ATIS-1000096

ATIS Standard on -

Signature-based Handling of Asserted information using toKENs (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks

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-1000096

ATIS Standard on

Signature-Based Handling of Asserted information Using Tokens (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks

Alliance for Telecommunications Industry Solutions

Approved July 15, 2021

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 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.

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

Table of Contents

Table of Figures

ATIS Standard on –

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

Out-of-Band PASSporT Transmission Involving TDM Networks

1 Scope, Purpose, & Application

1.1 Scope

This specification extends the SHAKEN framework to enable the transmission of Personal ASSertion Tokens (PASSporTs), as defined in RFC 8225, *Personal Assertion Token*, for calls that use TDM signaling and/or TDM switches during transit. This specification adheres to the following core principles:

1. The solution does not place any new requirements on SHAKEN-compliant VoIP service providers.
2. Preferably, the solution supports the most common call scenarios representing a majority of traffic but does not need to support all possible call scenarios.
3. The solution supports and facilitates the long-term industry goal of migrating to VoIP-based networks.

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 draft-ietf-stir-servprovider-oob-01, *Out-of-Band STIR for Service Providers*.

It is recommended that ATIS-1000097, *Technical Report on Alternatives for Caller Authentication for Non-IP Traffic*, 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.v002, *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)*, 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*. 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. *Out-of-Band PASSporT Transmission Involving TDM Networks* 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 remains 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-1000074.v002, *ATIS Standard on Signature-based Handling of Asserted Information using Tokens (SHAKEN).*[1]

[Ref 4] ATIS-1000080.v003, *SHAKEN: Governance Model and Certificate Management.*[1]

[Ref 5] ATIS-1000087, *Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN).* [1]

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

[Ref 7] IETF RFC 3966, *The tel URI for Telephone Numbers.* [2]

[Ref 8] IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax.* [2]

[Ref 9] IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace.* [2]

[Ref 10] IETF RFC 4949, *Internet Security Glossary, Version 2.* [2]

[Ref 11] IETF RFC 6585, *Additional HTTP Status Codes.* [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] draft-ietf-stir-servprovider-oob-01, *Out-of-Band STIR for Service Providers*. [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 >.

[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/ >.

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 [IETF RFC 3261, *SIP: Session Initiation Protocol*] message.

(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*]. 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 10].

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 10].

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 10].

Chain of Trust: Deprecated term referring to the chain of certificates to a trust anchor. Synonym for Certification Path or Certificate Chain [Ref 10].

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*]. (see Operating Company Number)

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 10].

Public Key: The public component of a pair of cryptographic keys used for asymmetric cryptography [Ref 10].

Public Key Infrastructure (PKI): The set of hardware, software, personnel, policy, and procedures used by a CA to issue and manage certificates [Ref 10].

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 logical 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.v003, *SHAKEN: Governance Model and Certificate Management*].

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 Resp Org ID assigned to a Resp Org as defined in ATIS-0417001-003.

Signature: Created by signing the message using the private key. It verifies the identity of the sender and the integrity of the data [Ref 10].

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
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
IBCF	Interconnection Border Control Function
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
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 Involving TDM Networks

Out-of-Band PASSporT Transmission Involving TDM Networks, as defined in this document, is a SHAKEN-specific implementation of draft-ietf-stir-servprovider-oob-01 [Ref 102]. Readers of this document are expected to be familiar with draft-ietf-stir-servprovider-oob-01 [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 access control. An STI-CPS has a standardized interface for service providers to publish and retrieve PASSporT(s).

In order 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 must include a JSON Web Token (JWT), as defined in RFC 7519, *JSON Web Token*, that is both fresh and signed by a valid, unrevoked STI certificate. In order to validate JWTs, the STI-CPS must interface with the STI-PA to retrieve the trusted Secure Telephone Identity Certification Authority (STI-CA) list and Certificate Revocation List (CRL).

Each STI-CPS must republish all PASSporT(s) received to every other STI-CPS within the country's SHAKEN ecosystem. This allows service providers to retrieve PASSporT(s) from any STI-CPS, regardless of which STI-CPS the PASSporT was originally published to. See Clause 7 for STI-CPS normative requirements.

The operator of the STI-CPS must be registered with the STI-PA and have an STI certificate to republish PASSporT(s) to other STI-CPSs using the publish PASSporT(s) Application Programming Interface (API) endpoint described in this document. The method for an STI-CPS to discover other STI-CPSs in the country's SHAKEN ecosystem is out of scope for this document.

The service provider that converts a call from SIP signaling to TDM signaling must publish all associated PASSporT(s) received in the SIP signaling, as defined in RFC 3261 [Ref 6] (e.g., SIP INVITE) to an STI-CPS. An OSP that sends a call via a TDM NNI must generate the applicable PASSporT(s) and then publish the PASSporT(s) to an STI-CPS. If a call is converted from SIP signaling to TDM signaling multiple times, then multiple service providers will publish the same PASSporT(s) to an STI-CPS.

The service provider that converts a call from TDM signaling to SIP signaling must send a request to an STI-CPS to retrieve all PASSporT(s) associated with the call and insert the retrieved PASSporT(s) into the SIP signaling in Identity header(s) as described in RFC 8224 [Ref 13]. If the service provider is unable to determine some required Identity header parameters, the service provider must still insert the Identity header into the SIP signaling with the PASSporT and all Identity header parameters that can be determined. A TSP, that receives a call via a TDM NNI, must send a request to an STI-CPS to retrieve all PASSporT(s) associated with the call and insert the retrieved PASSporT(s) into the SIP signaling in Identity header(s) for delivery to the TSP's STI-VS function. If the call is converted from TDM signaling to SIP signaling multiple times, then multiple service providers will retrieve the same PASSporT(s) from an STI-CPS.

This mechanism requires that the service provider that is retrieving the PASSporT(s) reconstruct any SIP headers that were lost in the conversion from SIP to TDM back to SIP, when the SIP headers are protected by the PASSporT(s) (e.g., SIP Resource Priority Header and/or Priority header when an "rph" PASSporT is retrieved).

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*.

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 the examples of Clause 8, below, 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 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).

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 to utilize SHAKEN functional elements. The STI-IWF accepts SS7 signaling messages (e.g., ISUP or TCAP), 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.

In a reference architecture illustrated in the examples of Clause 8, below, 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.

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 must implement the following three API endpoints:

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

The health check and publish PASSporT(s) API endpoints are used by both service providers and other STI-CPSs. The retrieve PASSporT(s) API endpoint is used only by service providers.

All API endpoints must 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.

The STI-CPS may support additional authentication mechanisms and/or additional API endpoints (e.g., retrieve PASSporT(s) for multiple calls at once).

The STI-CPS should not retain PASSporT(s) or corresponding authentication JWT(s) after the PASSporT(s) are no longer considered fresh according to the STI-CPS’s local freshness policy. A default retention period of 15 seconds is suggested.

7.1 Health Check

The health check API endpoint of each STI-CPS must be accessible via an HTTP GET request to the path “/health”. An HTTP 200 status code must 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 must 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 must return standard HTTP error response codes as defined in RFC 6585, *Additional HTTP Status Codes*.

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 must be accessible via an HTTP POST request to the path "/passports/DEST/ORIG". The "DEST" parameter must be replaced with the percent encoded, canonicalized called destination Telephone Number (TN) (e.g., TN in a SIP request URI) or, when there is no called destination TN that can be considered a "valid telephone number" as described in ATIS-1000074.v002 [Ref 3], the percent encoded called destination URI. Destination TN refers to the TN of a called user endpoint to be reached in a TSP network after the latest retargeting, if any, as derived from the SIP request URI. The "ORIG" parameter must be replaced with the percent encoded, canonicalized calling party TN (e.g., TN from SIP P-Asserted-Identity header or SIP From header) or, when there is no calling party TN that can be considered a "valid telephone number" as described in ATIS-1000074.v002 [Ref 3], the percent encoded calling party URI. The TN canonicalization procedures are described in RFC 8224 [Ref 13]. As an example, the TN "+1 (903) 246-9103" would be canonicalized as "19032469103". The percent encoding procedures are described in RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*. As an example, the URI "urn:service:sos" would be percent encoded as "urn%3Aservice%3Asos". As noted in Clause 7.3, not all URIs will lead to successful retrieval transactions when used as "ORIG" or "DEST" as part of an STI-CPS API path value.

The request must have a "Content-Type" header set to "application/json". The body of the request must be a JSON object. The JSON object must include the key "passports". The value of the key "passports" must be an array of strings where each string is a PASSporT. All PASSporT(s) received in the SIP signaling must be included in the array of "passports". If the request is being made by an STI-CPS to republish PASSporT(s), then the JSON object must also include the key "token". The value of the key "token" must be a string containing the authentication JWT that was used by the service provider to authenticate with the STI-CPS that is republishing the PASSporT(s).

The request must include a bearer token in the "Authorization" header. The bearer token must be a JWT that is both fresh and signed by a valid, unrevoked STI certificate that chains up to an approved STI-CA root certificate. The JWT header must include an "alg" claim with the value "ES256". The JWT header must include an "x5u" claim indicating the Uniform Resource Identifier (URI) of the STI certificate that was used to sign the JWT. The JWT payload must include an "iat" claim indicating the timestamp of when the JWT was signed. The JWT payload must include an "aud" claim with the Fully Qualified Domain Name (FQDN) of the STI-CPS as the value. The JWT payload must include an "iss" claim with the Service Provider Code (SPC) of the service provider that signed the JWT as

the value. The JWT payload must include a “sub” claim with the SPC of the service provider that is making the request as the value. Both the “iss” and “sub” claims must match the SPC in the TNAuthList extension of the certificate that was used to sign the JWT. If the JWT is generated by a service provider to publish PASSporT(s), then the JWT payload must include an "action" claim with the literal string "publish" as the value. If the JWT is generated by an STI-CPS to republish PASSporT(s), then the JWT payload must include an "action" claim with the literal string "republish" as the value. The JWT payload must 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 must 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*, as the value. The JWT payload must include an “orig” claim with a “tn” or “uri” value that is the same as the percent decoded “ORIG” parameter. The JWT payload must include a “dest” claim with a “tn” or “uri” value that is the same as the percent decoded “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 of these requirements, then the request must 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.crt"
}
```


Payload:


```
{
  "iat": 1608048420,
  "action": "publish",
  "passports": "sha256-YO4Hq/xE6mkCeuPoYYck5Pt6vACmfbzNfdi6aeq95dA=",
  "sub": "1234",
  "iss": "1234",
  "aud": "cps.example.com",
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059",
  "dest": {
    "tn": [
      "19032469103"
    ]
  },
  "orig": {
    "tn": "12013776051"
  }
}
```

The header and payload of an example authentication JWT for a “republish” request are below:

Header:


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


Payload:


```
{
  "iat": 1608048420,
  "action": "republish",
  "passports": "sha256-YO4Hq/xE6mkCeuPoYYck5Pt6vACmfbzNfdi6aeq95dA=",
  "sub": "1234",
  "iss": "1234",
  "aud": "cps.example.com",
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059",
  "dest": {
    "tn": [
      "19032469103"
    ]
  },
  "orig": {
    "tn": "12013776051"
  }
}
```


An HTTP 201 status code must be returned if the PASSporT(s) were published. An HTTP status code greater than 399 must be returned if the PASSporT(s) were not published. The publish API endpoint must return standard HTTP error response codes as defined in RFC 6585 [Ref 11]. If possible, a service provider should publish the PASSporT(s) to a different STI-CPS if a server error (HTTP 5xx status code) is received. The STI-CPS may, based on local policy, return an HTTP 201 status code prior to receiving an HTTP 201 status code from all republish requests.

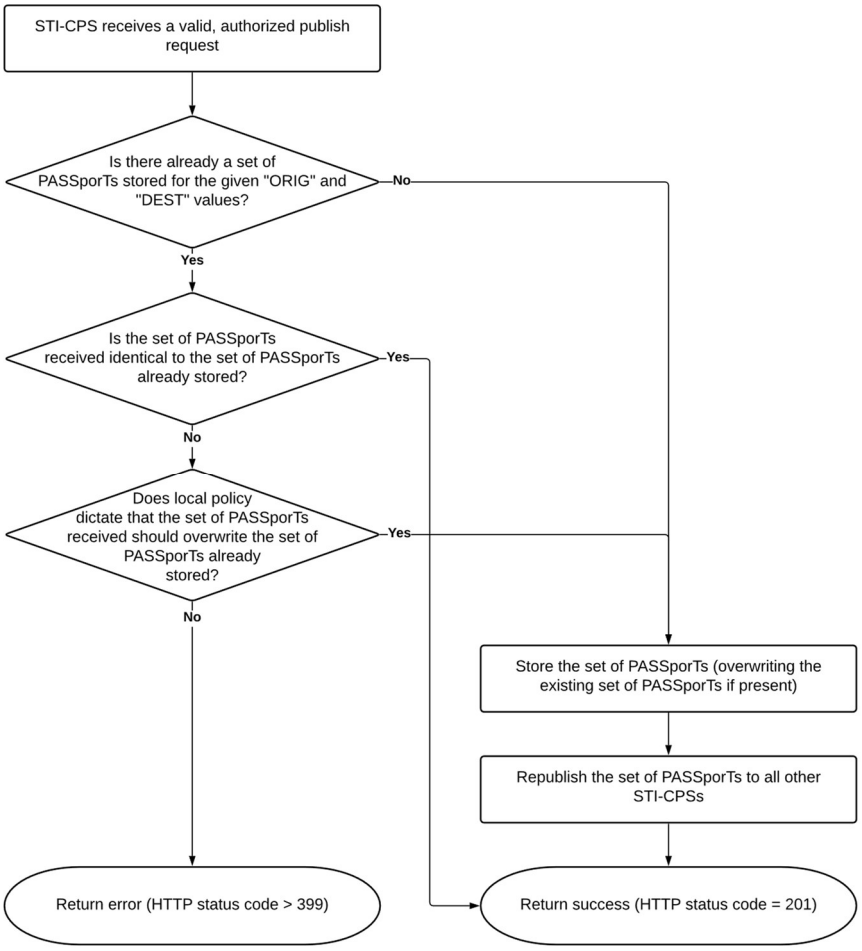

Figure 7-1: STI-CPS Processing Logic

Figure 7-1 shows the processing logic for how an STI-CPS must handle requests.

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/19032469103/12013776051 HTTP/1.1
Content-Type: application/json
Content-Length: 423
Host: cps.example.com
Authorization: Bearer
eyJhbGciOiJFUzI1NiIsIng1dSI6Imh0dHBzOi8vY2VydGlmaWNhdGVzLmV4YW1wbGUuY29tL2V4YW1wbGUuY3J0In0
.eyJpYXQiOjE2MDgwNDg0MjAsImFjdGlvbiI6InB1Ymxpc2giLCJwYXNzcG9ydHMiOiJzaGEyNTYtWU80SHEveEU2bW
tDZXVQb1lZY2s1UHQ2dkFDbWZiek5mZGk2YWVxOTVkQT0iLCJzdWIiOiIxMjM0IiwiaXNzIjoiMTIzNCIsImF1ZCI6I
mNwcy5leGFtcGxlLmNvbSIsImp0aSI6ImViY2JkN2YyLWI3OGItNDAxOS1iZjgzLTMyYzI1MTdlNjA1OSIsImRlc3Qi
OnsidG4iOlsiMTkwMzI0NjkxMDMiXX0sIm9yaWciOnsidG4iOiIxMjAxMzc3NjA1MSJ9fQ.1_Nty37vqW0aEHn7y5k9
Da9vXO_FvWSMGY6xOh6U_7RbGOSm0H9BK_xTqXRhtXCM6IcBm6rIsTW5BDEg6SwbBQ

{"passports":["eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0
cHM6Ly9jZXJ0aWZpY2F0ZXMuZXhhbXBsZS5jb20vZXhhbXBsZS5jcnQifQ.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0
biI6WyIxOTAzMjQ2OTEwMyJdfSwiaWF0IjoxNTg0OTgzNDAyLCJvcmlnIjp7InRuIjoiMTIwMTM3NzYwNTEifSwib3J
```

pZ2lkIjoiNGFlYzk0ZTItNTA4Yy00YzFjLTkwN2ItMzczN2JhYzBhODBlIn0.EMfXHyowsI5s73KqoBzJ9pzrrwGFNK
BRmHcx-YZ3DjPgBe4Mvqq9N-bThN1_HTWeSvbruAyet26fetRL1_bn1g"]}

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

```
POST /passports/19032469103/12013776051 HTTP/1.1
Content-Type: application/json
Content-Length: 955
Host: cps.example.com
Authorization: Bearer
eyJhbGciOiJFUzI1NiIsIng1dSI6Imh0dHBzOi8vY2VydGlmaWNhdGVzLmV4YW1wbGUuY29tL2V4YW1wbGUuY3J0In0
.eyJpYXQiOjE2MDgwNDg0MjAsImFjdGlvbiI6InJlcHVibGlzaCIsInBhc3Nwb3J0cyI6InNoYTI1Ni1ZTzRIcS94RT
Zta0NldVBvWVljazVQdDZ2QUNtZmJ6TmZkaTZhZXE5NWRBPSIsInN1YiI6IjEyMzQiLCJpc3MiOiIxMjM0IiwiYXVkI
joiY3BzLmV4YW1wbGUuY29tIiwianRpIjoiZWJjYmQ3ZjItYjc4Yi00MDE5LWJmODMtMzJjMjUxN2U2MDU5IiwiZGVz
dCI6eyJ0biI6WyIxOTAzMjQ2OTEwMyJdfSwib3JpZyI6eyJ0biI6IjEyMDEzNzc2MDUxIn19.1_Nty37vqW0aEHn7y5
k9Da9vXO_FvWSMGY6xOh6U_7RbGOSm0H9BK_xTqXRhtXCM6IcBm6rIsTW5BDEg6SwbBQ

{"token":"eyJhbGciOiJFUzI1NiIsIng1dSI6Imh0dHBzOi8vY2VydGlmaWNhdGVzLmV4YW1wbGUuY29tL2V4YW1wb
GUuY3J0In0.eyJpYXQiOjE2MDgwNDg0MjAsImFjdGlvbiI6InB1Ymxpc2giLCJwYXNzcG9ydHMiOiJzaGEyNTYtWU80
SHEveEU2bWtDZXVQb1lZY2s1UHQ2dkFDbWZiek5mZGk2YWVxOTVkQT0iLCJzdWIiOiIxMjM0IiwiaXNzIjoiMTIzNCI
sImF1ZCI6ImNwcy5leGFtcGxlLmNvbSIsImp0aSI6ImViY2JkN2YyLWI3OGItNDAxOS1iZjgzLTMyYzI1MTdlNjA1OS
IsImRlc3QiOnsidG4iOlsiMTkwMzI0NjkxMDMiXX0sIm9yaWciOnsidG4iOiIxMjAxMzc3NjA1MSJ9fQ.1_Nty37vqW
0aEHn7y5k9Da9vXO_FvWSMGY6xOh6U_7RbGOSm0H9BK_xTqXRhtXCM6IcBm6rIsTW5BDEg6SwbBQ","passports":[
"eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ0aW
ZpY2F0ZXMuZXhhbXBsZS5jb20vZXhhbXBsZS5jcnQifQ.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyIxOTAzMj
Q2OTEwMyJdfSwiaWF0IjoxNTg0OTgzNDAyLCJvcmlnIjp7InRuIjoiMTIwMTM3NzYwNTEifSwib3JpZ2lkIjoiNGFlY
zk0ZTItNTA4Yy00YzFjLTkwN2ItMzczN2JhYzBhODBlIn0.EMfXHyowsI5s73KqoBzJ9pzrrwGFNKBRmHcx-
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 must be accessible via an HTTP GET request to the path "/passports/DEST/ORIG". The "DEST" parameter must be replaced with the percent encoded, canonicalized called destination TN (e.g., SIP request URI) or, when there is no called destination TN that can be considered a "valid

telephone number" as described in [Ref 3], the percent encoded called destination URI. Destination TN refers to the TN of a called user endpoint to be reached in a TSP network after the latest retargeting, if any, as derived from the SIP request URI. The "ORIG" parameter must be replaced with the percent encoded, canonicalized calling party TN (e.g., TN from SIP P-Asserted-Identity header or SIP From header) or, when there is no calling party TN that can be considered a "valid telephone number" as described in ATIS-1000074.v002 [Ref 3], the percent encoded calling party URI. The TN canonicalization procedures are described in RFC 8224 [Ref 13]. As an example, the TN "+1 (903) 246-9103" would be canonicalized as "19032469103". The percent encoding procedures are described in RFC 3986 [Ref 8]. As an example, the URI "urn:service:sos" would be percent encoded as "urn%3Aservice%3Asos". The STI-CPS will treat DEST parameters of "urn:service:sos" and "911" as synonymous when determining which PASSporT(s) match the retrieve request. PASSporT(s) may not be retrievable if the call uses a destination URI or a calling party URI, and the URI cannot be determined after the conversion from SIP to TDM to SIP.

The request must include a bearer token in the "Authorization" header. The bearer token must be a JWT that is both fresh and signed by a valid, unrevoked STI certificate that chains up to an approved STI-CA root certificate. The STI-CA root certificate must be in the trust list of the STI-PA for the STI-CPS's local country. The JWT header must include an "alg" claim with the value "ES256". The JWT header must include an "x5u" claim indicating the URI of the STI certificate that was used to sign the JWT. The JWT payload must include an "iat" claim indicating the timestamp of when the JWT was signed. The JWT payload must include an "aud" claim with the FQDN of the STI-CPS as the value. The JWT payload must include an "iss" claim with the SPC of the service provider that signed the JWT as the value. The JWT payload must include a "sub" claim with the SPC of the service provider that is making the request as the value. Both the "iss" and "sub" claims must match the SPC in the TNAuthList extension of the certificate that was used to sign the JWT. The JWT payload must include an "action" claim with the literal string "retrieve" as the value. The JWT payload must include a "jti" claim with a unique version 4 UUID as the value. The JWT payload must include an "orig" claim with a "tn" or "uri" value that is the same as the percent decoded "ORIG" parameter. The JWT payload must include a "dest" claim with a "tn" or "uri" value that is the same as the percent decoded "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 of these requirements, then the request must 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.crt"
}
```


Payload:


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

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


If one or more PASSporTs are returned, then the response must have a “Content-Type” header set to “application/json”. The body of the response must be a JSON object. The JSON object must include the keys “tokens” and “passports”. The value of the key “tokens” must be an array of strings where each string is an authentication JWT. The authentication JWT used by the service provider to publish the PASSporT(s) must be included in the array of “tokens”. If the PASSporT(s) were republished by an STI-CPS, then the authentication JWT used by the STI-CPS to republish the PASSporT(s) must also be included in the array of “tokens”. The value of the key “passports” must be an array of strings where each string is a PASSporT. All PASSporT(s) received in the publish request must be included in the array of “passports”.

An HTTP 200 status code must be returned if one or more PASSporTs are returned. An HTTP status code greater than 399 must be returned if no PASSporT(s) are returned. The retrieve API endpoint must return standard HTTP error response codes as defined in RFC 6585 [Ref 11]. If possible, a service provider should retrieve the PASSporT(s) from a different STI-CPS if a server error (HTTP 5xx status code) is received.

The authentication JWTs could be logged by the service provider retrieving the PASSporT(s) for the purposes of traceback of the PASSporT(s) within the STI-CPS network.

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/19032469103/12013776051 HTTP/1.1
Content-Length: 0
Host: cps.example.com
Authorization: Bearer
eyJhbGciOiJFUzI1NiIsIng1dSI6Imh0dHBzOi8vY2VydGlmaWNhdGVzLmV4YW1wbGUuY29tL2V4YW1wbGUuY3J0In0
.eyJpYXQiOjE2MDgwNDg0NDQsImFjdGlvbiI6InJldHJpZXZlIiwic3ViIjoiMTIzNCIsImlzcyI6IjEyMzQiLCJhdW
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: 958

{"tokens":["eyJhbGciOiJFUzI1NiIsIng1dSI6Imh0dHBzOi8vY2VydGlmaWNhdGVzLmV4YW1wbGUuY29tL2V4YW1
wbGUuY3J0In0.eyJpYXQiOjE2MDgwNDg0MjAsImFjdGlvbiI6InB1Ymxpc2giLCJwYXNzcG9ydHMiOiJzaGEyNTYtWU
80SHEveEU2bWtDZXVQb1lZY2s1UHQ2dkFDbWZiek5mZGk2YWVxOTVkQT0iLCJzdWIiOiIxMjM0IiwiaXNzIjoiMTIzN
CIsImF1ZCI6ImNwcy5leGFtcGxlLmNvbSIsImp0aSI6ImViY2JkN2YyLWI3OGItNDAxOS1iZjgzLTMyYzI1MTdlNjA1
OSIsImRlc3QiOnsidG4iOlsiMTkwMzI0NjkxMDMiXX0sIm9yaWciOnsidG4iOiIxMjAxMzc3NjA1MSJ9fQ.1_Nty37v
qW0aEHn7y5k9Da9vXO_FvWSMGY6xOh6U_7RbGOSm0H9BK_xTqXRhtXCM6IcBm6rIsTW5BDEg6SwbBQ"],"passports
":["eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ
0aWZpY2F0ZXMuZXhhbXBsZS5jb20vZXhhbXBsZS5jcnQifQ.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyIxOTA
zMjQ2OTEwMyJdfSwiaWF0IjoxNTg0OTgzNDAyLCJvcmlnIjp7InRuIjoiMTIwMTM3NzYwNTEifSwib3JpZ2lkIjoiNG
FlYzk0ZTItNTA4Yy00YzFjLTkwN2ItMzczN2JhYzBhODBlIn0.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

Nine call scenario examples are detailed below but most call scenarios are supported by the key requirements in Clause 4. The scenarios include 1) a transit provider publishing PASSporT(s), 2) a VoIP service provider publishing PASSporT(s), and 3) a TDM switch publishing PASSporT(s) each enumerated with i) a transit provider retrieving PASSporT(s), ii) a VoIP service provider retrieving PASSporT(s), and iii) a TDM switch retrieving PASSporT(s).

8.1 Transit Provider Publish – Transit Provider Retrieve

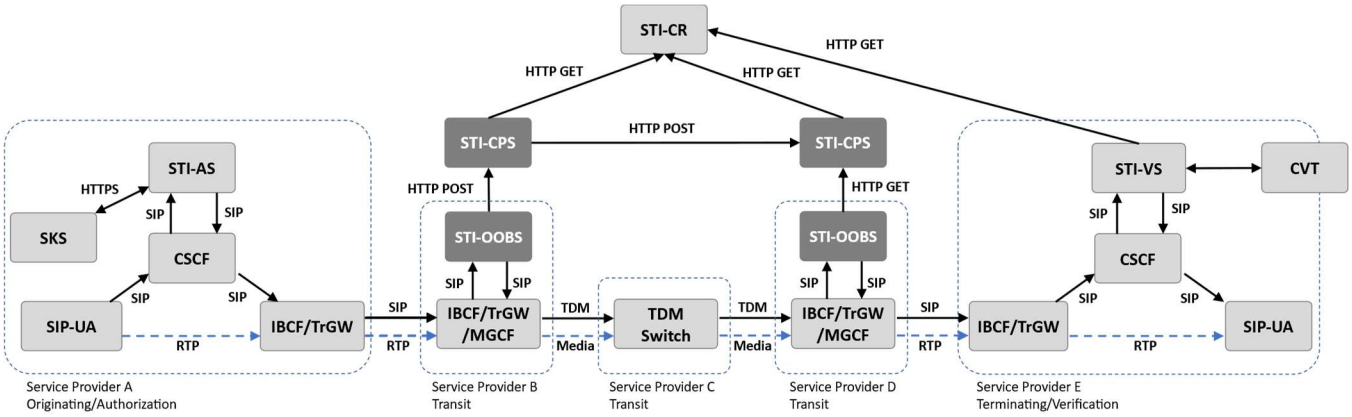

Figure 8-1: Transit Provider Publish – Transit Provider Retrieve

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 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.
4. Service Provider E performs SHAKEN verification.

8.2 Transit Provider Publish – VoIP Service Provider Retrieve

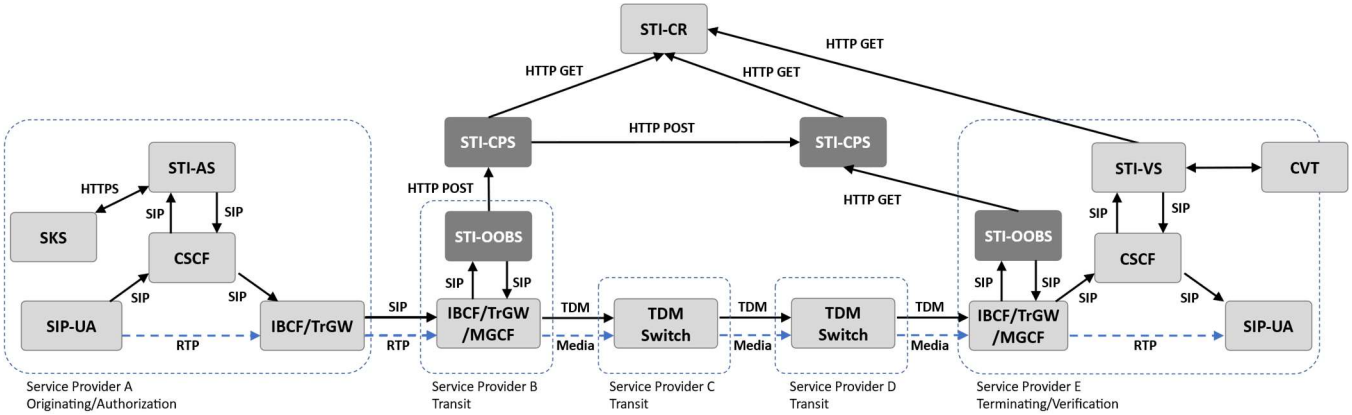

Figure 8-2: Transit Provider Publish – VoIP Service Provider Retrieve

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 E converts the call from TDM signaling to SIP signaling, retrieves the PASSporT(s) from an STI-CPS, and performs SHAKEN verification.

8.3 Transit Provider Publish – TDM Switch Retrieve

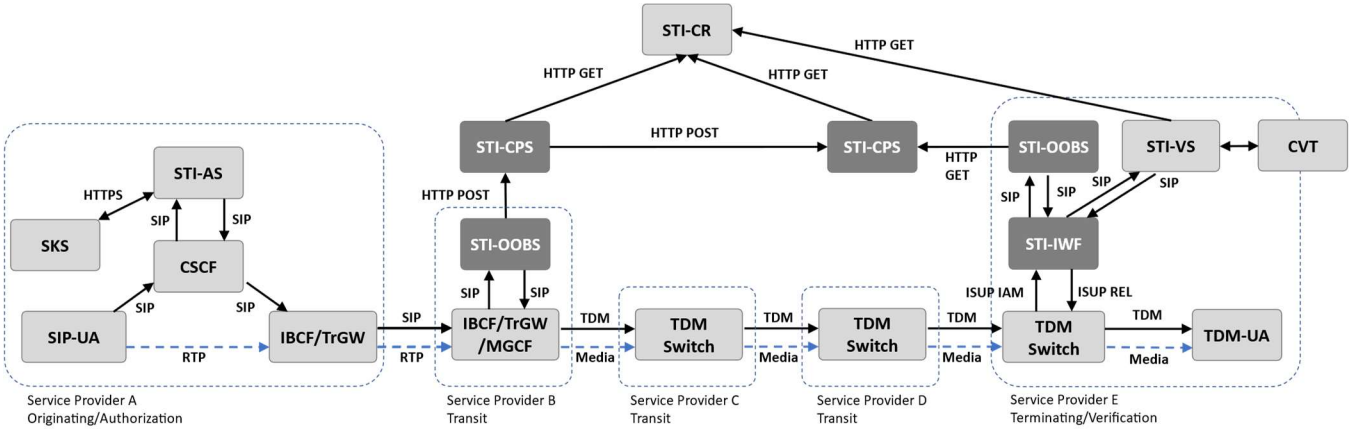

Figure 8-3: Transit Provider Publish – TDM Switch Retrieve

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 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 E (through an STI-IWF) retrieves the PASSporT(s) from an STI-CPS and performs SHAKEN verification.

8.4 VoIP Service Provider Publish - Transit Provider Retrieve

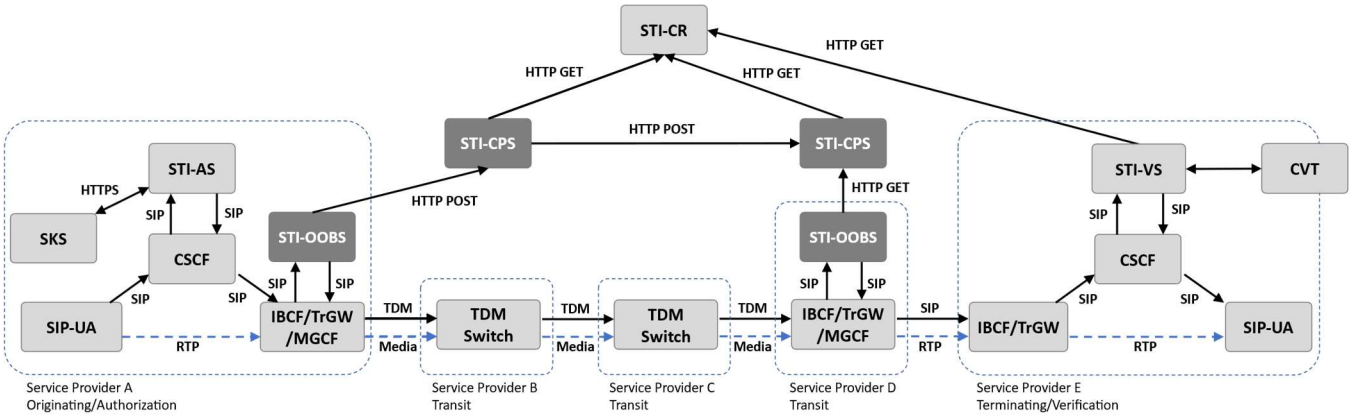

Figure 8-4: VoIP Service Provider Publish – Transit Provider Retrieve

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 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.
3. Service Provider E performs SHAKEN verification.

8.5 VoIP Service Provider Publish - VoIP Service Provider Retrieve

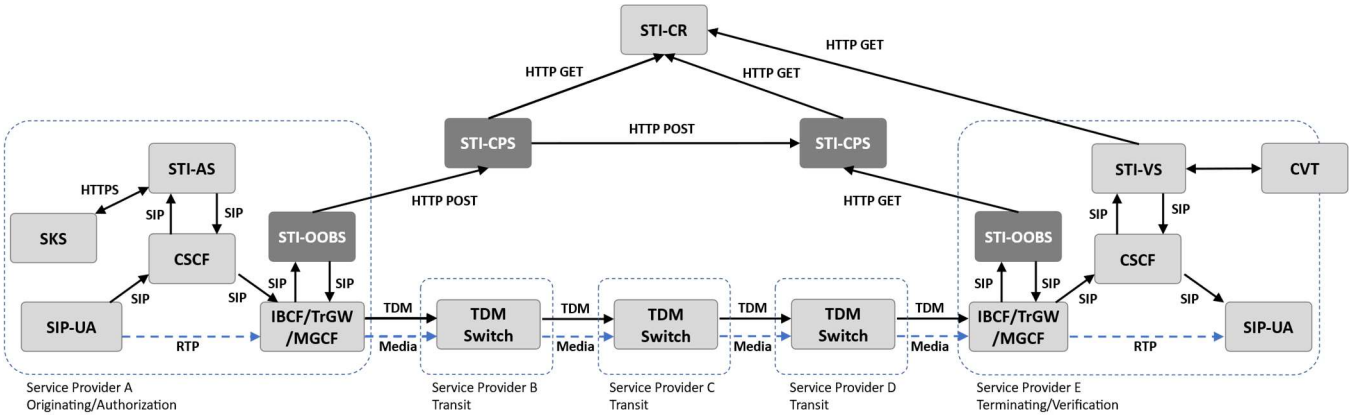

Figure 8-5: VoIP Service Provider Publish – VoIP Service Provider Retrieve

Figure 8-5 shows a call that is originated by a VoIP service provider 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 E converts the call from TDM signaling to SIP signaling, retrieves the PASSporT(s) from an STI-CPS, and performs SHAKEN verification.

8.6 VoIP Service Provider Publish - TDM Switch Retrieve

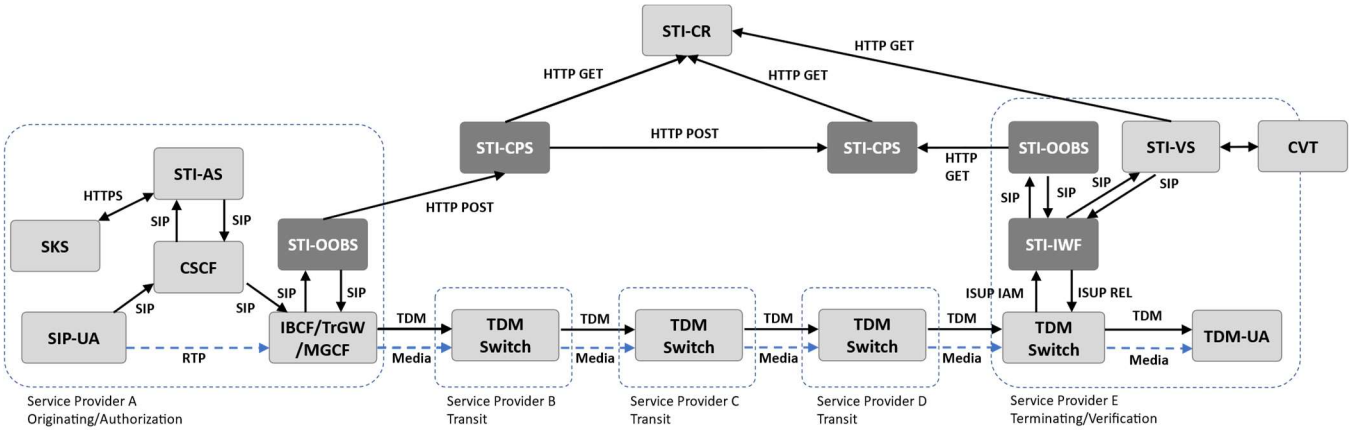

Figure 8-6: VoIP Service Provider Publish – TDM Switch Retrieve

Figure 8-6 shows a call that is originated by a VoIP service provider 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 E (through an STI-IWF) retrieves the PASSporT(s) from an STI-CPS and performs SHAKEN verification.

8.7 TDM Switch Publish - Transit Provider Retrieve

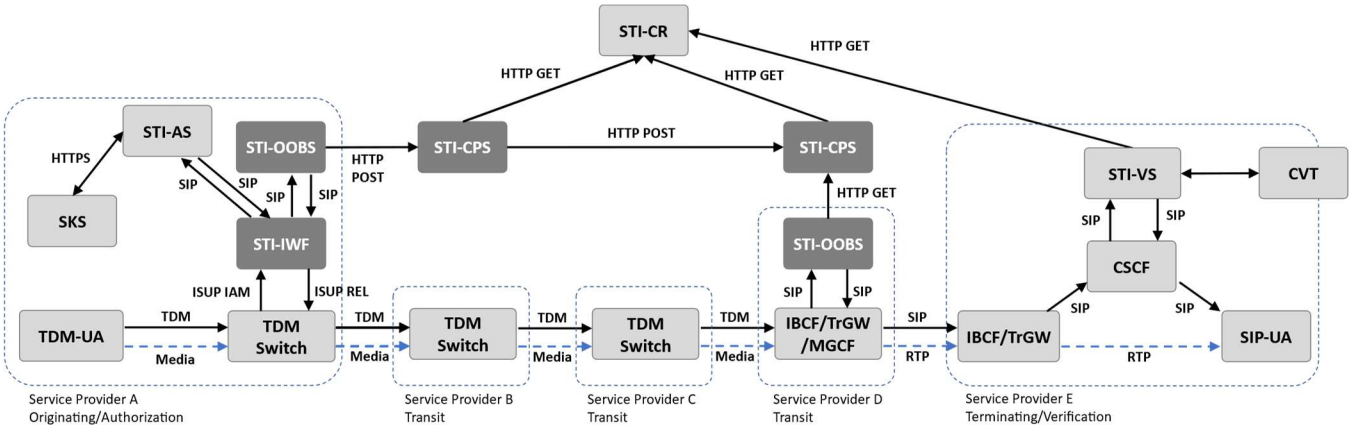

Figure 8-7: TDM Switch Publish – Transit Provider Retrieve

Figure 8-7 shows a call that is originated by 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 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.
3. Service Provider E performs SHAKEN verification.

8.8 TDM Switch Publish - VoIP Service Provider Retrieve

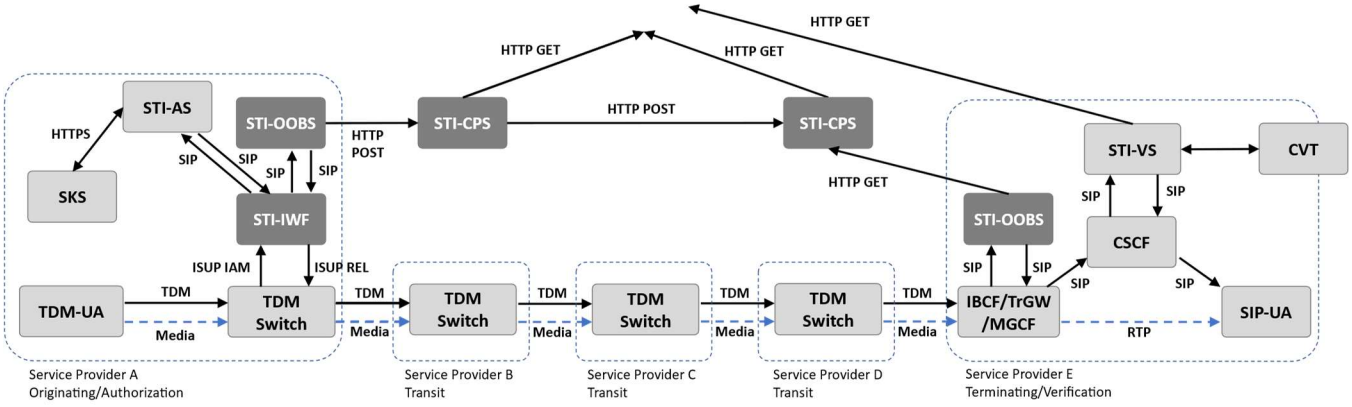

Figure 8-8: TDM Switch Publish – VoIP Service Provider Retrieve

Figure 8-8 shows a call that is originated by 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 E converts the call from TDM signaling to SIP signaling, retrieves the PASSporT(s) from an STI-CPS, and performs SHAKEN verification.

8.9 TDM Switch Publish - TDM Switch Retrieve

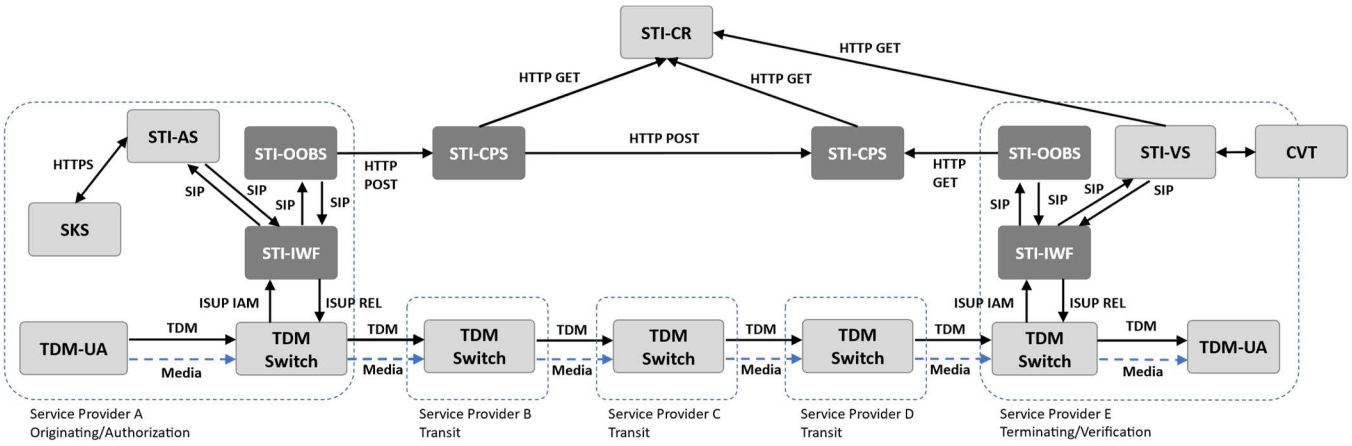

Figure 8-9: TDM Switch Publish – TDM Switch Retrieve

Figure 8-9 shows a call that is originated by a TDM switch and terminated by 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 E (through an STI-IWF) retrieves the PASSporT(s) from an STI-CPS and performs SHAKEN verification.

9 Cross-Border

ATIS-1000087, *Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)*, describes SHAKEN procedures for calls that traverse an international boundary. For the purposes of this document, an international boundary is generally treated the same as a SIP/TDM boundary. The STI-OOBS at the international boundary performs an HTTP GET and/or an HTTP POST to interact with the appropriate STI-CPS. The required functionality for cross-border traffic with either SIP signaling or TDM signaling is described below. Cross-border SHAKEN further requires certain agreements between the participating countries.

9.1 SIP Signaling

When a TDM network in one country uses SIP signaling for cross-border traffic, the STI-OOBS performs as described in Clause 8 for domestic traffic. This is true even if the cross-border SIP link is used to connect two TDM networks.

Figure 9-1 shows a TDM network in country “A” using SIP signaling for cross-border traffic. In this case, the STI-OOBS retrieves the appropriate PASSporT(s) from an STI-CPS in country “A” and inserts the PASSporT(s) in a SIP Identity header in the outgoing SIP signaling.

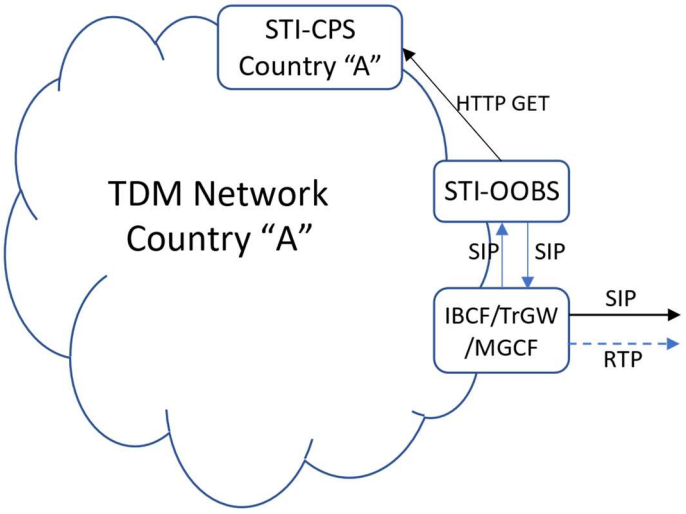

Figure 9-1: TDM Network with Outgoing Cross-Border SIP Signaling

Figure 9-2 shows a TDM network in country “B” receiving cross-border traffic using SIP signaling. In this case, the STI-OOBS extracts the PASSporT(s) from the incoming SIP Identity header and publishes the PASSporT(s) to an STI-CPS in country “B”.

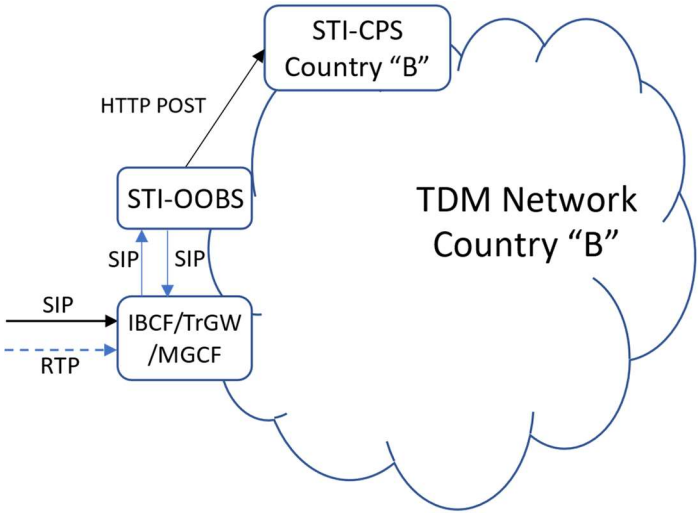

Figure 9-2: TDM Network with Incoming Cross-Border SIP Signaling

When the cross-border interconnect is using SIP signaling, the *Out-of-Band PASSporT Transmission Involving TDM Networks* functionality in the domestic TDM network does not depend on the technology used in the other network. As a result, it is possible to use this configuration for two TDM networks that are interconnected via SIP signaling, as shown in Figure 9-3.

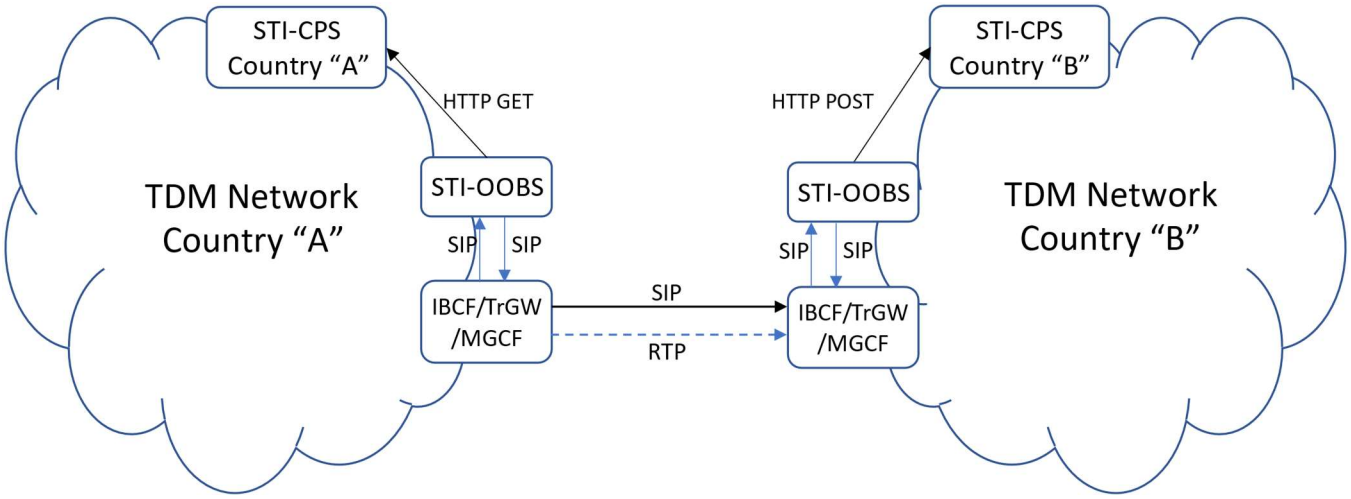

Figure 9-3: TDM Networks with Cross-Border SIP Signaling

9.2 TDM Signaling

Figure 9-4 shows the case where country "A" and country "B" are using TDM signaling for cross-border traffic between TDM networks, and each country has an independent deployment of *Out-of-Band PASSporT Transmission Involving TDM Networks*. At the international TDM Gateway (GW) (through an STI-IWF), the STI-OOBS authenticates with an STI-CPS using country "A" credentials and retrieves the appropriate PASSporT(s). Then the STI-OOBS is invoked again to publish the PASSporT(s) to an STI-CPS in country "B" using country "A" credentials.

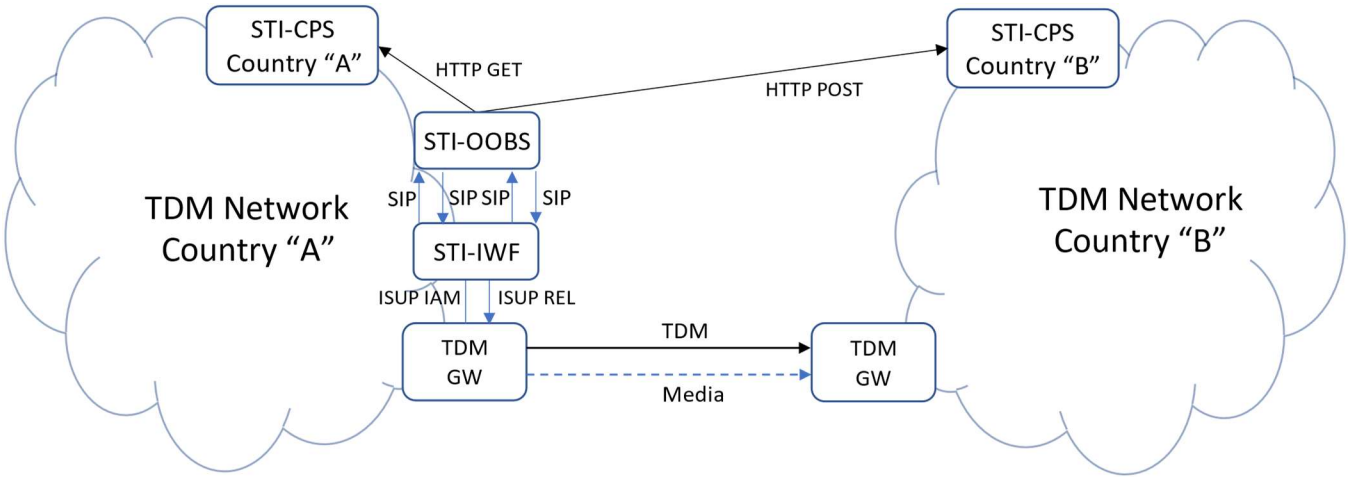

Figure 9-4: TDM Signaling for Cross-Border Traffic

Figure 9-5 shows the same scenario as Figure 9-4, but with traffic flowing in the opposite direction – i.e., calling from country "B" to country "A". In this case, the STI-OOBS in country "B" retrieves/publishes the PASSporT(s). This means that STI-OOBS will be required on both sides of the international border.

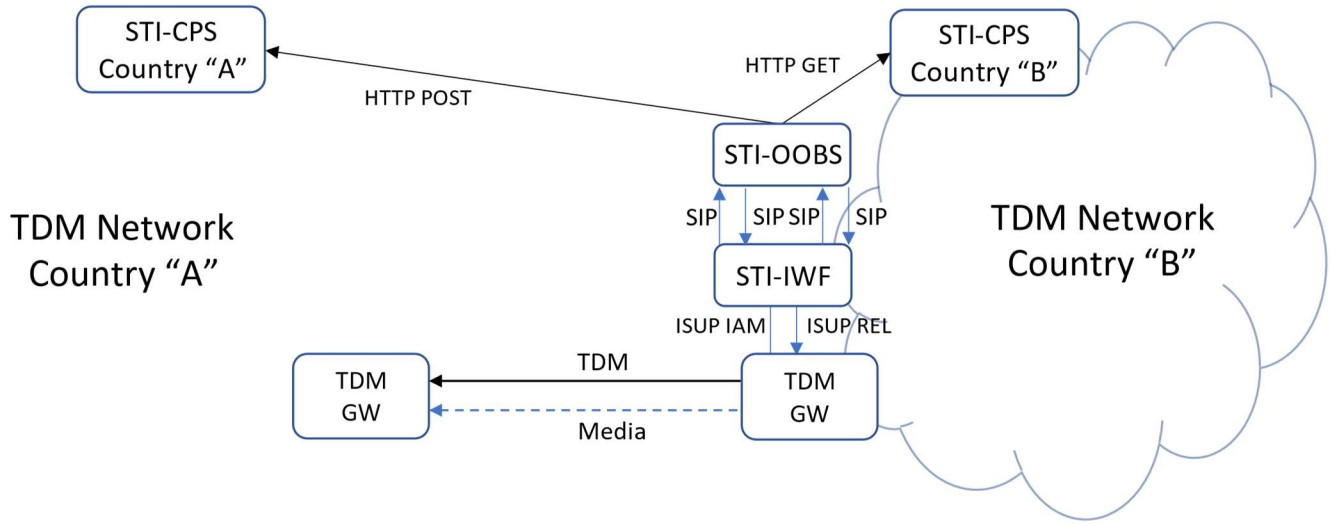

Figure 9-5: TDM Signaling for Cross-Border Traffic from "B" to "A"

In some cases, TDM signaling may be used when the network is SIP up to the border GW, as shown in Figure 9-6. In this case, the STI-OOBS functions the same as it does at the SIP signaling to TDM signaling transition within a domestic network, except that after the STI-OOBS accesses the PASSporT(s) from the SIP signaling in country "A", it publishes the PASSporT(s) to an STI-CPS in country "B".

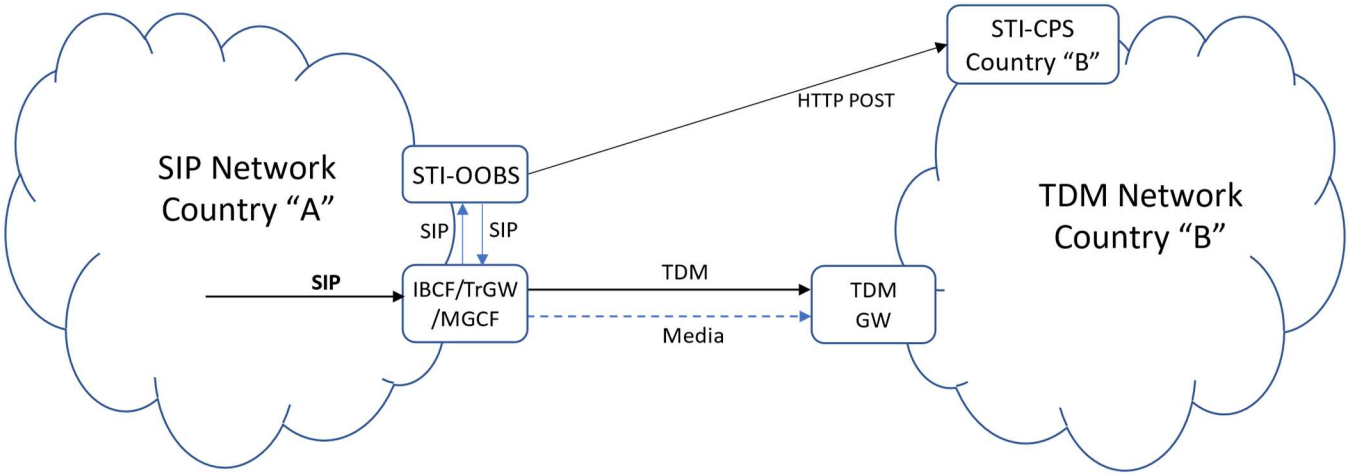

Figure 9-6: TDM Signaling from a SIP Network

With this approach, it is even technically possible to support two SIP networks that use TDM signaling. In this case, the STI-OOBS in country "A" extracts the PASSporT(s) from the incoming SIP signaling and publishes the PASSporT(s) to an STI-CPS in country "B". Then, in the receiving network, a local STI-OOBS retrieves the PASSporT(s) from a country "B" STI-CPS and inserts the PASSporT(s) into the outgoing SIP signaling. This is shown in Figure 9-7.

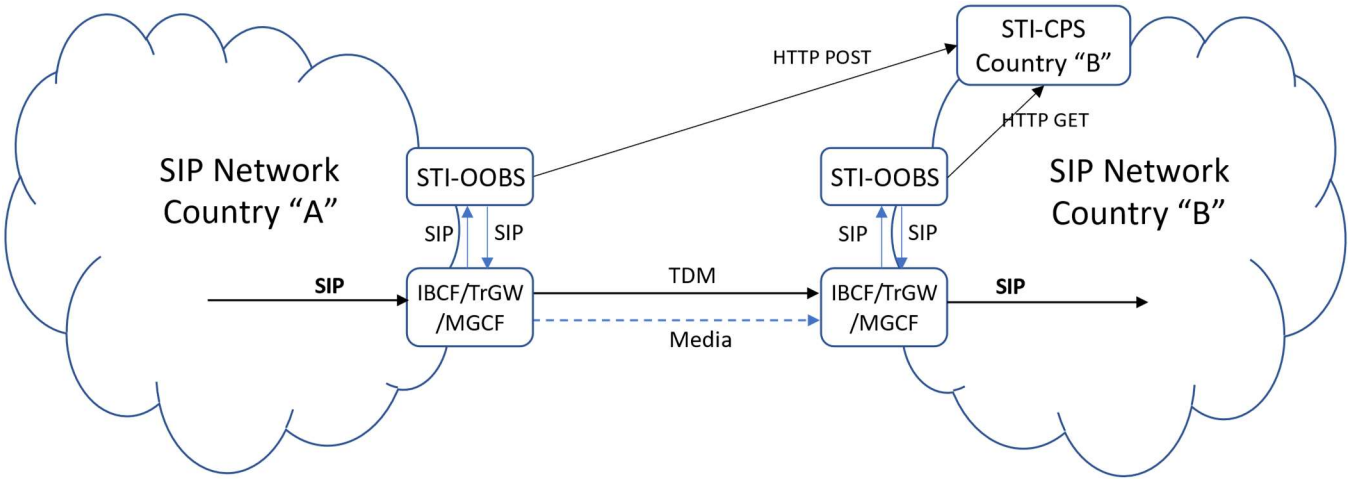

Figure 9-7: TDM Signaling Between SIP Networks