ATIS-1000105

ATIS Standard on -

Signature-based Handling of Asserted information using Tokens (SHAKEN):

Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using 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.

Published by

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

ATIS-1000105

ATIS Standard on

Signature-based Handling of Asserted information Using Tokens (SHAKEN): Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM

Alliance for Telecommunications Industry Solutions

Approved December 2, 2024

Abstract

The Signature-based Handling of Asserted information using toKENs (SHAKEN) framework enables an authorized Voice over Internet Protocol (VoIP) service provider to deliver a cryptographically protected assertion that the calling user is authorized to use the calling telephone number to a called user via Session Initiation Protocol (SIP) signaling that the calling user is authorized to use the calling telephone number. This specification extends the SHAKEN framework, governance model, and certificate management to enable service providers using Time Division Multiplexing (TDM) signaling to participate in the SHAKEN ecosystem without placing any new requirements on authorized SHAKEN service providers. This specification describes a mechanism where PASSporTs are exchanged between each pair of service providers that interconnect using TDM.

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.

> 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.

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

ATIS Standard on –

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

Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM

1 Scope, Purpose, & Application

1.1 Scope

This specification extends the SHAKEN framework, governance model, and certificate management to enable the transmission of Personal ASSertion Tokens (PASSporTs), as defined in RFC 8225, *Personal Assertion Token* [Ref 14], for calls that use TDM signaling and/or TDM switches during transit.

Within the specification, cryptographically signed PASSporT(s) are exchanged out-of-band, that is, separate from the telephone network signaling. The mechanism of exchanging PASSporT(s) out-of-band is based on RFC 8816, *Secure Telephone Identity Revisited (STIR) Out-of-Band Architecture and Use Cases* [Ref 102].

It is recommended that ATIS-1000097, *Technical Report on Alternatives for Caller Authentication for Non-IP Traffic* [Ref 101], evaluating the viability of implementing this call authentication mechanism for TDM networks, be considered along with this document.

1.2 Purpose & Application

The SHAKEN framework provides a set of tools that enable verification of the calling party's legitimate right to use a calling telephone number for a call. The SHAKEN protocol specification ATIS-1000074, *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)* [Ref 4], describes an authentication mechanism that can be invoked by the Originating Service Provider (OSP) to authenticate itself at a transit switch as the service provider responsible for the call origination and to "attest" to the legitimacy of the calling telephone number associated with a call. A cryptographic signature across the call parameters protects the integrity of the SIP parameters and the OSP's call markings. In the SHAKEN framework, the OSP's Secure Telephone Identity Authentication Service (STI-AS) creates a PASSporT and inserts this PASSporT in a SIP Identity header per RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol* [Ref 13]. The SIP INVITE is then routed over the network-to-network interface (NNI) through the standard inter-domain routing configuration.

TDM switching elements, in today's public switched telephone networks, do not support the Identity header necessary to interwork with SIP. Thus, the Identity header may fail to arrive at the Terminating Service Provider (TSP) network's transit switch for verification by their Secure Telephone Identity Verification Service (STI-VS) because the call may not be transmitted using SIP signaling end to end. The following specification may remedy this problem by enabling service providers to exchange PASSporT(s) through a Secure Telephone Identity Call Placement Service (STI-CPS). However, this is predicated on certain TDM interworking functions as identified later in this document. SHAKEN authentication, verification, and Public Key Infrastructure (PKI) operation remain the same.

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-0300251, *Codes for Identification of Service Providers for Information Exchange.*[1]

[Ref 2] ATIS-0417001-003, *Industry Guidelines for Toll Free Number Administration.*[1]

[Ref 3] ATIS-1000113.2015, *Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part.*[1]

[Ref 4] ATIS-1000074, *ATIS Standard on Signature-based Handling of Asserted Information using Tokens (SHAKEN).*[1]

[Ref 5] ATIS-1000080, *SHAKEN: Governance Model and Certificate Management.*[1]

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

[Ref 7] IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax.* [2]

[Ref 8] IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace.* [2]

[Ref 9] IETF RFC 4949, *Internet Security Glossary, Version 2.* [2]

[Ref 10] IETF RFC 6585, *Additional HTTP Status Codes.* [2]

[Ref 11] IETF RFC 7515, *JSON Web Signature (JWS)*. [2]

[Ref 12] IETF RFC 7519, *JSON Web Token*. [2]

[Ref 13] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.* [2]

[Ref 14] IETF RFC 8225, *Personal Assertion Token.*[2]

[Ref 15] IETF RFC 8785, *JSON Canonicalization Scheme (JCS).* [2]

[Ref 16] ITU Q.850 10/2018, *Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN user part.*[3]

2.2 Informative References

[Ref 101] ATIS-1000097, *Technical Report on Alternatives for Caller Authentication for Non-IP Traffic.* [1]

[Ref 102] IETF RFC 8816, *Secure Telephone Identity Revisited (STIR) Out-of-Band Architecture and Use Cases*. [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.

Caller ID: The originating or calling party telephone number used to identify the caller carried either in the P-Asserted Identity or From header in the SIP (RFC 3261, *SIP: Session Initiation Protocol* [Ref 6]) message.

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

[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/ >.

(Digital) Certificate: Binds a public key to a Subject (e.g., the end-entity). A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object (RFC 4949, *Internet Security Glossary, Version 2* [Ref 9]). See also STI Certificate.

Certification Authority (CA): An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate [Ref 9].

Certificate Chain: See Certification Path.

Certification Path: A linked sequence of one or more public-key certificates, or one or more public-key certificates and one attribute certificate, that enables a certificate user to verify the signature on the last certificate in the path, and thus enables the user to obtain (from that last certificate) a certified public key, or certified attributes, of the system entity that is the subject of that last certificate. Synonym for Certificate Chain [Ref 9].

Certificate Revocation List (CRL): A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire [Ref 9].

Company Code: A unique four-character alphanumeric code (NXXX) assigned to all Service Providers (ATIS-0300251, *Codes for Identification of Service Providers for Information Exchange* [Ref 1]).

Identity: Unless otherwise qualified (see, for example, Telephone Identity below), an identifier that unambiguously distinguishes an entity for authentication and other security and policy application purposes. In this standard, a Service Provider Code is an example of the identity of one kind of participant in certificate management and SHAKEN signing and verification.

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 [Ref 9].

Public Key: The public component of a pair of cryptographic keys used for asymmetric cryptography [Ref 9].

Public Key Infrastructure (PKI): The set of hardware, software, personnel, policy, and procedures used by a CA to issue and manage certificates [Ref 9].

Root CA: A CA that is directly trusted by an end-entity.

Secure Telephone Identity Call Placement Service (STI-CPS): A service, consisting of one or more components, that can receive a PASSporT from a service provider, for retrieval by another service provider.

Secure Telephone Identity (STI) Certificate: A public key certificate needed by a service provider to sign or verify a PASSporT (ATIS-1000080, *SHAKEN: Governance Model and Certificate Management* [Ref 5]).

Secure Telephone Identity InterWorking Function (STI-IWF): A logical function that can convert TDM signaling to SIP signaling and invoke the STI-OOBS, STI-AS, and STI-VS.

Secure Telephone Identity Out-of-Band Service (STI-OOBS): A service that can publish PASSporT(s) to an STI-CPS and retrieve PASSporT(s) from an STI-CPS.

Service Provider Code: In the context of this document, this term refers to any unique identifier that is allocated by a Regulatory and/or administrative entity to a service provider. In the U.S. and Canada, this would be a Company Code as defined in ATIS-0300251 [Ref 1], or a Responsible Organization ID assigned to a RespOrg as defined in ATIS-0417001-003, *Industry Guidelines for Toll Free Number Administration* [Ref 2].

Signature: Created by signing the message using the private key. It verifies the identity of the sender and the integrity of the data [Ref 9].

TDM Switch: A voice circuit switch or other element with a non-IP control plane.

Telephone Identity: An identifier associated with an originator of a telephone call. In the context of the SHAKEN framework, this is a SIP URI or a TEL URI from which a telephone number can be derived.

3.2 Acronyms & Abbreviations

API	Application Programming Interface
ATIS	Alliance for Telecommunications Industry Solutions

CPS	Call Placement Service
CRL	Certificate Revocation List
CSCF	Call Session Control Function
CVT	Call Validation Treatment
FQDN	Fully Qualified Domain Name
GW	GateWay
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAM	Initial Address Message
IBCF	Interconnection Border Control Function
IETF	Internet Engineering Task Force
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
JWS	JSON Web Signature
JWT	JSON Web Token
MGCF	Media Gateway Control Function
NNI	Network-to-Network Interface
OSP	Originating Service Provider
PASSporT	Personal ASSertion Token
PKI	Public Key Infrastructure
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SKS	Secure Key Store
SP	Service Provider
SPC	Service Provider Code
SS7	Signalling System No. 7
STI	Secure Telephone Identity
STI-AS	Secure Telephone Identity Authentication Service
STI-CA	Secure Telephone Identity Certification Authority
STI-CPS	Secure Telephone Identity Call Placement Service
STI-CR	Secure Telephone Identity Certificate Repository

STI-IWF	Secure Telephone Identity InterWorking Function
STI-OOBS	Secure Telephone Identity Out-of-Band Service
STI-PA	Secure Telephone Identity Policy Administrator
STI-VS	Secure Telephone Identity Verification Service
STIR	Secure Telephone Identity Revisited
TDM	Time Division Multiplexing
TN	Telephone Number
TrGW	Transition GateWay
TSP	Terminating Service Provider
UA	User Agent
URI	Uniform Resource Identifier
UUID	Universally Unique IDentifier
VoIP	Voice over Internet Protocol

4 Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM

This standard is a SHAKEN-specific implementation of RFC 8816 [Ref 102]. Readers are expected to be familiar with RFC 8816 [Ref 102].

A Secure Telephone Identity Call Placement Service (STI-CPS) is a SHAKEN-specific Call Placement Service (CPS) that service providers can use to exchange PASSporTs. An STI-CPS leverages the SHAKEN trust model for STI-CPS access control. An STI-CPS has a standardized interface for service provider's Secure Telephone Identity Out-of-Band Service (STI-OOBS) to publish and retrieve PASSporT(s).

To limit access to only Secure Telephone Identity Policy Administrator (STI-PA) approved service providers, a request to publish/retrieve PASSporT(s) to/from an STI-CPS shall include a JSON Web Token (JWT), as defined in RFC 7519, *JSON Web Token* [Ref 12], that is both fresh and signed by a valid, unrevoked STI certificate. To validate JWTs, the STI-CPS shall interface with the STI-PA(s) to retrieve the trusted Secure Telephone Identity Certification Authority (STI-CA) list and Certificate Revocation List (CRL).

Each pair of service providers that interconnect using TDM shall agree to use a particular STI-CPS for each call that traverses that TDM NNI. A service provider that has internal TDM NNIs[4] within its network shall determine a particular STI-CPS to use for calls that traverse its own TDM NNIs. For each TDM NNI that a call traverses, the PASSporT(s) associated with the call are published to and retrieved from an STI-CPS. The PASSporT(s) related to a given call may be published to and retrieved from an STI-CPS multiple times, once for each TDM NNI that the call traverses. The same or a different STI-CPS may be used at each TDM NNI. While the choice of STI-CPS is left open to bilateral agreement, allowing the service provider who is performing the publish to dictate the STI-CPS used for the call simplifies the publishing service provider's implementation because the PASSporTs do not need to be published again for each call attempt in the event of a route advance.

A service provider network that converts a call from SIP signaling to TDM signaling shall invoke an STI-OOBS to publish all associated PASSporT(s) received in the SIP signaling, as defined in RFC 3261 [Ref 6] (e.g., SIP INVITE) to the agreed STI-CPS and wait for confirmation of the publish before the call is sent downstream. If no PASSporT(s) are received, the service provider's STI-AS shall generate the applicable PASSporT(s) and then the STI-OOBS shall publish the generated PASSporT(s) to the agreed STI-CPS and wait for confirmation of the publish before the call is sent downstream. An OSP network that sends a call via a TDM NNI shall invoke an STI-AS to generate the applicable PASSporT(s) and then shall invoke an STI-OOBS to publish the generated PASSporT(s) to the agreed STI-CPS and wait for confirmation of the publish before the call is sent downstream.

A service provider network that converts a call from TDM signaling to SIP signaling shall invoke an STI-OOBS to retrieve all PASSporT(s) associated with the call from the agreed STI-CPS and then shall insert the retrieved PASSporT(s) into the SIP signaling in Identity header(s) as described in RFC 8224 [Ref 13]. A TSP network that receives a call via a TDM NNI shall invoke an STI-OOBS to retrieve all PASSporT(s) associated with the call from the agreed STI-CPS and then shall insert the retrieved PASSporT(s) into the SIP signaling in Identity header(s) for delivery to the TSP's STI-VS function.

A service provider network that receives a call via a TDM NNI and then sends that call via a TDM NNI shall invoke an STI-OOBS to retrieve all PASSporT(s) associated with the call from the agreed STI-CPS and then shall invoke an STI-OOBS to publish all associated PASSporT(s) to the agreed STI-CPS and wait for confirmation of the publish before the call is sent downstream.

The STI-OOBS should have reasonable timeouts for publish and retrieve requests to prevent excessive call setup latency. The timeouts and actions to take if a timeout occurs are left to local policy. Note that total call setup latency is impacted both by the time consumed by publishing and retrieving PASSporT(s) and the number of times such transactions are required.

SHAKEN-related error responses (e.g., 437 – 'Unsupported credential') may not be conveyed accurately due to limitations on mapping between SIP responses and Signalling System No. 7 (SS7) Q.850 cause codes, as defined in ITU Q.850 10/2018, *Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN user part* [Ref 16].

[4] This document uses the term Network-to-Network Interface (NNI) to refer to both intra-service provider and inter-service provider network interfaces.

5 STI-OOBS

The Secure Telephone Identity Out-of-Band Service (STI-OOBS) publishes PASSporT(s) to an STI-CPS and retrieves PASSporT(s) from an STI-CPS. In a reference architecture illustrated in Clause 8, the STI-OOBS has a SIP signaling interface to receive requests containing the call parameters received on a SIP or TDM NNI and provide responses. If the SIP signaling request includes one or more PASSporTs, then the STI-OOBS constructs a JWT for authentication and publishes the PASSporT(s) to an STI-CPS. Alternatively, if the SIP signaling request does not include any PASSporTs, then the STI-OOBS constructs a JWT for authentication, retrieves all available PASSporT(s) from an STI-CPS, and includes the retrieved PASSporT(s) in Identity header(s) in the SIP signaling response.

The STI-OOBS is a logical function that may be combined with other logical functions (e.g., STI-AS or STI-VS).

The STI-OOBS is typically invoked by an Interconnection Border Control Function (IBCF)/Transition GateWay (TrGW), Media Gateway Control Function (MGCF), Call Session Control Function (CSCF), or Secure Telephone Identity InterWorking Function (STI-IWF). However, this document places no implementation limitations or restrictions on the STI-OOBS and defines it only to be capable of supporting the end-to-end call flows illustrated in Clause 8.

6 STI-IWF

The Secure Telephone Identity InterWorking Function (STI-IWF) provides a mechanism for a TDM switch that is not otherwise capable of interacting with SHAKEN functional elements to use them in the call flow. The STI-IWF accepts SS7 signaling messages (e.g., ISUP or TCAP) [ATIS-1000113.2015, *Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part*], invokes the STI-AS, STI-VS, and/or STI-OOBS functions, and responds with an appropriate SS7 signaling message. The specific implementation of SS7 signaling and call handling depends on local network configuration and switch capabilities and assumes the development and use of an interworking capability that establishes the SHAKEN attestation level of a TDM-originated call and provides standard mapping to the SIP Identity header via interactions with an STI-AS.

In a reference architecture illustrated in Clause 8, when deployed by an OSP, the STI-IWF requests a PASSporT from the STI-AS utilizing the STI-AS's SIP signaling interface and then publishes the PASSporT(s) to an STI-CPS utilizing the SIP signaling interface of the STI-OOBS. When deployed by a TSP, the STI-IWF requests all available PASSporT(s) from an STI-CPS utilizing the STI-OOBS's SIP signaling interface and then sends the PASSporT(s) to the STI-VS to be verified utilizing the SIP signaling interface of the STI-VS. When deployed by an intermediate provider, the STI-IWF utilizes the SIP signaling interface of the STI-OOBS to retrieve the PASSporT(s) from an STI-CPS and publish the PASSporT(s) to an STI-CPS.

The STI-IWF is a logical function that may be combined with other logical functions (e.g., TDM switch or STI-OOBS).

This document places no implementation limitations or restrictions on the STI-IWF and defines it only to be capable of supporting the end-to-end call flows illustrated in Clause 8.

7 STI-CPS

Each STI-CPS shall implement the following three API endpoints:

1. Health check
2. Publish PASSporT(s)
3. Retrieve PASSporT(s)

All API endpoints shall support Hypertext Transfer Protocol Secure (HTTPS) and not accept requests using insecure Hypertext Transfer Protocol (HTTP) or redirect requests received on HTTP endpoints to HTTPS endpoints.

7.1 Health Check

The health check API endpoint of each STI-CPS shall be accessible via an HTTP GET request to the path "/health". An HTTP 200 status code shall be returned if the STI-CPS is able to both process requests to publish PASSporT(s) and process requests to retrieve PASSporT(s). An HTTP status code greater than 399 shall be returned if the STI-CPS is not able to process requests to publish PASSporT(s) or is not able to process requests to retrieve PASSporT(s). The health check API endpoint shall return standard HTTP error response codes as defined in RFC 6585, *Additional HTTP Status Codes* [Ref 10].

7.1.1 HTTP Request

The following message is an example of an HTTP GET made to an STI-CPS to check its health:

```
GET /health HTTP/1.1
Content-Length: 0
Host: cps.example.com
```

7.1.2 Successful HTTP Response

The following message is an example of an HTTP response from an STI-CPS to indicate that it is healthy:

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 29

{"status":200,"message":"OK"}
```

7.1.3 Error HTTP Response

The following message is an example of an HTTP response from an STI-CPS to indicate that it is not healthy:

```
HTTP/1.1 502 Bad Gateway
Content-Type: application/json
Content-Length: 38

{"status":502,"message":"Bad Gateway"}
```

7.2 Publish PASSporT(s)

The publish PASSporT(s) API endpoint of each STI-CPS shall be accessible via an HTTP POST request to the path "/passports/SPC/DEST/ORIG". The "SPC" parameter shall be replaced with the registered SPC of the service provider performing the publish request. The "DEST" parameter shall contain the same value as in the ISDN User Part (ISUP) Initial Address Message (IAM) Called Party Number parameter [Ref 3]. If the Called Party Number parameter contains the location routing number, then the parameter containing the dialed digits shall be used instead. The "ORIG" parameter shall contain the same value as in the ISUP IAM Calling Party Number [Ref 3]. Parameters shall be encoded per RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax* [Ref 7]. Telephone numbers shall be canonicalized per RFC 8224 [Ref 13].

> NOTE: In some scenarios the ISUP IAM may not be created until after the publish occurs. In these scenarios, the "DEST" parameter and "ORIG" parameter shall contain the same value as in the ISUP IAM that will be created.

The request shall have a "Content-Type" header set to "application/json". The body of the request shall be a JSON object. The JSON object shall include the key "passports". The value of the key "passports" shall be an array of strings where each string is a PASSporT. All PASSporT(s) received in the SIP signaling shall be included in the array of "passports".

The request shall include a bearer token in the "Authorization" header. The bearer token shall be a JWT that is both fresh (i.e., the "iat" claim contains a value within the STI-CPS's local policy for freshness) and signed by a valid,

unrevoked STI certificate that chains up to an approved STI-CA root certificate. The JWT header shall include an “alg” claim with the value “ES256”. The JWT header shall include an “x5u” claim indicating the Uniform Resource Identifier (URI) of the STI certificate that was used to sign the JWT. The JWT payload shall include an “iat” claim indicating the timestamp of when the JWT was signed. The JWT payload shall include an “exp” claim indicating the timestamp at which the call setup is guaranteed to be either completed or canceled based on the service provider’s routing and network protection timers (e.g., T7 timer [Ref 3]). The timestamp should be the earliest value possible that meets this requirement to reduce the likelihood of PASSporTs conflicting. The JWT payload shall include an “aud” claim with the Fully Qualified Domain Name (FQDN) of the STI-CPS as the value. The JWT payload shall include an “spc” claim with the registered SPC of the service provider performing the publish request. The “spc” claim shall match the “SPC” parameter. The JWT payload shall include an “iss” claim with the registered SPC of the service provider that signed the JWT as the value. The “iss” claim shall match the SPC in the TNAuthList extension of the certificate that was used to sign the JWT, the “spc” claim, and the “SPC” parameter. The JWT payload shall include an "action" claim with the literal string "publish" as the value. The JWT payload shall include a "passports" claim where the value is the literal string "sha256-" concatenated with the base64 encoded SHA-256 digest of the canonicalized value of the “passports” key in the JSON object of the request body. The canonicalization procedures are described in RFC 8785, *JSON Canonicalization Scheme (JCS)* [Ref 15]. The JWT payload shall include a "jti" claim with a unique version 4 Universally Unique IDentifier (UUID), as defined in RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace* [Ref 8], as the value. The JWT payload shall include an “orig” claim with a “tn” value that is the same as the “ORIG” parameter. The JWT payload shall include a “dest” claim with a “tn” value that is the same as the “DEST” parameter. The JWT may contain additional claims in the header and/or payload. If a request does not include an authentication JWT that meets all these requirements, then the request shall not be accepted by the STI-CPS. The header and payload of an example authentication JWT for a “publish” request are below:

Header:


```
{
  "alg": "ES256",
  "x5u": "https://certificates.example.com/example.pem"
}
```


Payload:


```
{
  "iat": 1608048420,
  "exp": 1608048425,
  "action": "publish",
  "passports": "sha256-YO4Hq/xE6mkCeuPoYYck5Pt6vACmfbzNfdi6aeq95dA=",
  "spc": "1234",
  "iss": "1234",
  "aud": "cps.example.com",
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059",
  "dest": {
    "tn": [
      "19032469103"
    ]
  },
```

```
  "orig": {
    "tn": "12013776051"
  }
}
```

An HTTP 201 status code shall be returned if the PASSporT(s) were published. An HTTP status code greater than 399 shall be returned if the PASSporT(s) were not published. The publish API endpoint shall return standard HTTP error response codes as defined in RFC 6585 [Ref 10].

The STI-CPS shall retain the PASSporT(s) and authentication JWT in every valid publish request until the time indicated in the “exp” claim of the authentication JWT in the given publish request. This includes cases when multiple valid publish requests are received with the same “SPC”, “DEST”, and “ORIG” parameters.

7.2.1 HTTP Request

The following message is an example of an HTTP POST made to an STI-CPS by a service provider to publish PASSporT(s) for a call:

```
POST /passports/1234/19032469103/12013776051 HTTP/1.1
Content-Type: application/json
Content-Length: 423
Host: cps.example.com
Authorization: Bearer
eyJhbGciOiJFUzI1NiIsIng1dSI6Imh0dHBzOi8vY2VydGlmaWNhdGVzLmV4YW1wbGUuY29tL2V4YW1wbGUucGVtIn0
.eyJpYXQiOjE2MDgwNDg0MjAsImV4cCI6MTYwODA0ODQyMDUsImFjdGlvbiI6InB1Ymxpc2giLCJwYXNzcG9ydHMiOi
JzaGEyNTYtWU80SHEveEU2bWtDZXVQb1lZY2s1UHQ2dkFDbWZiek5mZGk2YWVxOTVkQT0iLCJpc3MiOiIxMjM0IiwiY
XVkIjoiY3BzLmV4YW1wbGUuY29tIiwianRpIjoiZWJjYmQ3ZjItYjc4Yi00MDE5LWJmODMtMzJjMjUxN2U2MDU5Iiwi
ZGVzdCI6eyJ0biI6WyIxOTAzMjQ2OTEwMyJdfSwib3JpZyI6eyJ0biI6IjEyMDEzNzc2MDUxIn19.1_Nty37vqW0aEH
n7y5k9Da9vXO_FvWSMGY6xOh6U_7RbGOSm0H9BK_xTqXRhtXCM6IcBm6rIsTW5BDEg6SwbBQ

{"passports":["eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0
cHM6Ly9jZXJ0aWZpY2F0ZXMuZXhhbXBsZS5jb20vZXhhbXBsZS5wZW0ifQ.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0
biI6WyIxOTAzMjQ2OTEwMyJdfSwiaWF0IjoxNTg0OTgzNDAyLCJvcmlnIjp7InRuIjoiMTIwMTM3NzYwNTEifSwib3J
pZ2lkIjoiNGFlYzk0ZTItNTA4Yy00YzFjLTkwN2ItMzczN2JhYzBhODBlIn0.EMfXHyowsI5s73KqoBzJ9pzrrwGFNK
BRmHcx-YZ3DjPgBe4Mvqq9N-bThN1_HTWeSvbruAyet26fetRL1_bn1g"]}
```

7.2.2 Successful HTTP Response

The following message is an example of an HTTP response from an STI-CPS to indicate that the PASSporT(s) were published:

```
HTTP/1.1 201 Created
Content-Type: application/json
Content-Length: 34

{"status":201,"message":"Created"}
```

7.2.3 Error HTTP Response

The following message is an example of an HTTP response from an STI-CPS to indicate that the PASSporT(s) were not published:

```
HTTP/1.1 400 Bad Request
Content-Type: application/json
Content-Length: 38
```

{"status":400,"message":"Bad Request"}

7.3 Retrieve PASSporT(s)

The retrieve PASSporT(s) API endpoint of each STI-CPS shall be accessible via an HTTP GET request to the path "/passports/SPC/DEST/ORIG". The "SPC" parameter shall be replaced with the registered SPC of the service provider that the call was received from. The "DEST" parameter shall contain the same value as in the ISUP IAM Called Party Number parameter [Ref 3]. If the Called Party Number parameter contains the location routing number, then the parameter containing the dialed digits shall be used instead. The "ORIG" parameter shall contain the same value as in the ISUP IAM Calling Party Number [Ref 3]. Parameters shall be encoded per RFC 3986 [Ref 7]. Telephone numbers shall be canonicalized per RFC 8224 [Ref 13].

The request shall include a bearer token in the "Authorization" header. The bearer token shall be a JWT that is both fresh (i.e., the "iat" claim contains a value within the STI-CPS's local policy for freshness) and signed by a valid, unrevoked STI certificate that chains up to an approved STI-CA root certificate. The JWT header shall include an "alg" claim with the value "ES256". The JWT header shall include an "x5u" claim indicating the URI of the STI certificate that was used to sign the JWT. The JWT payload shall include an "iat" claim indicating the timestamp of when the JWT was signed. The JWT payload shall include an "aud" claim with the FQDN of the STI-CPS as the value. The JWT payload shall include an "spc" claim with the registered SPC of the service provider that the call was received from. The "spc" claim shall match the "SPC" parameter. The JWT payload shall include an "iss" claim with the registered SPC of the service provider that signed the JWT as the value. The "iss" claim shall match the SPC in the TNAuthList extension of the certificate that was used to sign the JWT. The JWT payload shall include an "action" claim with the literal string "retrieve" as the value. The JWT payload shall include a "jti" claim with a unique version 4 UUID as the value. The JWT payload shall include an "orig" claim with a "tn" value that is the same as the "ORIG" parameter. The JWT payload shall include a "dest" claim with a "tn" value that is the same as the "DEST" parameter. The JWT may contain additional claims in the header and/or payload. If a request does not include an authentication JWT that meets all these requirements, then the request shall not be accepted by the STI-CPS. The header and payload of an example authentication JWT are below:

Header:

{
  "alg": "ES256",
  "x5u": "https://certificates.example.com/example.pem"
}

Payload:

{
  "iat": 1608048420,
  "action": "retrieve",
  "spc": "1234",
  "iss": "4321",
  "aud": "cps.example.com",
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059",
  "dest": {
    "tn": [
      "19032469103"
    ]

```
  },
  "orig": {
    "tn": "12013776051"
  }
}
```


If there are multiple unexpired publish requests with the same “SPC”, “ORIG”, and “DEST” parameters, then if every unexpired publish request is similar, the PASSporT(s) from the most recent publish request shall be returned; otherwise, no PASSporT(s) shall be returned. Publish requests shall be considered similar if they meet all of the following conditions:

1. They contain the same number of PASSporTs.
2. Each PASSporT has identical header claims and payload claims, excluding “iat”, as a PASSporT from the other publish request.
3. Each PASSporT has the same signature validation (as described in Section 5.2 of RFC 7515, *JSON Web Signature (JWS)* [Ref 11]) result (either pass or fail) as the corresponding PASSporT (i.e., the PASSporT with the same claims excluding “iat”) from the other publish request.

If a given service provider with downstream TDM NNIs receives or originates multiple calls in a short period of time with the same calling and called numbers that contain non-similar PASSporTs, the PASSporT(s) for the calls may be lost because if the STI-CPS is not able to determine which authentication information is associated with each individual call, the STI-CPS returns no PASSporTs.

When an STI-CPS receives a retrieve request, the STI-CPS shall either return all the PASSporTs it received in the publish request or, in the case of multiple unexpired publish requests with non-similar PASSporTs, none of the PASSporTs it received in the publish request (due to not being able to associate the PASSporTs with the corresponding call). If one or more PASSporTs are returned, then the response shall have a “Content-Type” header set to “application/json”. The body of the response shall be a JSON object. The JSON object shall include the keys “token” and “passports”. The value of the key “token” shall be a string with the authentication JWT previously used by the service provider when the PASSporT(s) were published. The value of the key “passports” shall be an array of strings where each string is a PASSporT. All PASSporT(s) received in the publish request shall be included in the array of “passports” returned in the response to the retrieve request.

An HTTP 200 status code shall be returned if one or more PASSporTs are returned. An HTTP status code greater than 399 shall be returned if no PASSporT(s) are returned. The retrieve API endpoint shall return standard HTTP error response codes as defined in RFC 6585 [Ref 10].

The authentication JWT may be used by the service provider retrieving the PASSporT(s) to verify that the publish request was performed by the expected service provider.

7.3.1 HTTP Request

The following message is an example of an HTTP GET made to an STI-CPS to retrieve PASSporT(s) for a call:


```
GET /passports/1234/19032469103/12013776051 HTTP/1.1
Content-Length: 0
Host: cps.example.com
Authorization: Bearer
eyJhbGciOiJFUzI1NiIsIng1dSI6Imh0dHBzOi8vY2VydGlmaWNhdGVzLmV4YW1wbGUuY29tL2V4YW1wbGUucGVtIn0
.eyJpYXQiOjE2MDgwNDg0NDQsImFjdGlvbiI6InJldHJpZXZlIiwic3BjIjoiMTIzNCIsImlzcyI6IjQzMjEiLCJhdW
QiOiJjcHMuZXhhbXBsZS5jb20iLCJqdGkiOiJiODBlMTAyMy04ZGM0LTQ2NWQtYTFhYS1mMDhlODhmODkyNjUiLCJkZ
XN0Ijp7InRuIjpbIjE5MDMyNDY5MTAzIl19LCJvcmlnIjp7InRuIjoiMTIwMTM3NzYwNTEifX0.k3S9oNyj9B8olbga
ObL-eqdnCAB_sZaBOSuzfo8R7PDyqEBUOVvm-pFzG24giW8ztlg6339TerVQRGUQNhx9HQ
```

7.3.2 Successful HTTP Response

The following message is an example of an HTTP response from an STI-CPS to provide the requested PASSporT(s):

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 937

{"token":"eyJhbGciOiJFUzI1NiIsIng1dSI6Imh0dHBzOi8vY2VydGlmaWNhdGVzLmV4YW1wbGUuY29tL2V4YW1wb
GUucGVtIn0.eyJpYXQiOjE2MDgwNDg0MjAsImFjdGlvbiI6InB1Ymxpc2giLCJwYXNzcG9ydHMiOiJzaGEyNTYtWU80
SHEveEU2bWtDZXVQb1lZY2s1UHQ2dkFDbWZiek5mZGk2YWVxOTVkQT0iLCJpc3MiOiIxMjM0IiwiYXVkIjoiY3BzLmV
4YW1wbGUuY29tIiwianRpIjoiZWJjYmQ3ZjItYjc4Yi00MDE5LWJmODMtMzJjMjUxN2U2MDU5IiwiZGVzdCI6eyJ0bi
I6WyIxOTAzMjQ2OTEwMyJdfSwib3JpZyI6eyJ0biI6IjEyMDEzNzc2MDUxIn19.1_Nty37vqW0aEHn7y5k9Da9vXO_F
vWSMGY6xOh6U_7RbGOSm0H9BK_xTqXRhtXCM6IcBm6rIsTW5BDEg6SwbBQ","passports":["eyJhbGciOiJFUzI1N
iIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ0aWZpY2F0ZXMuZXhhbXBs
ZS5jb20vZXhhbXBsZS5wZW0ifQ.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyIxOTAzMjQ2OTEwMyJdfSwiaWF0
IjoxNTg0OTgzNDAyLCJvcmlnIjp7InRuIjoiMTIwMTM3NzYwNTEifSwib3JpZ2lkIjoiNGFlYzk0ZTItNTA4Yy00YzF
jLTkwN2ItMzczN2JhYzBhODBlIn0.EMfXHyowsI5s73KqoBzJ9pzrrwGFNKBRmHcx-YZ3DjPgBe4Mvqq9N-
bThN1_HTWeSvbruAyet26fetRL1_bn1g"]}
```

7.3.3 Error HTTP Response

The following message is an example of an HTTP response from an STI-CPS to indicate that the requested PASSporT(s) are not available:

```
HTTP/1.1 404 Not Found
Content-Type: application/json
Content-Length: 36

{"status":404,"message":"Not Found"}
```

8 Call Scenario Examples

Multiple call scenario examples are detailed below but most call scenarios are supported by the key requirements in Clause 4. The scenarios include 1) a VoIP OSP with an SIP NNI, 2) a VoIP OSP with a TDM NNI, and 3) a TDM OSP each enumerated with i) a VoIP TSP with an SIP NNI, ii) a VoIP TSP with a TDM NNI, and iii) a TDM TSP. The last two call scenario examples depict a call traversing a network that uses an internal TDM NNI with 1) external SIP NNIs and 2) external TDM NNIs.

> NOTE: These scenarios depict cases where each STI-CPS is able to determine the PASSporT(s) associated with each call per the procedures in Clause 7.3.

8.1 VoIP OSP with SIP NNI – VoIP TSP with SIP NNI

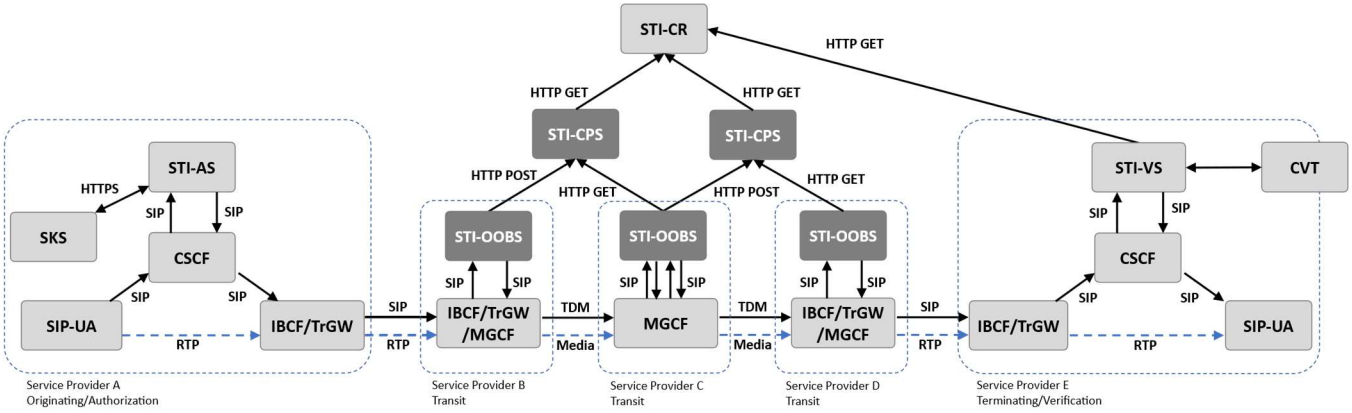

Figure 8-1: VoIP OSP with SIP NNI – VoIP TSP with SIP NNI

Figure 8-1 shows a call that is originated by a VoIP service provider, converted from SIP signaling to TDM signaling by a transit provider, converted back from TDM signaling to SIP signaling by a transit provider, and terminated by a VoIP service provider. The following SHAKEN procedure occurs:

1. Service Provider A performs SHAKEN authentication.
2. Service Provider B publishes the PASSporT(s) received in the SIP signaling to an STI-CPS and converts the call from SIP signaling to TDM signaling.
3. Service Provider C retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
4. Service Provider D converts the call from TDM signaling to SIP signaling, retrieves the PASSporT(s) from an STI-CPS, and inserts the retrieved PASSporT(s) into the SIP signaling.
5. Service Provider E performs SHAKEN verification.

NOTE: If Service Provider C has a TDM switch instead of an MGCF, an STI-IWF is used to interface with the STI-OOBS. The TDM switch invokes the STI-IWF once and the STI-IWF invokes the STI-OOBS twice, first to retrieve the PASSporT(s) from the first STI-CPS and second to publish the PASSporT(s) to the second STI-CPS.

8.2 VoIP OSP with SIP NNI – VoIP TSP with TDM NNI

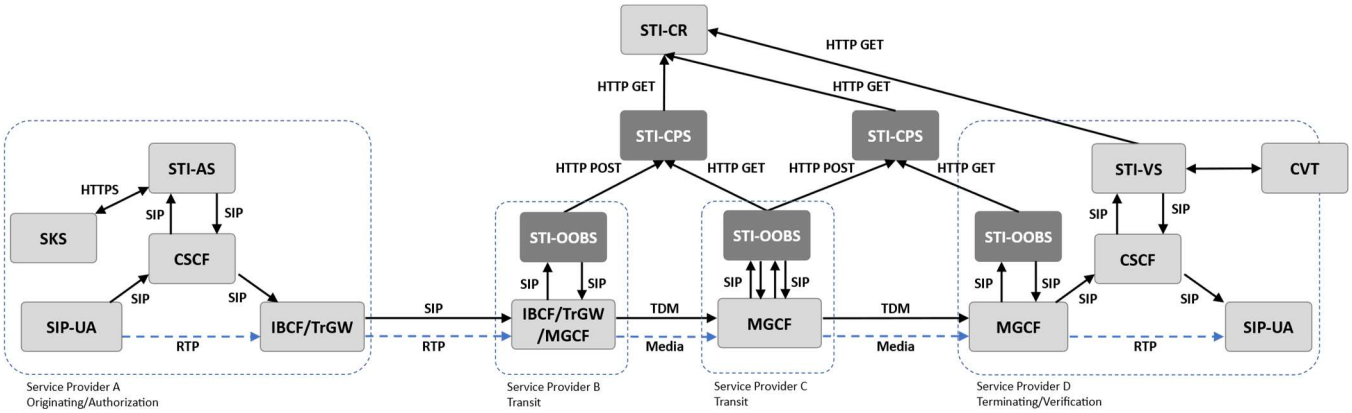

Figure 8-2: VoIP OSP with SIP NNI – VoIP TSP with TDM NNI

Figure 8-2 shows a call that is originated by a VoIP service provider, converted from SIP signaling to TDM signaling by a transit provider, and terminated by a VoIP service provider using TDM signaling. The following SHAKEN procedure occurs:

1. Service Provider A performs SHAKEN authentication.
2. Service Provider B publishes the PASSporT(s) received in the SIP signaling to an STI-CPS and converts the call from SIP signaling to TDM signaling.
3. Service Provider C retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
4. Service Provider D converts the call from TDM signaling to SIP signaling, retrieves the PASSporT(s) from an STI-CPS, and performs SHAKEN verification.

NOTE: If Service Provider C has a TDM switch instead of an MGCF, an STI-IWF is used to interface with the STI-OOBS. The TDM switch invokes the STI-IWF once and the STI-IWF invokes the STI-OOBS twice, first to retrieve the PASSporT(s) from the first STI-CPS and second to publish the PASSporT(s) to the second STI-CPS.

8.3 VoIP OSP with SIP NNI – TDM TSP

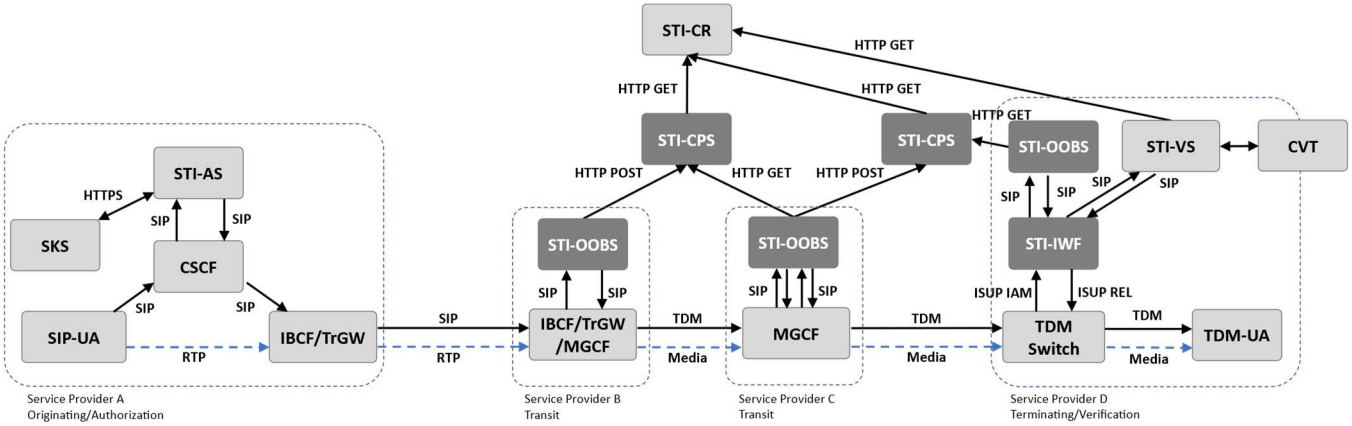

Figure 8-3: VoIP OSP with SIP NNI – TDM TSP

Figure 8-3 shows a call that is originated by a VoIP service provider, converted from SIP signaling to TDM signaling by a transit provider, and terminated by a service provider using a TDM switch. The following SHAKEN procedure occurs:

1. Service Provider A performs SHAKEN authentication.
2. Service Provider B publishes the PASSporT(s) received in the SIP signaling to an STI-CPS and converts the call from SIP signaling to TDM signaling.
3. Service Provider C retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
4. Service Provider D (through an STI-IWF) retrieves the PASSporT(s) from an STI-CPS and performs SHAKEN verification.

NOTE: If Service Provider C has a TDM switch instead of an MGCF, an STI-IWF is used to interface with the STI-OOBS. The TDM switch invokes the STI-IWF once and the STI-IWF invokes the STI-OOBS twice, first to retrieve the PASSporT(s) from the first STI-CPS and second to publish the PASSporT(s) to the second STI-CPS.

8.4 VoIP OSP with TDM NNI – VoIP TSP with SIP NNI

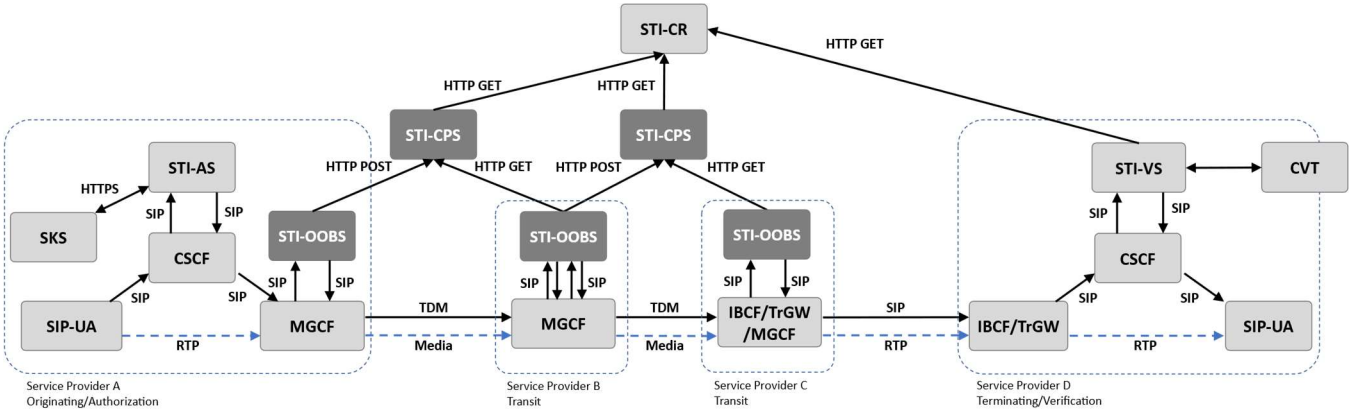

Figure 8-4: VoIP OSP with TDM NNI – VoIP TSP with SIP NNI

Figure 8-4 shows a call that is originated by a VoIP service provider using TDM signaling, converted back from TDM signaling to SIP signaling by a transit provider, and terminated by a VoIP service provider. The following SHAKEN procedure occurs:

1. Service Provider A performs SHAKEN authentication, publishes the PASSporT(s) to an STI-CPS, and converts the call from SIP signaling to TDM signaling.
2. Service Provider B retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
3. Service Provider C converts the call from TDM signaling to SIP signaling, retrieves the PASSporT(s) from an STI-CPS, and inserts the retrieved PASSporT(s) into the SIP signaling.
4. Service Provider D performs SHAKEN verification.

NOTE: If Service Provider B has a TDM switch instead of an MGCF, an STI-IWF is used to interface with the STI-OOBS. The TDM switch invokes the STI-IWF once and the STI-IWF invokes the STI-OOBS twice, first to retrieve the PASSporT(s) from the first STI-CPS and second to publish the PASSporT(s) to the second STI-CPS.

8.5 VoIP OSP with TDM NNI – VoIP TSP with TDM NNI

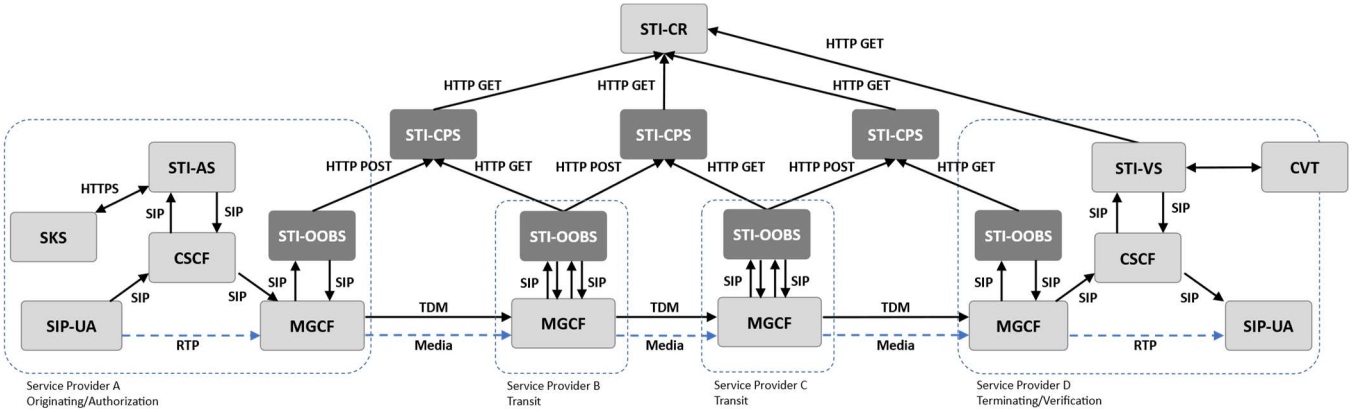

Figure 8-5: VoIP OSP with TDM NNI – VoIP TSP with TDM NNI

Figure 8-5 shows a call that is originated by a VoIP service provider using TDM signaling, transited by service providers using TDM signaling, and terminated by a VoIP service provider using TDM signaling. The following SHAKEN procedure occurs:

1. Service Provider A performs SHAKEN authentication, publishes the PASSporT(s) to an STI-CPS, and converts the call from SIP signaling to TDM signaling.
2. Service Provider B retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
3. Service Provider C retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
4. Service Provider D converts the call from TDM signaling to SIP signaling, retrieves the PASSporT(s) from an STI-CPS, and performs SHAKEN verification.

NOTE: If Service Provider B and/or Service Provider C have a TDM switch instead of an MGCF, an STI-IWF is used to interface with the STI-OOBS. The TDM switch invokes the STI-IWF once and the STI-IWF invokes the STI-OOBS twice, first to retrieve the PASSporT(s) from the first STI-CPS and second to publish the PASSporT(s) to the second STI-CPS.

8.6 VoIP OSP with TDM NNI – TDM TSP

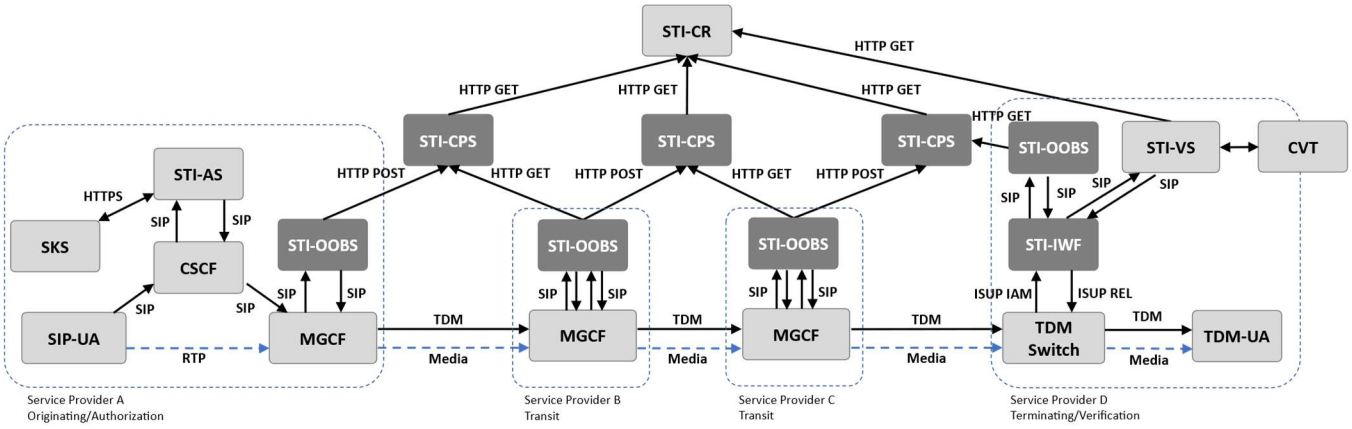

Figure 8-6: VoIP OSP with TDM NNI – TDM TSP

Figure 8-6 shows a call that is originated by a VoIP service provider using TDM signaling, transited by service providers using TDM signaling, and terminated by a service provider using a TDM switch. The following SHAKEN procedure occurs:

1. Service Provider A performs SHAKEN authentication, publishes the PASSporT(s) to an STI-CPS, and converts the call from SIP signaling to TDM signaling.
2. Service Provider B retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
3. Service Provider C retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
4. Service Provider D (through an STI-IWF) retrieves the PASSporT(s) from an STI-CPS and performs SHAKEN verification.

NOTE: If Service Provider B and/or Service Provider C have a TDM switch instead of an MGCF, an STI-IWF is used to interface with the STI-OOBS. The TDM switch invokes the STI-IWF once and the STI-IWF invokes the STI-OOBS twice, first to retrieve the PASSporT(s) from the first STI-CPS and second to publish the PASSporT(s) to the second STI-CPS.

8.7 TDM OSP – VoIP TSP with SIP NNI

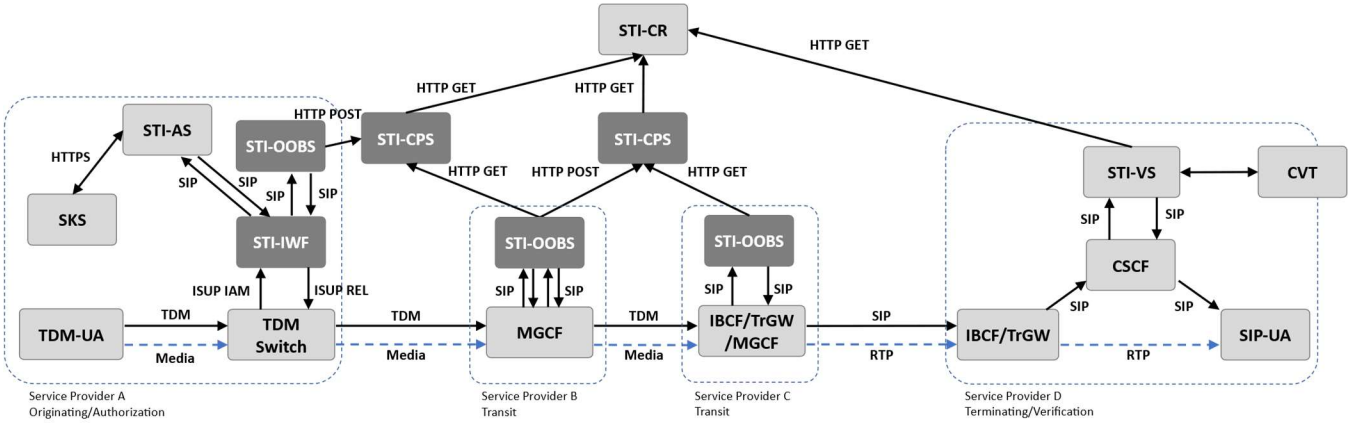

Figure 8-7: TDM OSP – VoIP TSP with SIP NNI

Figure 8-7 shows a call that is originated by a service provider using a TDM switch, converted back from TDM signaling to SIP signaling by a transit provider, and terminated by a VoIP service provider. The following SHAKEN procedure occurs:

1. Service Provider A (through an STI-IWF) performs SHAKEN authentication and publishes the PASSporT(s) to an STI-CPS.
2. Service Provider B retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
3. Service Provider C converts the call from TDM signaling to SIP signaling, retrieves the PASSporT(s) from an STI-CPS, and inserts the retrieved PASSporT(s) into the SIP signaling.
4. Service Provider D performs SHAKEN verification.

NOTE: If Service Provider B has a TDM switch instead of an MGCF, an STI-IWF is used to interface with the STI-OOBS. The TDM switch invokes the STI-IWF once and the STI-IWF invokes the STI-OOBS twice, first to retrieve the PASSporT(s) from the first STI-CPS and second to publish the PASSporT(s) to the second STI-CPS.

8.8 TDM OSP – VoIP TSP with TDM NNI

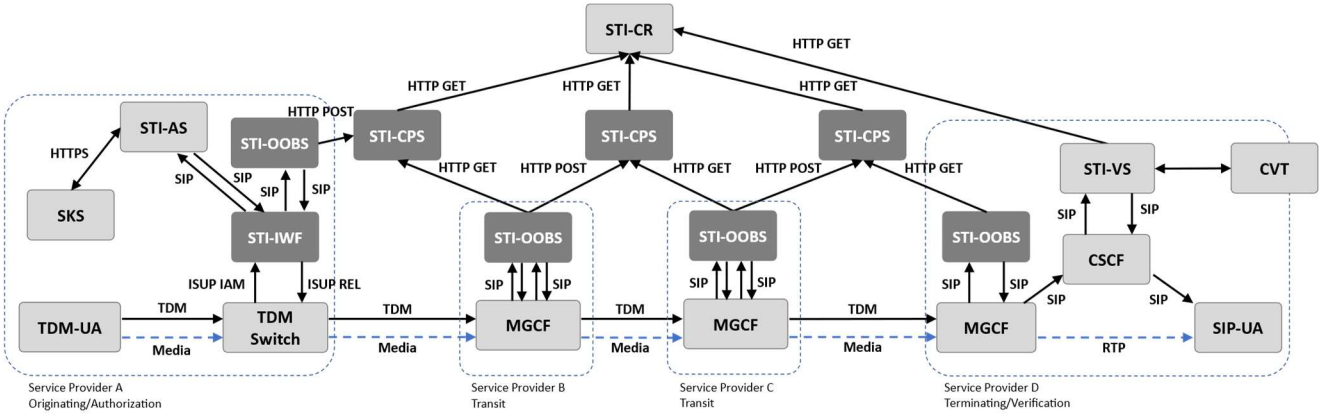

Figure 8-8: TDM OSP – VoIP TSP with TDM NNI

Figure 8-8 shows a call that is originated by a service provider using a TDM switch and terminated by a VoIP service provider using TDM signaling. The following SHAKEN procedure occurs:

1. Service Provider A (through an STI-IWF) performs SHAKEN authentication and publishes the PASSporT(s) to an STI-CPS.
2. Service Provider B retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
3. Service Provider C retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
4. Service Provider D converts the call from TDM signaling to SIP signaling, retrieves the PASSporT(s) from an STI-CPS, and performs SHAKEN verification.

NOTE: If Service Provider B and/or Service Provider C have a TDM switch instead of an MGCF, an STI-IWF is used to interface with the STI-OOBS. The TDM switch invokes the STI-IWF once and the STI-IWF invokes the STI-OOBS twice, first to retrieve the PASSporT(s) from the first STI-CPS and second to publish the PASSporT(s) to the second STI-CPS.

8.9 TDM OSP – TDM TSP

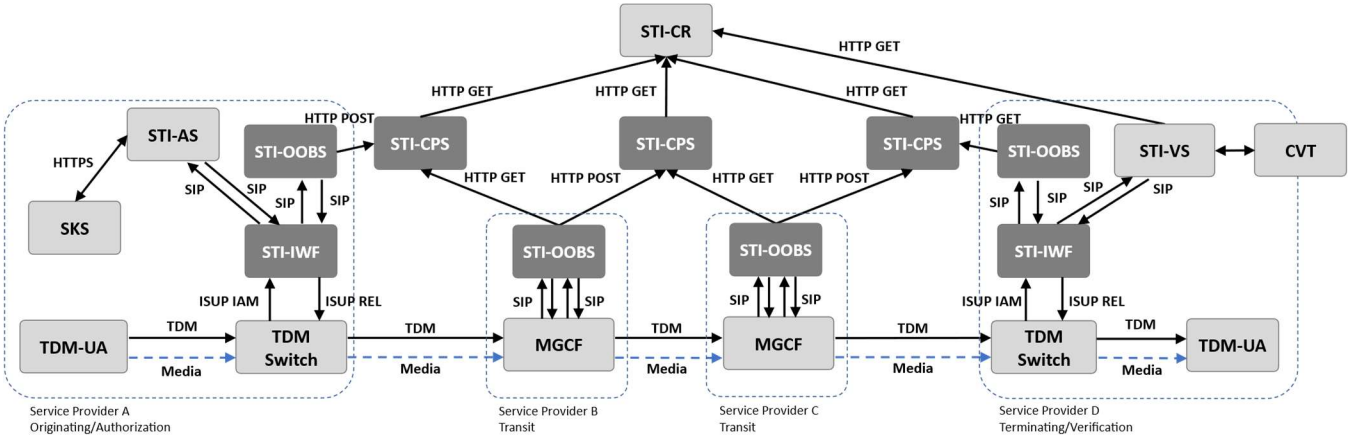

Figure 8-9: TDM OSP – TDM TSP

Figure 8-9 shows a call that is originated by a service provider using a TDM switch, transited by service providers using TDM signaling, and terminated by a service provider using a TDM switch. The following SHAKEN procedure occurs:

1. Service Provider A (through an STI-IWF) performs SHAKEN authentication and publishes the PASSporT(s) to an STI-CPS.
2. Service Provider B retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
3. Service Provider C retrieves the PASSporT(s) from an STI-CPS and publishes the PASSporT(s) to an STI-CPS.
4. Service Provider D (through an STI-IWF) retrieves the PASSporT(s) from an STI-CPS and performs SHAKEN verification.

NOTE: If Service Provider B and/or Service Provider C have a TDM switch instead of an MGCF, an STI-IWF is used to interface with the STI-OOBS. The TDM switch invokes the STI-IWF once and the STI-IWF invokes the STI-OOBS twice, first to retrieve the PASSporT(s) from the first STI-CPS and second to publish the PASSporT(s) to the second STI-CPS.

8.10 Internal TDM NNI – External SIP NNIs

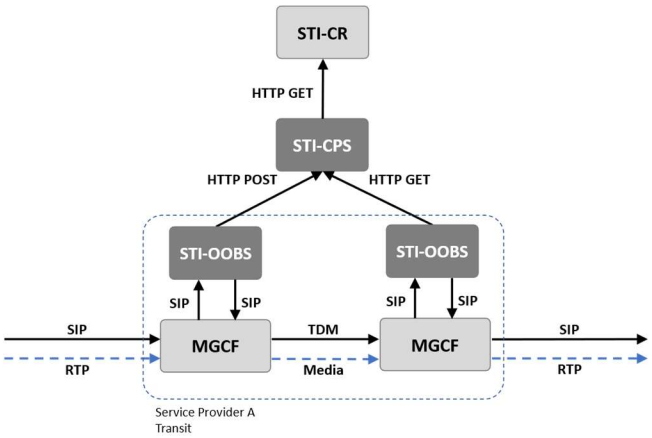

Figure 8-10: Internal TDM NNI – External SIP NNIs

Figure 8-10 shows a call that traverses an internal TDM NNI with external SIP NNIs. The following SHAKEN procedure occurs:

1. Service Provider A publishes the PASSporT(s) to an STI-CPS.
2. Service Provider A retrieves the PASSporT(s) from an STI-CPS.

8.11 Internal TDM NNI – External TDM NNIs

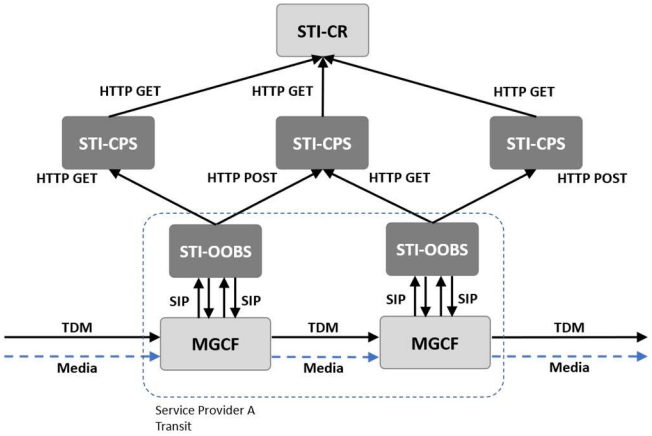

Figure 8-11: Internal TDM NNI – External TDM NNIs

Figure 8-11 shows a call that traverses an internal TDM NNI with external TDM NNIs. The following SHAKEN procedure occurs:

1. Service Provider A retrieves the PASSporT(s) from an STI-CPS.
2. Service Provider A publishes the PASSporT(s) to an STI-CPS.
3. Service Provider A retrieves the PASSporT(s) from an STI-CPS.
4. Service Provider A publishes the PASSporT(s) to an STI-CPS.

NOTE: If Service Provider A has TDM switches instead of MGCFs, an STI-IWF is used to interface with the STI-OOBS. Each TDM switch invokes the STI-IWF once and the STI-IWF invokes the STI-OOBS twice, first to retrieve the PASSporT(s) from the first STI-CPS and second to publish the PASSporT(s) to the second STI-CPS.