PASSporTs shall execute the following procedure upon receiving an IAM with a PASSporT encoded in ISUP UUI:

- The same procedures as for the “Only “nam”/“crn” claim(s) present as part of “shaken” PASSporT” case are followed.

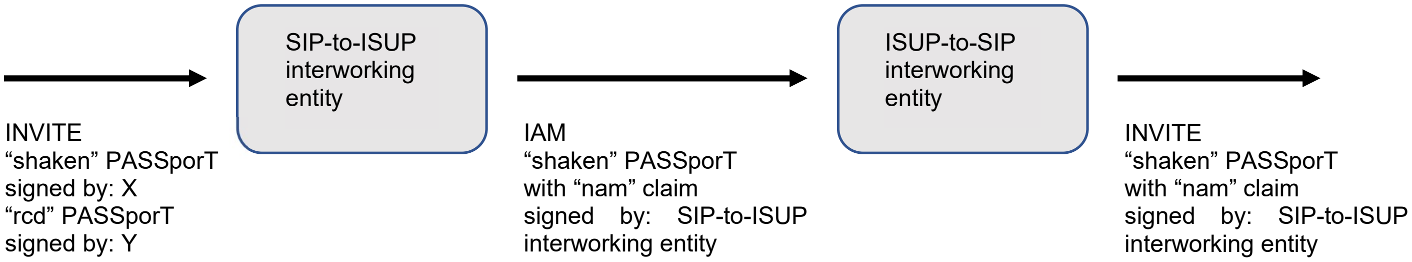

SIP-to-ISUP interworking entity
ISUP-to-SIP interworking entity
INVITE
“shaken” PASSporT
signed by: X
“rcd” PASSporT
signed by: Y
IAM
“shaken” PASSporT
with “nam” claim
signed by: SIP-to-ISUP interworking entity
INVITE
“shaken” PASSporT
with “nam” claim
signed by: SIP-to-ISUP interworking entity

Figure 4-14: “shaken” PASSporT/”rph” PASSporT transferred via ISUP UUI

4.11.8.5 Support For “shaken”, “rph”, and “rcd” Claims

Simultaneous support for “shaken”, “rph”, and “rcd” claims is handled the same as described in the relevant clauses for each claim. The only difference is the value used for “ppt/alg” field in the ISUP UUI parameter.

The ISUP UUI parameter “shaken”, “rph”, “rcd”, and “nam”/“crn” claims (“nam”/“crn” claims populated in the ISUP UUI parameter) shall be encoded as in the following table [Table 4-14]:

Table 4-14: ISUP UUI encoding of “rph” & “shaken” PASSporT information with “nam” & “crn” claims

Field	Bit Positions	Value	Definition
UUI protocol discriminator	0 - 7	0b01001010	ITU Q.931 [Ref 12], defines use of the first byte of ISUP UUI to identify its intended use.

			This value specifies that it is used for encoded STI PASSporT.
ppt/alg	8 - 13	0b011100/ 0b100000	Defines the PASSporT type and algorithm used to generate the signature. This value represents a “shaken” PASSporT with “ES256” signature algorithm.
attest	14 - 15	0b00 = “A” 0b01 = “B” 0b10 = “C”	Attestation level
x5u	16 - 103		ASCII encoded URL without protocol (assumes HTTPS). Most significant bytes are padded with NULL characters (“00000000”). Allows up to 11 characters.
iat	104 - 135		32-bit unsigned integer. Number of seconds since UNIX epoch
origid	136 - 263		128-bit UUID
rph namespace	263 - 269		A bitmap of namespaces present in the “rph” claim. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
Spare	270 - 271		Reserved for future use. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
rph namespace value-1	272 - 274		The first rph namespace value to be used for “rph” claim interworking Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
rph namespace value-2	275 - 277		The second rph namespace value to be used for “rph” claim interworking Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
sph indicator	278		A flag indicating whether “sph” claim is present. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
Spare	279		Reserved for future use. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
Signature	280 - 791		PASSporT signature The provided length is for ES256. The length would vary depending on signature algorithm used.
nam crn	792 – end of UUI		ASCII encoded nam and crn claims. Record separator character (0b00011110) used to separate nam and crn. The separator is not included if no crn is included. Allows up to 29 characters combined between nam and crn or 30 characters for nam if only nam is included.

ISUP UUI “shaken”, “rph”, “rcd”, “nam”, and “crn” claims (“nam” and “crn” claims used to populate ISUP Display Information/Generic Name parameter) shall be encoded as in the following table [Table 4-15]:

Table 4-15: ISUP UUI encoding of “rph” & “shaken” PASSporT information with “nam” & “crn” claims in other ISUP parameters

Field	Bit Positions	Value	Definition
UUI protocol discriminator	0 - 7	0b01001010	ITU Q.931 [Ref 12], defines use of the first byte of ISUP UUI to identify its intended use. This value specifies that it is used for encoded STI PASSporT.
ppt/alg	8 - 13	0b011100/ 0b100000	Defines the PASSporT type and algorithm used to generate the signature. This value represents a “shaken” PASSporT with “ES256” signature algorithm.
attest	14 - 15	0b00 = “A” 0b01 = “B” 0b10 = “C”	Attestation level
x5u	16 - 103		ASCII encoded URL without protocol (assumes HTTPS). Most significant bytes are padded with null characters (“00000000”). Allows 10 characters.
iat	104 - 135		32-bit unsigned integer. Number of seconds since UNIX epoch
origid	136 - 263		128-bit UUID
rph namespace	264 - 269		A bitmap of namespaces present in the “rph” claim. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
Spare	270 - 271		Reserved for future use. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
rph namespace value-1	272 - 274		The first rph namespace value to be used for “rph” claim interworking Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
rph namespace value-2	275 - 277		The second rph namespace value to be used for “rph” claim interworking Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
sph indicator	278		A flag indicating whether “sph” claim is present. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
Spare	279		Reserved for future use. Optional, present only if “ppt/alg” field indicates that “rph” claim is interworked.
Signature	280 - 791		PASSporT signature The provided length is for ES256. The length would vary depending on signature algorithm used.

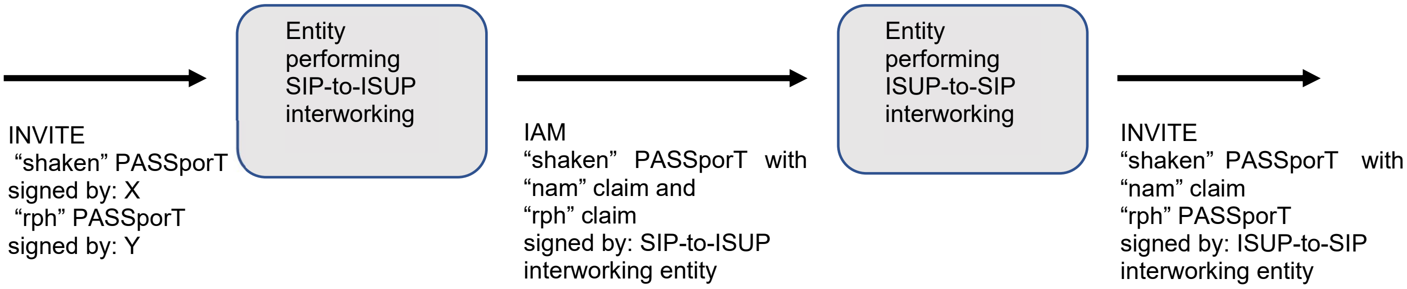

INVITE
"shaken" PASSporT
signed by: X
"rph" PASSporT
signed by: Y
Entity performing SIP-to-ISUP interworking
IAM
"shaken" PASSporT with "nam" claim and "rph" claim
signed by: SIP-to-ISUP interworking entity
Entity performing ISUP-to-SIP interworking
INVITE
"shaken" PASSporT with "nam" claim
"rph" PASSporT
signed by: ISUP-to-SIP interworking entity

Figure 4-15: "shaken" PASSporT/"rph" PASSporT/"rcd" PASSporT transferred via ISUP UUI

4.12 Combining Methods

Multiple methods of carrying verified "shaken" attestation levels over TDM signaling are described in this document and in ATIS-1000096 [Ref 12]. These methods are:

- Using Trunk Groups as described in Clause 4.2,
- Using ISUP Screening Indicator as described in Clause 4.2,
- Using the ISUP UUI parameter as described in Clause 4.11, and
- Using the Out-of-Band method to transport PASSporTs as described in ATIS-1000096 [Ref 12].

These methods may be implemented individually or multiple methods can be implemented together.

When multiple methods are implemented by an OSP or a SIP-to-TDM interworking entity, the rules for each method must be followed – e.g., if the ISUP Screening Indicator method has been implemented along with one or more of the above methods, then the ISUP screening indicator shall be set as described in Clause 4.2.

When multiple methods are implemented by a TSP or a TDM-to-SIP interworking entity, the following precedence rules determine which method to use.

- If the UUI PASSporT method is implemented then check, per the procedures in Clause 4.11, if a UUI encoded PASSporT is present, validated, and contains a supported ppt/alg value.
  - If the check passes then procedures in Clause 4.11 shall be followed and subsequent steps are skipped.
- If the Out-of-Band Transport of PASSporTs method is implemented then check, per the procedures in [Ref 12], if Out-of-Band PASSporTs can be retrieved and validated.
  - If the check passes then procedures in [Ref 12] shall be followed and subsequent steps are skipped.
- If the ISUP Screening Indicator method is implemented, then the ISUP Screening Indicator procedures in Clause 4.2 shall be followed and subsequent steps are skipped.
- If the Trunk Group method is implemented, then the Trunk Group procedures in Clause 4.2 shall be followed.

NOTE: A consequence of these precedence rules is that, in the event of any conflict between methods (e.g., UUI PASSporT indicates "A" level Attestation and Screening Indicator indicates "C" level Attestation), only the method with the highest precedence would apply.

An example of when supporting multiple methods may be useful is if all SPs connected via a local tandem have entered into a multilateral agreement where support of some methods are mandatory and some are optional – e.g., support of the ISUP Screening Indicator method could be mandatory and support of ISUP UUI and Out-of-Band PASSporTs methods could be optional. This would allow SPs with different implementations to interoperate as long as the mandatory method is supported by all SPs; i.e., a TSP would always be able to use the ISUP Screening Indicator in the case that for a given call neither of the other two methods was used.