ATIS-0x0000x

ATIS Standard on

**Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Out-of-Band Token Transmission**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

The SHAKEN framework enables a SHAKEN-authorized VoIP Service Provider to deliver cryptographic proof to a called user via SIP signaling that the calling user is authorized to use the calling telephone number. This specification extends this current framework to enable an originating service provider to send the caller identity PASSporTs to the terminating service provider out-of-band, that is, across the internet, separate from the SIP signaling.

**Foreword**

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [**COMMITTEE NAME**] Committee [**INSERT MISSION**]. [**INSERT SCOPE**].

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes 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, [**COMMITTEE NAME**], 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, [**COMMITTEE NAME**], which was responsible for its development, had the following leadership:

[**LEADERSHIP LIST**]

The **[SUBCOMMITTEE NAME]** Subcommittee was responsible for the development of this document.

**Table of Contents**

1 Scope, Purpose, & Application 1

1.1 Scope 1

1.2 Purpose 1

2 Normative References 1

3 Definitions, Acronyms, & Abbreviations 2

3.1 Definitions 2

3.2 Acronyms & Abbreviations 3

4 Overview 5

4.1 Problem Statement – Why Out-of-Band SHAKEN is needed 5

5 Out-of-Band SHAKEN 5

5.1 Out-of-Band SHAKEN Architecture 5

5.2 Out-of-Band SHAKEN Overview 6

5.3 Out-of-Band SHAKEN Call Flow Ladder 6

5.4 Example of Out-of-Band SHAKEN HTTP POST 7

6 CPS Discovery 7

6.1 CPS Discovery by OCN 8

6.1.1 STI-PA 8

6.1.2 STI-CAs 9

6.2 CPS Discovery for Toll-Free Calls 9

6.3 CPS Discovery by Local Policy 9

7 Appendix A: Out-of-Band SHAKEN Call Scenarios 10

7.1 Direct TDM-TDM 10

7.2 Indirect TDM-Transit-TDM 10

7.3 Indirect TDM-Transit-SIP 10

7.4 Indirect SIP-Transit-TDM 11

7.5 Indirect SIP-Transit-SIP 11

8 Appendix B - SHAKEN Retargeting Call Scenarios 12

8.1 In-band Only 12

8.2 Out-of-band Only 12

8.3 Out-of-band and In-band 13

8.4 In-band and Out-of-band 13

9 Appendix C - Out-of-Band STIR Overview 13

# Scope, Purpose, & Application

## Scope

This specification extends the currently defined SHAKEN framework to enable an originating service provider (OSP) to send PASSporTs to the terminating service provider (TSP) out-of-band, that is, separate from the telephone network signaling. The mechanism described in this specification is based on the *STIR Out-of-Band Architecture and Use Cases* defined in [draft-ietf-stir-oob] and *Out-of-Band STIR for Service Providers* in [draft-peterson-stir-servprovider-oob].

## Purpose

The current SHAKEN framework provides a set of tools that enable verification of the calling party's authorization to use a calling telephone number for a call. The SHAKEN protocol specification [ATIS-1000074-E] describes an authentication mechanism that can be invoked by the OSP to "attest" to the legitimacy of the calling telephone number associated with a call. In this framework, the OSP’s STI-AS creates a PASSporT and inserts this PASSporT in the SIP Identity header per RFC 8224. The SIP INVITE is then routed over the network-to-network interface (NNI) through the standard inter-domain routing configuration.

In today’s PSTN, and for the foreseeable future, the Identity header may fail to arrive at the TSP’s network for verification by their STI-VS because the call is not transmitted using SIP end to end. Out-of-Band SHAKEN remedies this problem by sending the PASSporT to the TSP separately, out-of-band, through implementation of a Call Placement Service (CPS) described in this document. All other SHAKEN steps for authentication, use of Public Key Infrastructure (PKI), and verification remain the same.

# Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ATIS-0300251, *Codes for Identification of Service Providers for Information Exchange.*

ATIS-0417001-003, *Industry Guidelines For Toll Free Number Administration.*

ATIS-1000074-E, *Errata on ATIS Standard on Signature-based Handling of Asserted Information using Tokens (SHAKEN).*

ATIS-1000080.v002, *SHAKEN: Governance Model and Certificate Management.*

ATIS-1000084-E, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators.*

ATIS-1000085, *Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): SHAKEN Support of "div" PASSporT.*

IETF RFC 2616, *Hypertext Transfer Protocol -- HTTP/1.1.*1

IETF RFC 2914, *Congestion Control Principles.*1

IETF RFC 3261, *SIP: Session Initiation Protocol.*1

IETF RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks.*1

IETF RFC 3966, *The tel URI for Telephone Numbers.*1

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace.*1

IETF RFC 4949, *Internet Security Glossary, Version 2.*1

IETF RFC 5681, *TCP Congestion Control.*1

IETF RFC 6585, *Additional HTTP Status Codes.*1

IETF RFC 7044, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*.1

IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*1

IETF RFC 8225, *Personal Assertion Token.*[[1]](#footnote-2)

IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates.*1

draft-ietf-stir-oob-007, *STIR Out-of-Band Architecture and Use Cases.*1

draft-peterson-stir-servprovider-oob-00, *Out-of-Band STIR for Service Providers*.1

3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).*[[2]](#footnote-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> >.

## Definitions

The following provides some key definitions used in this document.

**(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]. See also STI Certificate.

**Call Placement Service (CPS):** A device that can receive a PASSporT from a call source, for retrieval by the call destination’s STI-VS. (draft-ietf-stir-oob-07)

**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 [RFC 4949].

**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 [RFC 4949].

**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 [RFC 4949].

**Certificate Signing Request (CSR):** A CSR is sent to a CA to request a certificate. A CSR contains a public key of the end-entity that is requesting the certificate.

**Carrier Identification Code (CIC):** A unique four-character alphanumeric code (XXXX) assigned to Service Providers.

**Chain of Trust:** Deprecated term referring to the chain of certificates to a trust anchor. Synonym for Certification Path or Certificate Chain [RFC 4949].

**Certificate Validation:** An act or process by which a certificate user established that the assertions made by a certificate can be trusted [RFC 4949].

**Company Code:** A unique four-character alphanumeric code (NXXX) assigned to all Service Providers [ATIS-0300251]. (see Operating Company Number)

**End-Entity:** An entity that participates in the Public Key Infrastructure (PKI). Usually a Server, Service, Router, or a Person. In the context of this document, an end-entity is a Service Provider, TN Service Provider, or VoIP Entity.

**Fingerprint:** A hash result ("key fingerprint") used to authenticate a public key or other data [RFC 4949].

**Identity:** Either a canonical Address-of-Record (AoR) SIP Uniform Resource Identifier (URI) employed to reach a user (such as ”sip:alice@atlanta.example.com”), or a telephone number, which commonly appears in either a TEL URI [RFC 3966] or as the user portion of a SIP URI. See also Caller ID [RFC 8224].

**Operating Company Number (OCN):** A unique four-character alphanumeric code (NXXX) assigned to all Service Providers [ATIS-0300251]. (see Company Code)

**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 [RFC 4949].

**Public Key:** The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography [RFC 4949].

**Public Key Infrastructure (PKI):** The set of hardware, software, personnel, policy, and procedures used by a CA to issue and manage certificates [RFC 4949].

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

**Secure Telephone Identity (STI) Certificate:** A public key certificate used by a service provider to sign and verify a PASSporT.

**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], 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 ensures the identity of the sender and the integrity of the data [RFC 4949].

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

**VoIP Entity:** A non-STI-authorized customer entity that purchases (or otherwise obtains) delegated telephone numbers from a TNSP

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| 3GPP | 3rd Generation Partnership Project |
| ATIS | Alliance for Telecommunications Industry Solutions |
| B2BUA | Back-to-Back User Agent |
| CIC | Carrier Identification Code |
| CPS | Call Placement Service |
| CRL | Certificate Revocation List |
| CSCF | Call Session Control Function |
| CVT | Call Validation Treatment |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| IBCF | Interconnection Border Control Function |
| IETF | Internet Engineering Task Force |
| IMS | IP Multimedia Subsystem |
| IP | Internet Protocol |
| JSON | JavaScript Object Notation |
| JWS | JSON Web Signature |
| NNI | Network-to-Network Interface |
| OCN | Operating Company Number |
| OCSP | Online Certificate Status Protocol |
| OSP | Originating Service Provider |
| PASSporT | Persona Assertion Token |
| PBX | Private Branch Exchange |
| PKI | Public Key Infrastructure |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| SKS | Secure Key Store |
| SP | Service Provider |
| SPID | Service Provider IDentifier |
| STI | Secure Telephone Identity |
| STI-AS | Secure Telephone Identity Authentication Service |
| STI-CA | Secure Telephone Identity Certification Authority |
| STI-CR | Secure Telephone Identity Certificate Repository |
| STI-VS | Secure Telephone Identity Verification Service |
| STIR | Secure Telephone Identity Revisited |
| TLS | Transport Layer Security |
| TN | Telephone Number |
| TNSP | TN Service Provider |
| TSP | Terminating Service Provider |
| UA | User Agent |
| URI | Uniform Resource Identifier |
| UUID | Universally Unique IDentifier |
| VoIP | Voice over Internet Protocol |

# Overview

## Problem Statement – Why Out-of-Band SHAKEN is needed

SHAKEN describes a framework for OSPs to create a SHAKEN PASSporT that can be carried by the SIP signaling protocol to cryptographically attest the identity of callers. The SHAKEN framework requires that the entire call path be SIP for the PASSporT to be delivered to the TSP.

Not all telephone calls use SIP signaling. Some calls use SIP for only part of their signaling path. The scale and scope of this problem is large. For example, the NTCA, a trade association representing nearly 850 rural local exchange carriers (RLECs), reports that 93% of its members have IP enabled switches. However, for most NTCA members, local SIP interconnect access to the Public Switched Telephone Network (PSTN) is not currently an economic option. Further, many urban CLECs receive inbound calls from the PSTN via the local tandem. For these urban CLECs, a SIP interconnect to the local tandem switch is not always an option. The reality is that the transition to all SIP interconnection is years away.

Although desirable, the underlying realities slow the transition of the PSTN from its current state to a future state where PASSporTs can be carried reliably end-to-end using SIP signaling. Meanwhile, requirements for call authentication are on a much faster pace. Legislation has been signed into law to require SHAKEN in VoIP networks and reasonable measures for call authentication in non-IP networks. Thus, there is a timing mismatch between the requirement for call authentication versus the readiness of the network to accommodate end-to-end SIP signaling. This mismatch will create a situation where some consumers get the benefits of call authentication while others cannot.

Out-of-Band SHAKEN addresses this mismatch. It provides another way to transmit PASSporTs within the SHAKEN framework. It works with today’s telephone network and provides a way to give more service providers access to SHAKEN so they can more quickly deliver the benefits of call authentication to their customers. In addition to SHAKEN PASSporTs, Out-of-Band SHAKEN can support other PASSporT types or extensions that are compatible with the currently defined SHAKEN framework.

Out-of-Band SHAKEN, as defined in this document, is implemented by OSPs and TSPs. There are no requirements for transit providers to enable Out-of-Band SHAKEN unless the transit provider is supporting SHAKEN call authentication services on behalf of an OSP. Service providers may choose to implement Out-of-Band SHAKEN for only authentication, only verification, or both authentication and verification.

Under current regulatory policy, network upgrades from the legacy TDM infrastructure to a SIP infrastructure are expected to only continue at a modest pace. Meanwhile, Out-of-Band SHAKEN provides a complementary approach to deliver the benefits of call authentication more broadly today.

# Out-of-Band SHAKEN

Out-of-Band SHAKEN, as defined in this document, is a specific use case of Out-of-Band STIR. With Out-of-Band SHAKEN, each service provider has its own CPS. Therefore, the CPS does not have a public interface to retrieve PASSporTs. This approach removes the privacy concerns of operating a single CPS and eliminates the need for PASSporT encryption. This approach also addresses the security issues associated with a public interface for retrieving PASSporTs. From a trust perspective, Out-of-Band SHAKEN is a “constrained intra-network deployment” since it should be limited to service providers that have been approved by the STI-PA.

Out-of-Band SHAKEN specifically addresses the call scenarios where both the OSP and TSP support SIP yet TDM is still used as part of the transit path for calls between the two service providers. See Section 7 (Appendix A) for diagrams of targeted scenarios. Out-of-Band SHAKEN also supports call retargeting by using the method described in ATIS-1000085, SHAKEN: SHAKEN Support of "div" PASSporT. See Section 8 (Appendix B) for diagrams that illustrate such support. As the SHAKEN architecture defined in ATIS 1000074-E is further extended, Out-of-Band SHAKEN is expected to extend with it (e.g., through support of other PASSporT types and multiple PASSporTs in a SIP INVITE).

Out-of-Band SHAKEN can be used with SHAKEN PASSporTs or any other PASSporT type or extension. Multiple PASSporTs for a single call can be sent to the CPS for use cases when multiple PASSporTs are in the SIP INVITE.

## Out-of-Band SHAKEN Architecture

The following diagram shows the SHAKEN architecture defined in ATIS 1000074-E with the addition of a CPS for Out-of-Band SHAKEN. The CPS deployed by Service Provider B has an interface to receive SHAKEN PASSporTs from Service Provider A via an HTTPS POST message as defined by the Out-of-Band STIR IETF draft (an example of which is provided later in Section 5.3).

A screenshot of a cell phone

Description automatically generated

Figure 1. Architecture with Out-of-Band SHAKEN CPS

The direct relationship between the CPS and the STI-VS is the key design difference between Out-of-Band STIR and Out-of-Band SHAKEN. This explicit trust relationship between the CPS and STI-VS enables TSPs to optimize the implementation of their CPS infrastructure.

## Out-of-Band SHAKEN Overview

The OSP STI-AS has a local mapping that provides the CPS URL for most call scenarios. Section 6 of this document details these scenarios. For call scenarios where the CPS URL cannot be determined, the HTTP POST to the CPS is not performed. The OSP STI-AS may need additional information (i.e., LNP routing number, CIC, etc.) to perform CPS discovery.

Before the PASSporT is persisted, the TSP’s CPS verifies it as described in ATIS 1000074-E (except for checking that the date, “orig” claim “tn” and “dest” claim “tn” values match the SIP INVITE) to confirm that the PASSporT was generated by an approved service provider within the SHAKEN ecosystem using a valid SHAKEN certificate.

The CPS should use local policy to determine which PASSporTs to discard if the CPS is nearing an overload condition. The CPS should use standard HTTP and TCP congestion control during high load conditions. PASSporTs received from the CPS are deleted when the call is received by the STI-VS or when the PASSporT becomes stale, whichever occurs first. If the STI-VS receives different PASSporTs in-band and out-of-band, local policy is used to determine which to use.

The interface for the STI-VS to retrieve a PASSporT from the CPS is private because the CPS is logically associated or combined with the STI-VS. The protocol for the STI-VS connection to the CPS is specifically not defined in this document because it is only used internally within a service provider’s network. The HTTP GET message, as defined in the Out-of-Band STIR IETF draft, may be used as a reference.

## Out-of-Band SHAKEN Call Flow Ladder

The following call flow is representative of the Out-of-Band SHAKEN use case. In this example, the PASSporT is sent both via in-band SIP signaling and out-of-band to the TSP.

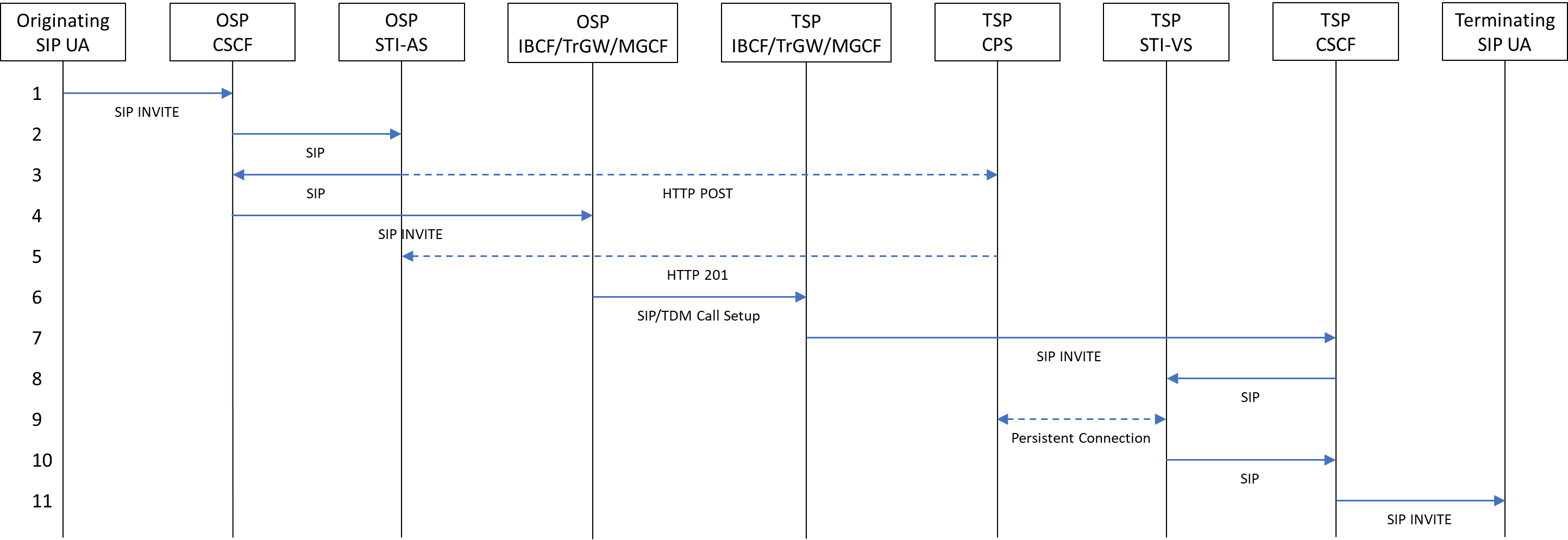


Figure 2. Out-of-Band SHAKEN Call Ladder

**Call Flow Details**

1. Originating SIP UA sends a SIP INVITE to OSP CSCF.
2. OSP CSCF sends a SIP message to request a PASSporT from OSP STI-AS.
3. OSP STI-AS simultaneously sends the PASSporT to TSP CPS and sends a SIP message containing the PASSporT to OSP CSCF.
4. OSP CSCF sends a SIP INVITE to OSP IBCF/TrGW/MGCF.
5. TSP CPS returns an HTTP 201 to OSP STI-AS. The timing of this response has no impact on call processing so it may occur earlier or later than described.
6. OSP IBCF/TrGW/MGCF sends a SIP/TDM Call Setup message to TSP IBCF/TrGW/MGCF.
7. TSP IBCF/TrGW/MGCF sends a SIP INVITE to TSP CSCF.
8. TSP CSCF sends a SIP message to request the verification result from TSP STI-VS.
9. Depending on the implementation chosen by the TSP, either the TSP CPS pushes the PASSporT to TSP STI-VS or TSP STI-VS requests the PASSporT from TSP CPS using the persistent connection.
10. TSP STI-VS sends a SIP message containing the verification result and any PASSporTs received out-of-band to the TSP CSCF.
11. TSP CSCF sends a SIP INVITE to Terminating SIP UA.

## Example of Out-of-Band SHAKEN HTTP POST

The following message is an example of an HTTP POST to a CPS:

POST /cps/company/1234 HTTP/1.1

Content-Type: application/passport

Content-Length: 487

Host: cps.transnexus.com

eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ0aWZpY2F0ZXMuY2xlYXJpcC5jb20vNGE4NzFjMDYtZTBiNS00Y2I5LTgzNDctNDMxMjZiZDg2Yzg1LzY0NmIxYmUzNzNmMTZlYWY4NzUzNzk5ZTM0OTkwMzJhLmNydCJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyIxOTAzMjQ2OTEwMyJdfSwiaWF0IjoxNTg0OTgzNDAyLCJvcmlnIjp7InRuIjoiMTIwMTM3NzYwNTEifSwib3JpZ2lkIjoiNGFlYzk0ZTItNTA4Yy00YzFjLTkwN2ItMzczN2JhYzBhODBlIn0.EMfXHyowsI5s73KqoBzJ9pzrrwGFNKBRmHcx-YZ3DjPgBe4Mvqq9N-bThN1\_HTWeSvbruAyet26fetRL1\_bn1g

The body contains the same PASSporT(s) transmitted in-band via the SIP signaling per established SHAKEN standards. Multiple PASSporTs can be included in the body separated by a newline for applicable use cases. The connection between the STI-AS and CPS must be secured using HTTPS.

# CPS Discovery

Out-of-Band SHAKEN defines a model with one CPS per TSP. The STI-AS of the OSP must be able to discover the publicly accessible URL of the TSP’s CPS. CPS discovery by Operating Company Number (OCN) and Carrier Identification Code (CIC) cover the most common use cases. OSP local policy can be used for most other use cases.

## CPS Discovery by OCN

CPS discovery by OCN uses a mapping of the called party digits to a portability corrected OCN which is then used to identify the URL of the TSP’s CPS. The mapping of TSP OCNs to CPS URLs must be handled in a trusted and authoritative fashion. Multiple implementation models are possible to achieve this trusted CPS discovery service. The STI-PA is a logical party to fulfill this role with minimal incremental effort. The STI-CAs are also logical parties to fulfill this role with minimal incremental effort.

### STI-PA

The following diagram, recreated from ATIS 1000084-E, summarizes the roles and responsibilities associated with the STI-PA, including the interfaces to other functional elements. This version of the diagram, however, includes the additional function of providing accurate CPS discovery. The two additions to the diagram are noted in bold text:

1. **CPS URL** provisioned by the service provider, and
2. **Mapping of OCNs to CPS URLs** published by the STI-PA.

A close up of a device

Description automatically generated

Figure 3. CPS Discovery by OCN through the STI-PA

The CPS URL mapping is published via an API in the same way that the STI-PA publishes the list of approved STI-Certification Authorities (STI-CAs). The STI-PA generates a JSON Web Token (JWT) containing the CPS mapping data. This token is then signed using the STI-PA’s private key. A sample JWT header and body are below:

Header:

{

"alg": "ES256",

"typ": "JWT",

"x5u": "https://sti-pa.com/download/v1/certificate/certificateId\_1.crt"

}

Payload:

{

"version": "1.0",

"sequence": 1,

"exp": 1590000000,

"cpsMapping": {

"1234": "https://example.com/cps/company/1234",

"5678": "https://example.com/cps/company/5678"

}

}

### STI-CAs

Service providers supply their CPS URL to their chosen STI-CA. The STI-CA generates a JSON Web Token (JWT) containing the CPS mapping data. This token is then signed using a private key that chains up to the STI-CA’s root key. A sample JWT header and body are below:

Header:

{

"alg": "ES256",

"typ": "JWT",

"x5u": "https://sti-ca.com/download/v1/certificate/certificateId\_1.crt"

}

Payload:

{

"version": "1.0",

"sequence": 1,

"exp": 1590000000,

"cpsMapping": {

"1234": "https://example.com/cps/company/1234",

"5678": "https://example.com/cps/company/5678"

}

}

This JWT is publicly accessible and is secured with HTTPS.

Routinely, each service provider requests these JWTs from each STI-CA.

STI-CAs may choose to create a master file that contains the JWTs from all STI-CAs, including their own. Service providers can then just request this one master file from their STI-CA.

Regardless of how the JWTs are delivered to the service provider, the service provider verifies that the JWT was signed by a certificate that chains up to a certificate in the STI-CA root list. The JWT gives accountability for who vouches for each CPS mapping.

## CPS Discovery for Toll-Free Calls

When toll-free calls are routed by CIC, CPS discovery by CIC is required. The mapping of TSP CICs to CPS URL must be handled in a trusted and authoritative fashion. Multiple implementation models are possible to achieve this trusted CPS discovery service. The toll-free number administrator, for example, is a logical party to fulfill this role with minimal incremental effort.

## CPS Discovery by Local Policy

When CPS discovery is not possible though external sources, OSPs can use local policy to determine the correct CPS URL. For example, if an OSP relies on a single transit provider for all toll-free termination, the OSP may use local policy to direct PASSporTs for all toll-free calls to the transit provider. The transit provider can then use CPS Discovery for Toll-Free by CIC as described above for sending the PASSporT to the TSP.

# Appendix A: Out-of-Band SHAKEN Call Scenarios

Figure 1 describes a general Out-of-Band SHAKEN call scenario. This appendix provides more diagrams of the targeted call scenarios generalized by Figure 1.

Out-of-Band SHAKEN is not dependent on the number of transit providers between the OSP and TSP nor the signaling medium used by the transit providers. So, the entire transit path (whether SIP, TDM, or a combination of the two) is encompassed in a single “Transit” box in the diagrams below.

## Direct TDM-TDM

The OSP and TSP use TDM to directly interconnect.

A screenshot of a cell phone

Description automatically generated

Figure 4. Out-of-Band SHAKEN Call Scenario – Direct TDM-TDM

## Indirect TDM-Transit-TDM

The OSP uses TDM to interconnect with the transit provider and the TSP uses TDM to interconnect with the transit provider.

A screenshot of a cell phone

Description automatically generated

Figure 5. Out-of-Band SHAKEN Call Scenario – Indirect TDM-Transit-TDM

## Indirect TDM-Transit-SIP

The OSP uses TDM to interconnect with the transit provider and the TSP uses SIP to interconnect with the transit provider.

A screenshot of a cell phone

Description automatically generated

Figure 6. Out-of-Band SHAKEN Call Scenario – Indirect TDM-Transit-SIP

## Indirect SIP-Transit-TDM

The OSP uses SIP to interconnect with the transit provider and the TSP uses TDM to interconnect with the transit provider.

A screenshot of a cell phone

Description automatically generated

Figure 7. Out-of-Band SHAKEN Call Scenario – Indirect SIP-Transit-TDM

## Indirect SIP-Transit-SIP

The OSP uses SIP to interconnect with the transit provider, the TSP uses SIP to interconnect with the transit provider, and TDM is used in the transit path.

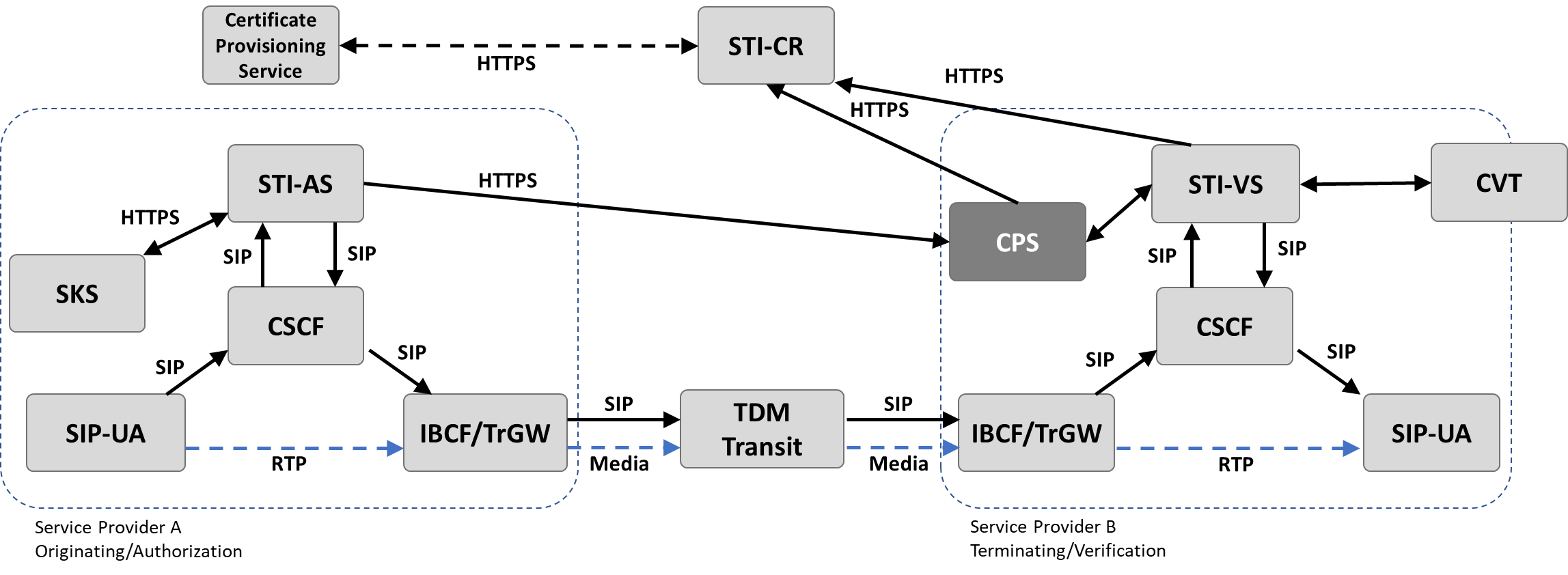


Figure 8. Out-of-Band SHAKEN Call Scenario – Indirect SIP-Transit-SIP

# Appendix B - SHAKEN Retargeting Call Scenarios

This appendix provides diagrams of retargeting call scenarios. Examples of retargeting include call forwarding and toll-free. The scenarios below cover only a single use case of call retargeting, but multiple cases are supported. A generated PASSporT can be transmitted in-band or out-of-band each time a call is retargeted.

The SHAKEN call retargeting logic is described in ATIS-1000085. The logic is independent of whether the PASSporT is sent in-band or out-of-band.

## In-band Only

The OSP and retargeting provider use in-band SHAKEN. The retargeting provider and TSP use in-band SHAKEN.

A screenshot of a cell phone

Description automatically generated

Figure 9. SHAKEN Retargeting Call Scenario – In-band Only

## Out-of-band Only

The OSP and retargeting provider use Out-of-Band SHAKEN. The retargeting provider and TSP use Out-of-Band SHAKEN.

A screen shot of a social media post

Description automatically generated

Figure 10. SHAKEN Retargeting Call Scenario – Out-of-band Only

## Out-of-band and In-band

The OSP and retargeting provider use Out-of-Band SHAKEN. The retargeting provider and TSP use in-band SHAKEN.

A screen shot of a social media post

Description automatically generated

Figure 11. SHAKEN Retargeting Call Scenario – Out-of-band and In-band

## In-band and Out-of-band

The OSP and retargeting provider use in-band SHAKEN. The retargeting provider and TSP use Out-of-Band SHAKEN.

A screen shot of a social media post

Description automatically generated

Figure 12. SHAKEN Retargeting Call Scenario – In-band and Out-of-band

# Appendix C - Out-of-Band STIR Overview

Out-of-band STIR is described in an IETF draft, *STIR Out-of-Band Architecture and Use Cases*. It describes a method of sending PASSporTs to a CPS, which is a place to send, temporarily store, and retrieve PASSporTs, as follows:

1. The OSP creates a PASSporT using the standard STI-AS function and STIR PKI.
2. The OSP encrypts the PASSporT using the public key of the TSP and sends it to the CPS.
3. When the TSP receives a call, the TSP retrieves any PASSporTs for the call from the CPS.
4. The TSP’s private key is used to decrypt the PASSporTs.
5. The normal STI-VS function proceeds using the PASSporT(s) received from the CPS.

The following diagram presents the SHAKEN architecture, as defined in ATIS 1000074-E, with the addition of an Out-of-Band STIR CPS.

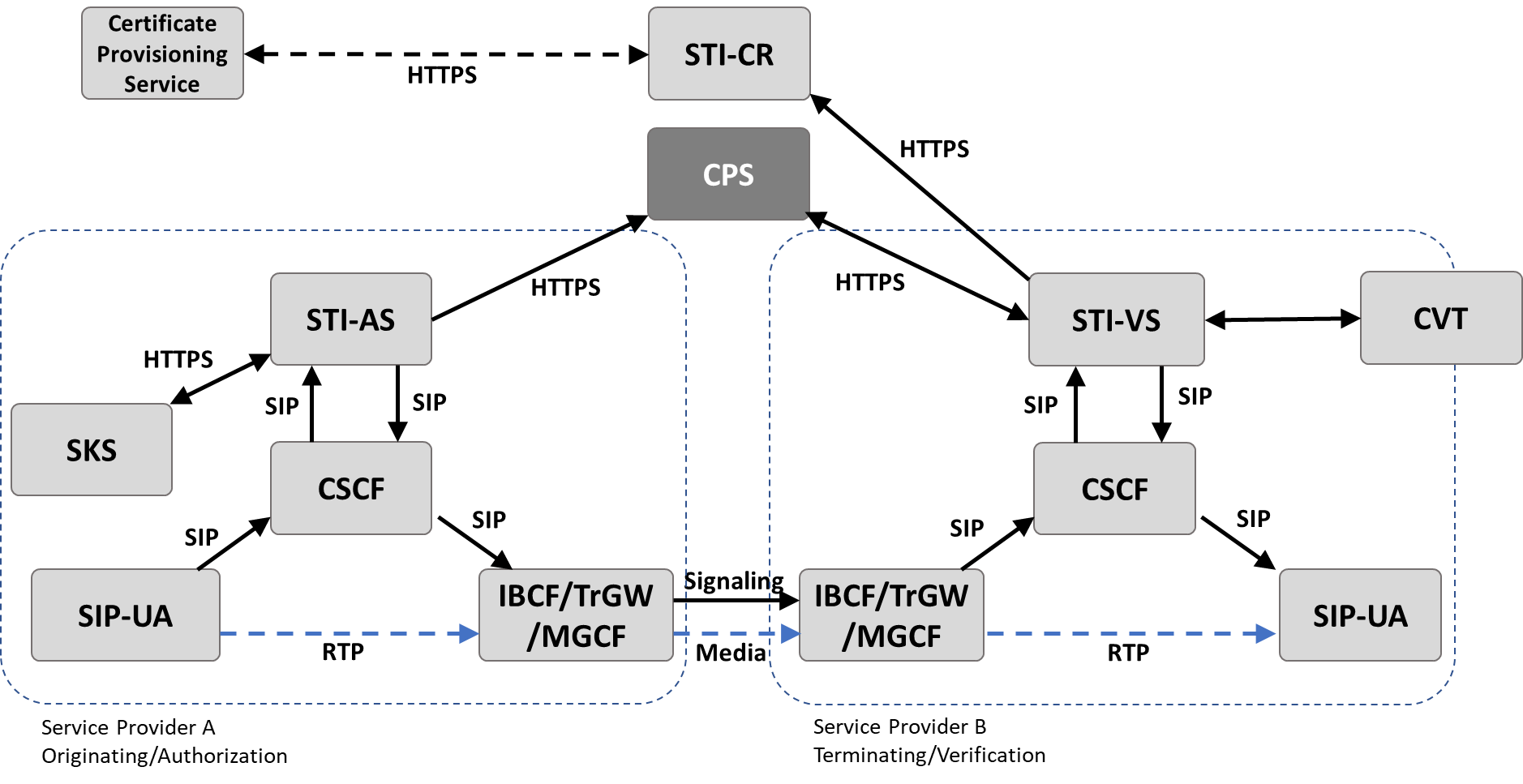


Figure 13. SHAKEN Architecture with Out-of-Band STIR

In the above referenced IETF draft, the CPS has a public interface for sending and receiving PASSporTs. Anyone can send PASSporTs to the CPS using an HTTP POST, and anyone can retrieve PASSporTs from the CPS using an HTTP GET. This is why the OSP encrypts the PASSporT using the TSP’s public key. The TSP then uses their private key to decrypt the PASSporT. Therefore, only the TSP can read the PASSporTs.

1. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-2)
2. Available from 3rd Generation Partnership Project (3GPP) at: < [https://www.3gpp.org](http://www.3gpp.org) > [↑](#footnote-ref-3)