ATIS-1000097.v002

Alternatives for Call Authentication for Non-IP Traffic

TECHNICAL REPORT

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.

ATIS-1000097.v002, *Alternatives for Call Authentication for Non-IP Traffic*

Published by

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

ATIS-1000097.v002

ATIS Technical Report on

Alternatives for Call Authentication for Non-IP Traffic

Alliance for Telecommunications Industry Solutions

Approved September 2, 2022

Abstract

The SHAKEN framework enables a SHAKEN-authorized 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 SIP signaling. This Technical Report considers scenarios where SIP connectivity is not available end-to-end (i.e., "non-IP" scenarios) and identifies and assesses potential approaches to determine and convey that the calling user is authorized to use the calling telephone number.

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 technical report, 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 Technical Report on –

Alternatives for Call Authentication for Non-IP Traffic

1 Scope, Purpose, & Application

1.1 Scope

ATIS-1000074, *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)*, defines a call authentication approach for Session Initiation Protocol (SIP) traffic but does not address non-Internet Protocol (IP) traffic. This Technical Report is limited to call authentication approaches that have been proposed for non-IP scenarios.

1.2 Purpose

The current SHAKEN framework provides a set of tools that enable verification of the calling party's authorization to use a calling telephone number for a call. The SHAKEN protocol specification [Ref 1] describes an authentication approach that can be invoked by the Originating Service Provider (OSP) to authenticate itself 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 call markings.

In the SHAKEN framework, the OSP's Secure Telephone Identity Authentication Service (STI-AS) creates a Personal ASSertion Token (PASSporT) and inserts this PASSporT in the 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.

SHAKEN requires that the call have SIP end-to-end, but this is not always the case in today's Public Switched Telephone Network (PSTN). For the purposes of this Technical Report, any scenario that does not have SIP end-to-end is considered a "non-IP" scenario.

This Technical Report identifies non-IP call authentication scenarios and provides a framework to evaluate potential approaches that could provide call authentication even when the call is not SIP end-to-end.

2 References

The following standards contain provisions which, through reference in this text, constitute provisions of this Technical Report. 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-1000074, *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN).*[1]

[Ref 2] ATIS-1000095, *Extending STIR/SHAKEN over TDM.*[1]

[Ref 3] ATIS-1000096, *Out-of-Band PASSporT Transmission Involving TDM Networks.*[1]

[Ref 4] ATIS-1000098, *Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling*.[1]

[Ref 5] This item intentionally left blank.

[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 4949, *Internet Security Glossary, Version 2.*[2]

[Ref 9] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*[2]

[Ref 10] IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates.*[2]

[Ref 11] ITU Q.763 (12/1999), *Signalling System No. 7 – ISDN user part formats and codes.*[3]

2.2 Informative References

[Ref 101] IETF RFC 8225, *PASSporT: Personal Assertion Token*.[2]

[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.

(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.

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, Telephone Number (TN) Service Provider, or Voice over Internet Protocol (VoIP) Entity.

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. For example, a Service Provider Code in an STI certificate is an identity for an OSP in 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 8].

Public Key: The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography [Ref 8].

Public Key Infrastructure (PKI): The set of hardware, software, personnel, policy, and procedures used by a Certification Authority (CA) to issue and manage certificates [Ref 8].

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.

---

[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/ >.

Secure Telephone Identity (STI) Certificate: A public key certificate needed by a service provider to sign or verify a PASSporT [RFC 8226, *Secure Telephone Identity Credentials: Certificates*].

Secure Telephone Identity InterWorking Function (STI-IWF): A logical function that can interwork between TDM signaling and SIP signaling, in either direction, and invoke the Secure Telephone Identity Out-of-Band Service (STI-OOBS), STI-AS, and Secure Telephone Identity Verification Service (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.

Signature: Created by signing the message using the private key. It ensures the identity of the sender and the integrity of the data [Ref 8].

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 Uniform Resource Identifier [URI] or a TEL URI) from which a telephone number can be derived.

3.2 Acronyms & Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
CA	Certification Authority
CDR	Call Detail Record
CNAM	Calling Name
CPS	Call Placement Service
CRL	Certificate Revocation List
CVT	Call Validation Treatment
GW	Gateway
HTTP	Hypertext Transfer Protocol
IAM	Initial Address Message
IBCF	Interconnection Border Control Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IN	Intelligent Network
IP	Internet Protocol
ISUP	Integrated Services Digital Network User Part
MFA	Multi-Factor Authentication
MGCF	Media Gateway Control Function
NNI	Network-to-Network Interface
OSP	Originating Service Provider
PASSporT	Personal ASSertion Token
PKI	Public Key Infrastructure
PRI	Primary Rate Interface

PSTN	Public Switched Telephone Network
RPH	Resource-Priority Header
SBC	Session Border Controller
SCP	Service Control Point
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SP	Service Provider
SSP	Service Switching Point
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-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
STP	Signal Transfer Point
TDM	Time Division Multiplexing
TN	Telephone Number
TrGW	Transition GateWay
TSP	Terminating Service Provider
URI	Uniform Resource Identifier
UUI	User-to-User Information
VoIP	Voice over Internet Protocol

4 Overview

4.1 Problem Statement

STIR/SHAKEN describes a framework for the OSP to create a “shaken” PASSporT that cryptographically protects the SIP call parameters and an “attestation” value, which is an assertion as to whether or not the OSP has ascertained the identity of an originating customer and determined the customer’s legitimate right to use the telephone number (caller ID). This PASSporT can be carried by the SIP signaling protocol and then cryptographically verified by the Terminating Service Provider (TSP) to provide information about the source and legitimacy of the caller ID.

Not all telephone networks use SIP, and even when the OSP and TSP use SIP, not every call will have SIP signaling end-to-end. Some calls use SIP for only part of their signaling path, and some calls that originate and terminate as SIP may have non-IP signaling for part of the path.

Meanwhile, requirements for call authentication are moving at a fast pace. Legislation has been signed into law to require STIR/SHAKEN in Voice over Internet Protocol (VoIP) networks and reasonable measures for call authentication in non-IP networks.

STIR/SHAKEN is based on a well-defined scenario – SIP end-to-end – and there is broad industry consensus on the path forward. Evaluating non-IP scenarios is not as simple, since there are many different things that could disrupt the end-to-end SIP path. The OSP could have a Time Division Multiplexing (TDM) network, the TSP could have a TDM network, or one or more TDM transport links could be used to interconnect a SIP-based OSP and TSP. Each of these scenarios could have a different architecture and set of requirements. Therefore, it is important to consider each scenario separately to determine if/how practical call authentication can be provided in a way that complements STIR/SHAKEN.

4.2 Objective

The objective of this Technical Report is to do the following:

- Provide architectural descriptions of typical non-IP scenarios.
- Identify approaches that could potentially provide call authentication for these non-IP scenarios.
- Propose a framework for evaluating non-IP call authentication approaches.

4.3 Evaluation of Non-IP Call Authentication Approaches

The following factors should be considered when evaluating non-IP call authentication approaches:

- **Scope**: The degree of support for “call authentication” for TDM service providers, including the level of call authentication provided (i.e., is it comparable to STIR/SHAKEN) as well as the coverage it can provide (i.e., what portion of calls and lines are covered).
- **Non-IP** call flows, including:
    - TDM → TDM
    - SIP → TDM
    - TDM → SIP
    - SIP → TDM → SIP
    - TDM → SIP → TDM
- **TDM network impact**: Are changes required to existing TDM interfaces, functions, or standards?
- **Co-existence**: Can the approach co-exist with other non-IP call authentication approaches?
- **Network topology**: Is a priori network topology knowledge required to support the approach? If a priori knowledge is required, identify where it is required, and how it is obtained. Examples of network knowledge that might be required include:
    - Terminating service provider identity, needed by the originating service provider before beginning to route the call.
    - Identity of specific intermediate network elements, either existing elements or new elements.

- **Use cases**: Identify the level of support for various call scenarios and services, and how this support is provided. Potential use cases to consider include:
    - Call forwarding in non-SIP domains
    - SIP forking
    - Call forking (application level) in SIP/non-SIP domains
    - Crankback in SIP/non-SIP domains
- **Security considerations**: Security approaches and vulnerabilities.
- **Transition to IP**: What is the impact on the transition to all-IP (e.g., does the approach lead to "stranded" functionality or disincentives for completing the transition to IP)?
- **SHAKEN compatibility**: Does the approach complement SHAKEN, rather than duplicate or compete? This would include things like:
    - Does it use a standard "shaken" PASSporT?
    - Can the approach interwork with SHAKEN?
    - What is the impact on existing SIP networks that have deployed SHAKEN? Ideally any approach would be transparent to SIP networks that have implemented SHAKEN and would not require additional functionality in SIP networks to accommodate non-IP call authentication.
    - What PASSporT types and extensions are supported? (e.g., Resource-Priority Header [RPH] support)
    - Can it support future extensions?
- **International**: How will the approach be extended to support full international deployment?
- **Dependencies**: Are there any dependencies other than those already identified (e.g., changes to existing standards, interfaces, processes or policies)?

5 Non-IP Call Path Scenarios

This Technical Report identifies call path scenarios that do not have end-to-end SIP connectivity.

5.1 TDM → SIP

This section illustrates scenarios where the OSP is TDM-based, and the TSP is SIP-based. The call originates in a TDM network and is converted to SIP at a "TDM/SIP GW" function, with SIP signaling to the TSP.

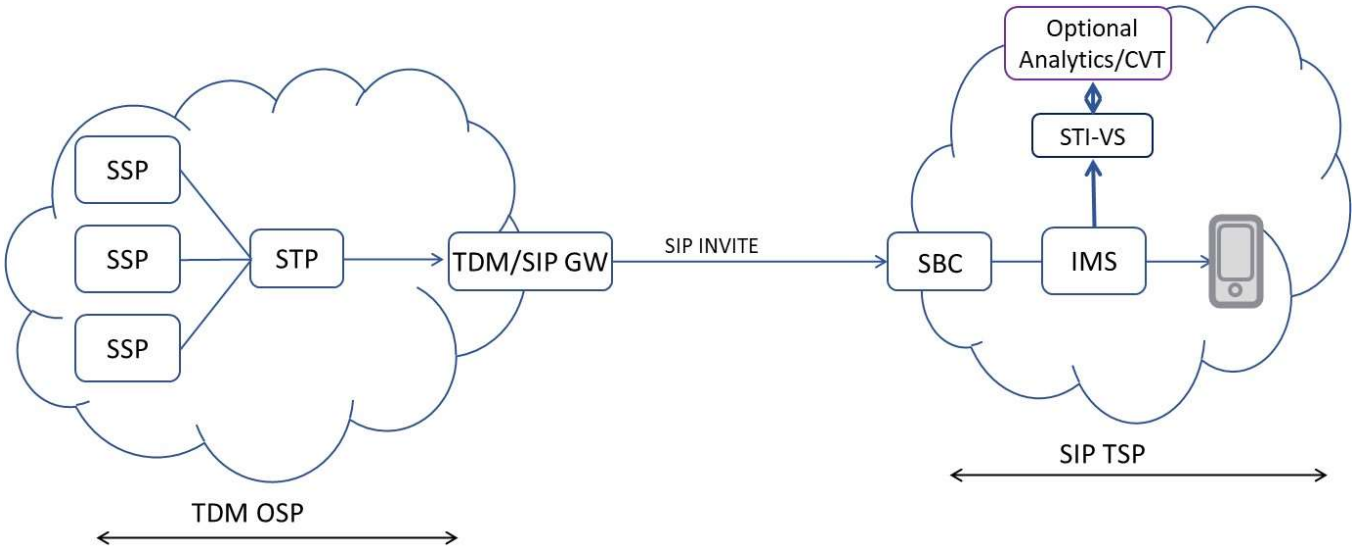

Figure 5-1: TDM → SIP call

5.2 SIP → TDM

This section illustrates scenarios where the OSP is SIP-based, and the TSP is TDM-based. In the first diagram (Figure 5-2) the SIP/TDM GW is located at the TSP, while in the second diagram (Figure 5-3) the SIP-to-TDM conversion is performed by the transit provider. This scenario can have different implications since the entity doing the conversion may not have a direct relationship with either the originating or terminating service provider.

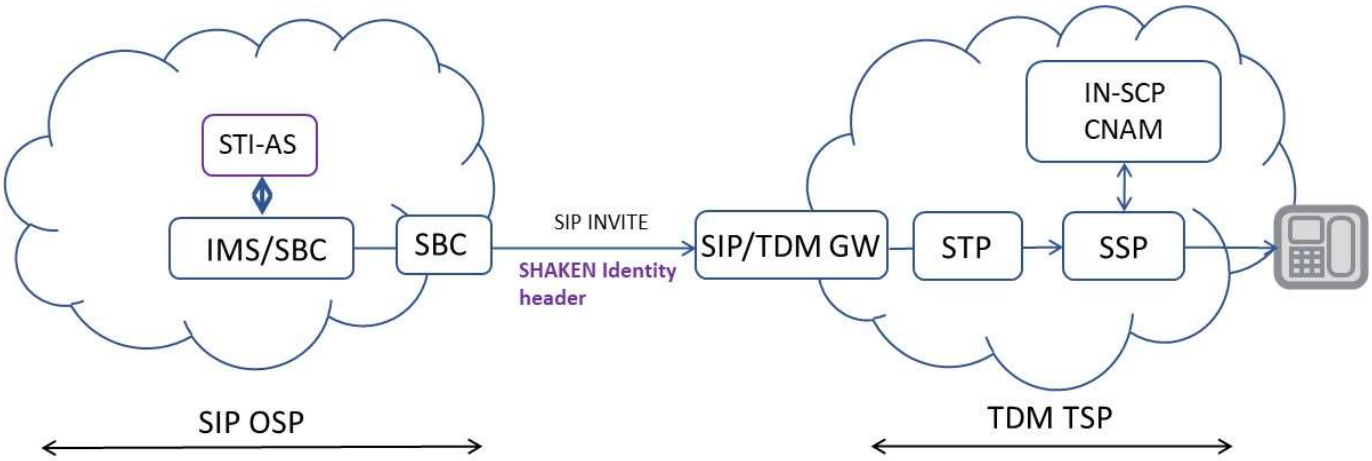

Figure 5-2: SIP → TDM

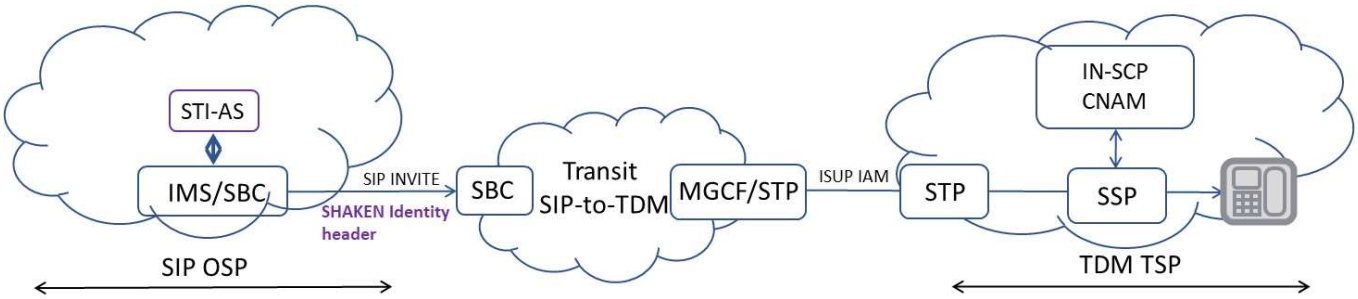

Figure 5-3: SIP → TDM With Conversion in the Transit Network

5.3 SIP → TDM → SIP

This section illustrates scenarios where the OSP and TSP are both SIP-based but one or more transit links are TDM-based. For analysis, this is divided into two sub-sections.

5.3.1 SIP → TDM Transport

This section illustrates scenarios where the OSP is SIP-based, and the transport network to one or more transit network peers is TDM-based.

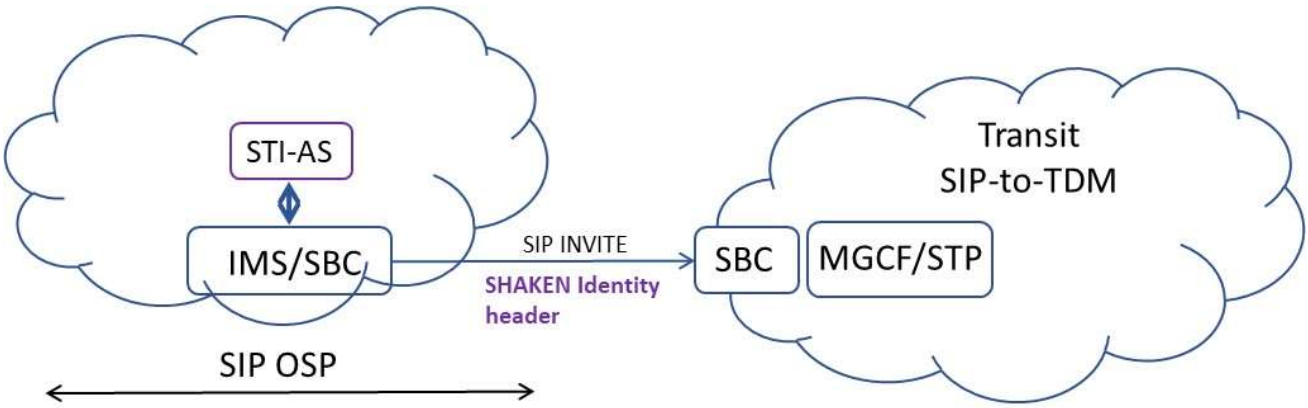

Figure 5-4: SIP → TDM Transit Network

5.3.2 TDM Transport → SIP

This section illustrates scenarios where the transport network from one or more upstream transit peers is TDM-based, and the TSP is SIP-based.

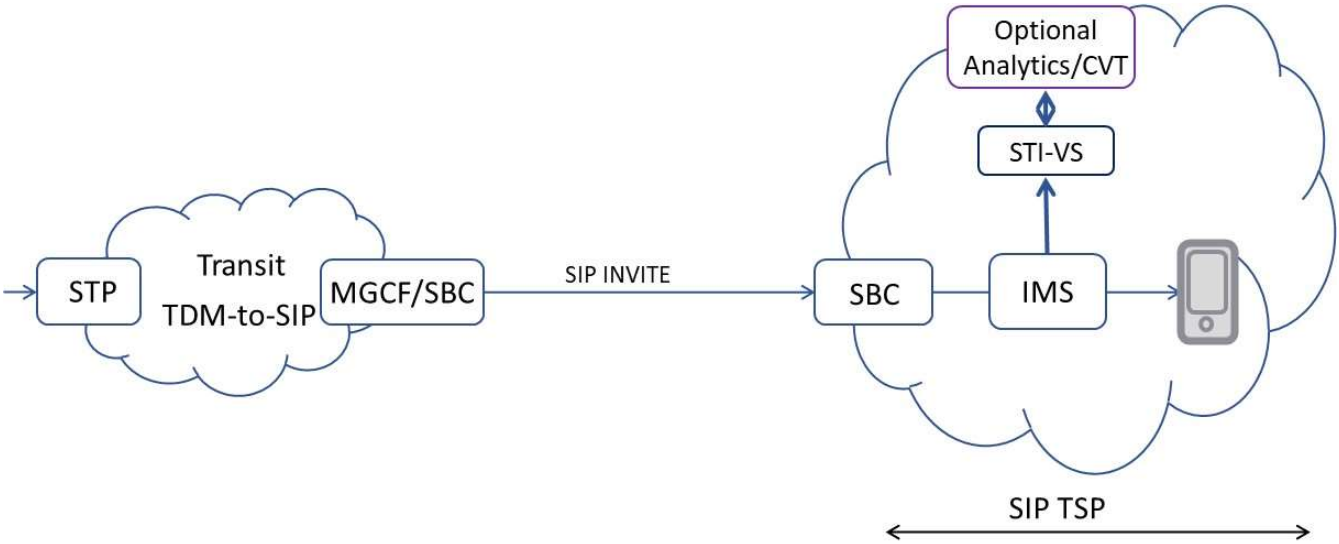

Figure 5-5: TDM → SIP

5.4 TDM-to-TDM

This section illustrates scenarios where the call is TDM end-to-end, including originating SP, terminating SP, transit links from both OSP and TSP, and any links within the transit network.

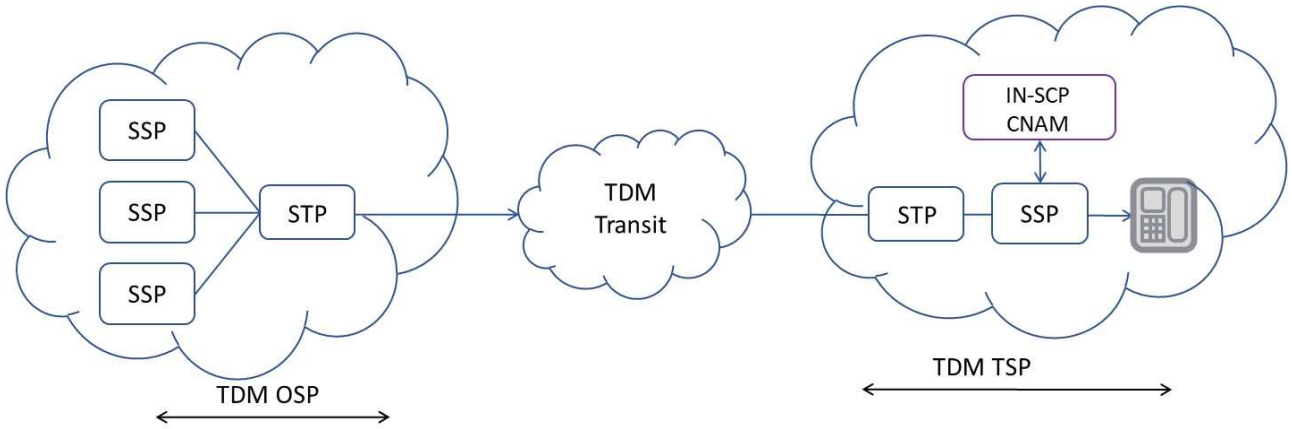

Figure 5-6: TDM → TDM

5.5 TDM-to-IP-to-TDM

This section illustrates scenarios where the originating and terminating SPs are TDM and the transport from the OSP and TSP to the transit network is TDM, but the transit links within the transit network are IP-based.

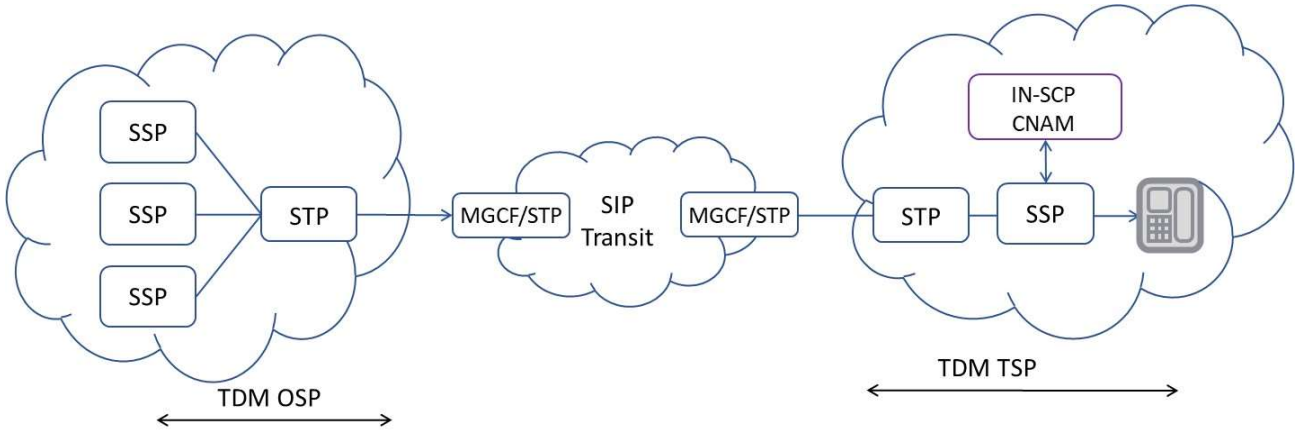

Figure 5-7: TDM → TDM with SIP Transit Network

6 Assessment

This Technical Report identifies non-IP call scenarios where standard SHAKEN cannot provide call authentication because the call path is not end-to-end IP. In some of the scenarios the origination and termination networks are SIP-based, but other portions of the call path are TDM-based. In other scenarios, the origination and/or termination networks are TDM-based. The Annex of this Technical Report assesses the ability of the two proposed non-IP call authentication approaches to provide call authentication for all identified scenarios. Note that this assessment does not attempt to identify a "preferred" approach for non-IP call authentication. However, Annex A identifies the key attributes of each approach, based on the factors identified in Clause 4.3 to provide a better understanding of each scenario.

Both approaches described in Annex A can be utilized in the call path of a single call.

The two approaches may be used independently by different service providers in the call path, as shown in Figure 6-1.

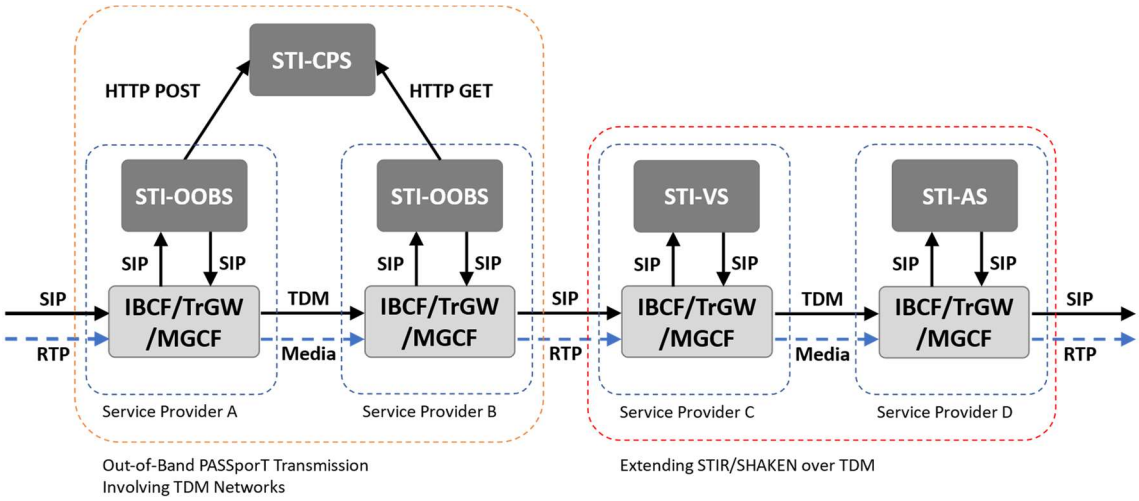

Figure 6-1: Independent Usage of Approaches

The two approaches may also be used by the same service provider, as shown in Figure 6-2. The boundary point (the point where one approach is used at ingress and the other approach is used at egress) is treated the same way that a SIP-TDM or TDM-SIP boundary point is treated. Two service providers with a TDM interconnect between each other would need to agree on one of the approaches for transmitting attestation levels over the TDM interconnect.

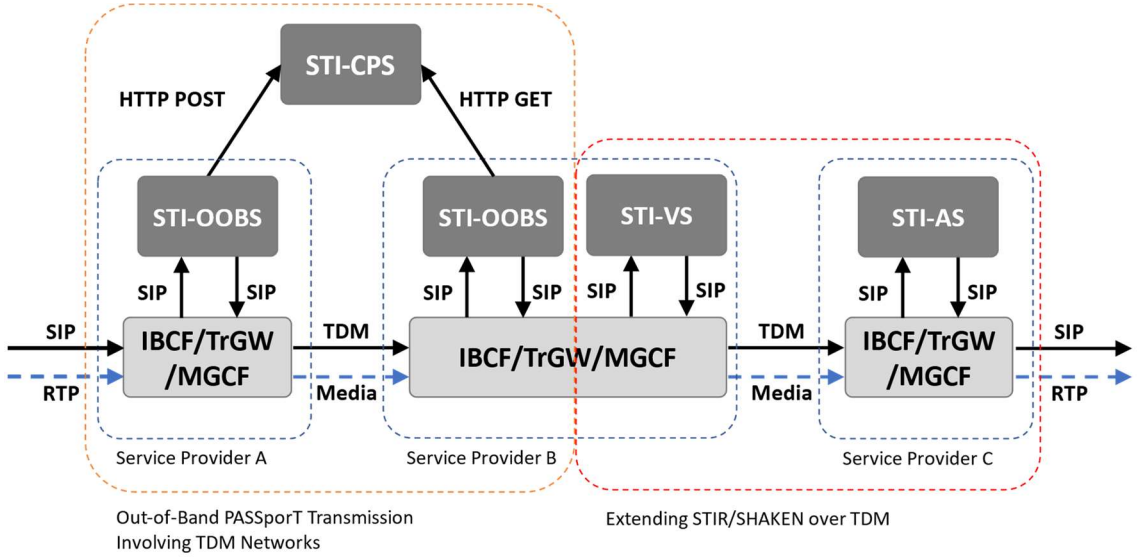

Figure 6-2: Boundary Point Usage of Approaches

The two approaches may be used simultaneously by service providers in the call path. In the example shown in Figure 6-3, Service Provider A generates a “shaken” PASSporT and then both publishes the “shaken” PASSporT to the STI-CPS, as specified in ATIS-1000096 [Ref 3], and populates the Integrated Services Digital Network User Part (ISUP) User-to-User Information (UUI) parameter with the encoded PASSporT, as specified in ATIS-1000095 [Ref 2]. Service Provider C verifies the PASSporT in the ISUP UUI if one is received, otherwise it verifies the PASSporT retrieved from the STI-CPS. The design illustrated in Figure 6-3 removes the need for bilateral agreements. However, bilateral agreements would still be required if the Screening Indicator mapping is to be supported as a “fallback” to the UUI-based mechanism. It also allows Service Provider A to ensure that calls it originates will be verified regardless of which approach Service Provider C implemented. Additionally, it ensures

Service Provider C will be able to verify calls it terminates regardless of which approach Service Provider A implemented.

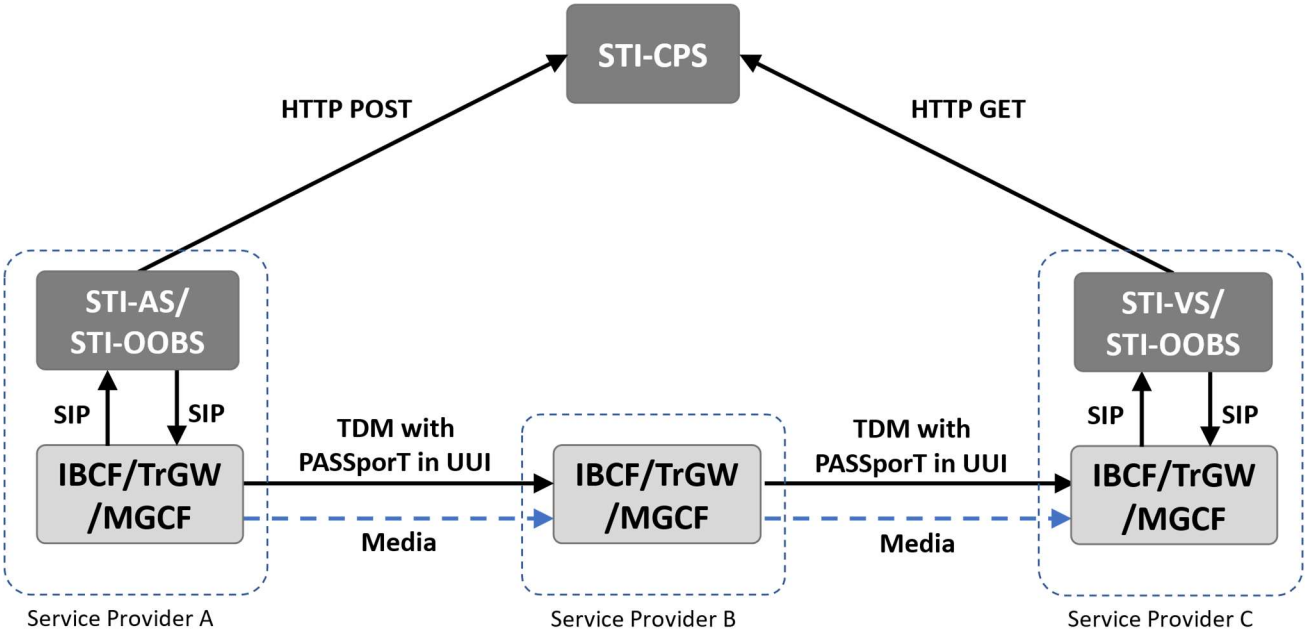

Figure 6-3: Simultaneous Usage of Approaches

Annex A: Non-IP Call Authentication Approaches (Informative)

A.1 Out-of-Band PASSporT Transmission Involving TDM Networks

ATIS-1000096, *Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks*, extends the currently defined SHAKEN framework to enable the transmission of PASSporTs for calls that use TDM signaling and/or TDM switches during origination, termination, and/or transit. The specification adheres to the following core principles:

1. The solution does not place any new requirements on SHAKEN-compliant VoIP service providers with only SIP-based interconnects.
2. 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.

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 providers to publish and retrieve PASSporT(s).

If a call originated by a VoIP service provider is delivered to an interconnected network using TDM signaling or if a call is originated by a TDM service provider using a TDM switch, then the OSP generates the applicable PASSporT(s) and then publishes the PASSporT(s) to an STI-CPS. If a call is converted from SIP to TDM at an intermediate point along the signaling path, the service provider that converts a call from SIP signaling to TDM signaling publishes all PASSporT(s) received in the SIP signaling, as defined in RFC 3261, *SIP: Session Initiation Protocol*, (e.g., SIP INVITE), to an STI-CPS. If a call is converted from SIP signaling to TDM signaling multiple times, then the PASSporT(s) will be published to an STI-CPS each time the signaling is converted from SIP to TDM.

The service provider that converts a call from TDM signaling to SIP signaling retrieves all PASSporT(s) associated with the call from an STI-CPS and inserts the retrieved PASSporT(s) into the SIP signaling. If a call is received at a TSP network via a TDM NNI, whether the terminating network uses VoIP or TDM technology to reach the terminating customer, then the TSP retrieves all PASSporT(s) associated with the call from an STI-CPS. If a 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 approach has the following characteristics:

- **Scope**: Fully supports multiple PASSporTs and any PASSporT extension, including but not limited to “shaken”, “div”, “rcd”, and “rph” PASSporTs. PASSporT(s) may not be retrievable if the call uses an origination or destination Uniform Resource Identifier (URI), and this URI cannot be determined after the conversion from SIP to TDM and then back to SIP. No changes to the standard or functional elements are expected when future PASSporT extensions are defined.
- **Non-IP calls**: All non-IP call scenarios are supported.
- **Network impact**: Additional functionality is required in TDM networks at the network level and at the end office level. Specifically, TDM networks may need the same functional elements that IP networks need (STI-AS, STI-VS, etc.) and a Secure Telephone Identity Out-of-Band Service (STI-OOBS). Depending on the capabilities of the TDM equipment, a Secure Telephone Identity InterWorking Function (STI-IWF) may also be required. For calls originated in TDM networks, new functionality is required to be implemented at the end office to determine the appropriate level of attestation for a call and to use this information to generate a PASSporT and publish it to the STI-CPS. There is no network impact on SHAKEN-compliant SIP networks that do not use TDM interconnects. In addition, this approach requires an STI-CPS mesh across all participating service providers with each having access to at least one STI-CPS. A governance structure is also required to support STI-CPS discovery and to issue STI certificates to the STI-CPS, but ATIS-1000096 [Ref 3] does not specify the governance structure nor the STI-CPS discovery mechanism.
- **Network topology**: No a priori network topology knowledge is required.
- **Use cases**: Supports call forwarding, call forking, and crankback. If a TDM entity performs any operation that requires a new PASSporT to be generated, then the service provider performing this operation may

need to retrieve any existing PASSporT(s) for the call from an STI-CPS (if the PASSporT(s) have not already been retrieved), generate a new PASSporT, and publish all of the PASSporT(s) to an STI-CPS.

- **Security considerations**: Leverages the extensive security analysis performed in the IETF [Ref 5]. Drastically simplifies the security requirements by limiting access to only Secure Telephone Identity Policy Administrator (STI-PA)-approved service providers. PASSporTs (as defined in RFC 8225 [Ref 101]) have minimal replay attack prevention. The combination of calling number, called number, and approximate timestamp are all that bind a PASSporT to a call. An attacker with timely access to a PASSporT can perform a replay attack. Note that the attacker must use the same calling number and called number as the original call for the replay attack to result in a successful verification. Out-of-Band SHAKEN (as defined in ATIS-1000096 [Ref 3]) potentially offers an additional attack surface that can be used to perform replay attacks. With Out-of-Band SHAKEN, an attacker may not need timely access to the PASSporT if certain conditions are met. The attacker must still have timely knowledge of a call occurring from a given calling number to a given called number or have a method of triggering a call from a given calling number to a given called number (e.g., triggering a Multi-Factor Authentication (MFA) phone call after compromising a password). The attacker must be able to originate a call with the given calling number (meaning the attacker's originating service provider must not prevent the attacker from spoofing a calling number). The original call must use TDM and the service provider who converts the call from SIP to TDM (or the originating service provider if the call originates TDM) must publish the PASSporT to the STI-CPS (note that the attacker does not control this behavior nor have any way of knowing it is occurring). The attacker's call must also use TDM, but in this case the service provider who converts the call from SIP to TDM (or the originating service provider if the call originates TDM) must not publish the PASSporT to the STI-CPS (note that the attacker does not control this behavior nor have any way of knowing it is occurring). For the attacker's call, the service provider who converts the call from TDM to SIP (or the terminating service provider if the call terminates TDM) must retrieve the PASSporT from the STI-CPS (note that the attacker does not control this behavior nor have any way of knowing it is occurring). Due to the number of conditions that must be met, the attacker will likely need to originate a large volume of calls to successfully perform a single replay attack. The large volume of calls with the same calling and called number should be detectable by the originating service provider, terminating service provider, and STI-CPS. Therefore, it is recommended that the originating service provider, terminating service provider, and STI-CPS analyze traffic to detect this attack vector and take preventative actions. It is also recommended that STI-CPSs retain PASSporT(s) for as short a time as practical to make this attack vector more difficult to exploit. IETF RFC 8816 section 7.4 [Ref 102] describes this attack vector and mitigation techniques in more detail. In addition, PASSporTs are distributed to all STI-CPS in the national network, and therefore calling patterns are visible to all STI-CPS in the national network.
- **Transition**: As TDM networks transition to IP, the need for this approach will decrease and eventually disappear, resulting in stranded functionality (e.g., STI-CPS, STI-OOBS, STI-IWF). This transition will not have any impact on SHAKEN-compliant SIP networks that do not use TDM interconnects.
- **SHAKEN compatibility**: This approach complements SHAKEN by transparently extending PASSporTs into the TDM domain:
    - Uses standard PASSporTs
    - Interworks transparently with SHAKEN
    - Does not require any changes to SHAKEN-compliant SIP networks that do not use TDM interconnects
    - Fully supports "shaken", "div", "rcd", and "rph" PASSporTs
    - Should support future PASSporT extensions without changes to standards or functional elements.
- **International**: Fully supports cross-border SHAKEN.
- **Dependencies**: This approach:
    - Requires the STI-CPS to have an STI certificate in order to publish PASSporTs to another STI-CPS.
    - Requires each TDM entity that is generating, publishing, or retrieving PASSporT(s) to have an STI certificate.
    - Requires all STI-CPSs within a national network to form a mesh network.
    - Requires that the PASSporT(s) are received by the STI-CPS before the TDM entity (either the terminating switch or the TDM/SIP gateway) queries for the PASSporT.
    - Multiple calls with the same calling/called party identifiers, within the PASSporT retention window, could result in retrieval of incorrect PASSporT(s).

- Covers scenarios where a call goes between two switches (inter-switch), but it does not cover the case for calls within a single switch (intra-switch). Many legacy networks have experienced significant central office consolidation which increases switch size and therefore increases the number of intra-switch calls.
- Does not explicitly address the functionality required in a TDM terminating network/switch to process verification status information generated by an STI-VS or to deliver a call and associated call authentication information to the called party.
- Requires a governance authority and policy administrator to provide an STI-CPS discovery mechanism but does not specify these capabilities.
- Requires the service provider that is retrieving the PASSporT(s) to reconstruct any SIP headers that were lost in the conversion from SIP to TDM back to SIP, which are protected by the PASSporT(s) (e.g., SIP Resource Priority Header and/or Priority header when an "rph" PASSporT is retrieved [ATIS-1000098, *Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling*]).
- In order to validate authentication tokens, the STI-CPS is required to interface with the STI-PA to retrieve the trusted Secure Telephone Identity Certification Authority (STI-CA) list and Certificate Revocation List (CRL).

Summary: ATIS-1000096 [Ref 3] is structured to maximize alignment with SHAKEN, as specified in ATIS-1000074 [Ref 1]. It uses the identical PASSporT format and supports the same services and PASSporT types. It does not place any requirements on pure SIP networks (i.e., SIP switching and all-SIP interconnects). It introduces new functional elements (STI-OOBS, STI-CPS, STI-IWF) and uses existing functional elements (e.g., STI-AS and STI-VS), which may simplify the transition to an all-SIP network. As a result, this approach may work best for networks that have already started the transition to SIP (in particular, SIP switches that use TDM interconnects) although it does place new requirements on intermediate networks that convert from TDM-to-SIP. The approach can also support TDM switches, but this requires new functionality in the network and in end offices. Some of this new equipment may not be re-usable once the network is upgraded to SIP switches.

ATIS-1000096 [Ref 3] requires deployment of an STI-CPS (STI Call Placement Service) to allow service providers to post and retrieve PASSporTs. The STI-CPS distributes PASSporTs to all other STI-CPS in the national network, and as a result, calling patterns are visible to all STI-CPS. A governance structure is also required to support STI-CPS discovery and to issue STI certificates to the STI-CPS, but is not specified in ATIS-1000096 [Ref 3].

Finally, ATIS-1000096 [Ref 3] provides an approach to provide call authentication for inter-switch calls, but does not address intra-switch calls (i.e., calls that originate and terminate on the same switch). In some networks, central office consolidation has dramatically increased the size of switches, especially legacy TDM switches, and as a result a significant portion of calls can be intra-switch.

A.2 Extending STIR/SHAKEN over TDM

The SHAKEN framework enables a SHAKEN-authorized 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 SIP signaling. ATIS-1000095, *Extending STIR/SHAKEN over TDM*, extends the SHAKEN framework to enable conveying of verified attestation levels over TDM interconnects, originations, and terminations.

This approach relies on bilateral agreements and transitive trust between operators on each end of a TDM connection. The nature of the agreement and whether there is an agreement at all is on a per-TDM connection basis. Therefore, it is flexible in terms of its applicability. An operator may choose to have a different agreement or no agreement on each of its TDM interconnects. This allows partial upgrades and does not require any universal agreement. In the case of calls that traverse a TDM-to-TDM tandem/transit network that transparently passes signaling parameters between multiple peers, this may also require multi-lateral agreement between all service providers that may exchange traffic through the tandem/transit network. It also covers cases where several TDM connections need to be traversed for the signaling path of a particular call, but if a call traverses multiple TDM links and multiple service providers, bilateral agreements are required for every link and service provider in the path. Even a single link not covered by a bilateral agreement will break the transitive trust and it will not be possible to convey the verified attestation levels end-to-end.

The STIR/SHAKEN relationship is terminated/re-generated on the two ends of the TDM interconnect. The terminating side of the STIR/SHAKEN relationship (i.e., the originating side of the TDM interconnect) signals the verified attestation level via the TDM Interconnect to the terminating side of the TDM interconnect (i.e., the side regenerating the STIR/SHAKEN relationship). This can be achieved by making use of the (ISUP Screening Indicator or by making use of dedicated trunk groups pertaining to different attestation levels. The side responsible for re-generating the PASSporT does so based on the received attestation level in the ISUP signaling, and uses its own private key (i.e., STI certificate) to generate a new PASSporT for the SIP signaling. Each STIR/SHAKEN relationship can be considered as a separate "STIR/SHAKEN leg".

Clause 4.11 of ATIS-1000095 [Ref 2] introduces an optional mechanism for being able to reconstruct STIR/SHAKEN PASSporTs after ISUP transport. This mechanism makes use of ISUP to transport some claims and signatures from STIR/SHAKEN PASSporTs, in an encoded form, over ISUP signaling using the ISUP User-to-User Information (UUI) parameter. This approach can support full SHAKEN call authentication end-to-end, but it does not work in all scenarios. Examples of situations where this optional mechanism might not work include:

- The ISUP standard [Ref 11] reserves the UUI parameter for use by the end user. The optional usage of the UUI parameter in the context of non-IP call authentication differs from that specified in that standard. In many service scenarios this parameter is already being used to support end user services. In these cases, the UUI parameter is not available for use in call authentication.
- In some call scenarios, such as call forwarding, the encoded form may exceed the size limit of the UUI parameter.
- ISUP has many optional parameters that in some network configurations can cause the ISUP message size to approach the "message fragmentation limit". In these cases, it may not be possible to use the UUI parameter for call authentication, even if it is available.

ATIS-1000095 [Ref 2] specifies that if the optional mechanism to transport the PASSporT in the ISUP UUI parameter cannot work, then one of the mechanisms defined in Clause 4.2 of ATIS-1000095 [Ref 2] (i.e., using the ISUP Screening Indicator parameter to indicate the level of attestation) will be used instead. Because the level of call authentication might "fallback" to another of the mechanisms defined in ATIS-1000095 [Ref 2], the remainder of this annex includes an assessment of the mechanisms defined in Clause 4.2 of ATIS-1000095 [Ref 2] unless otherwise specified.

- **Scope**: STIR/SHAKEN "shaken" and "div" claims are fully supported in the sense that the appropriate level of attestation is communicated across the TDM network. However, some information available from SHAKEN (e.g., the identity of the OSP and additional caller information provided by the original "origid") may not be available in the PASSporT received by the TSP. This information could be recovered using Call Detail Record (CDR)-based traceback across the TDM domain(s), or by making use of the optional procedures defined in ATIS-1000095 [Ref 2] to carry the original signer and "origid" information in the TDM signaling. In addition, "rcd" and "rph" claims are partially supported, although this is limited because not all of the relevant information can be expressed in an ISUP Initial Address Message (IAM) message.
- **Non-IP calls**: All non-IP call scenarios are supported.

  NOTE: Applicability to 9-1-1 calls is for further study.

- **Network impact**: No changes or additional equipment are required for SIP networks that do not use TDM interconnects. For calls originated in TDM networks, new functionality is required to determine the appropriate level of attestation for a call and to map that into ISUP signaling, or to assign the call to the appropriate trunk group. Additional functionality is also required where SIP/TDM interworking occurs, to verify the PASSporT(s) and map attestation levels into ISUP or to generate a PASSporT based on the information in the ISUP signaling. Depending on the capability and level of support for existing TDM equipment, this new functionality could involve provisioning/configuration changes, software upgrades, and/or additional equipment. In addition, the methods specified in ATIS-1000095 [Ref 2] Clause 4.11 requires new functionality at the SIP/ISUP interworking point to encode STIR/SHAKEN claims and signatures to include in the ISUP UUI parameter and the corresponding functionality at the ISUP/SIP interworking point to reconstruct the PASSporT. Attestation level is sent together with call signaling and therefore not subject to any race conditions or timing issues. It always will be present for the TDM/SIP interworking functionality to be applied if and when it is needed.
- **Network topology**: No a priori network topology knowledge is required.

- **Use cases**: There are no limitations on call flows or deployment models. All call types (e.g., call forwarding, call forking, crankback) in the TDM domain are supported. Simultaneous calls between the same calling/called party pairs are supported without the possibility of any attestation level ambiguity as attestation level is always attached to the call signaling. Calls which stay in the TDM domain for a non-negligible amount of time during call setup (e.g., due to announcements or for digit collection) do not pose a problem as reconstructing the PASSporT is not time sensitive. It is not associated with a timer which may expire.
- **Security considerations**: The existing STIR/SHAKEN framework is utilized to deduce the "shaken" attestation level pertaining to a call. Transitive trust is required in the TDM domain. This approach does not introduce additional concerns about information leakage pertaining to calling patterns since no information is exposed to entities which are not already in the call signaling path.
- **Transition**: As TDM networks transition to IP, the need for this approach will decrease and eventually disappear, resulting in stranded functionality within existing network elements. This transition will not have any impact on SHAKEN-compliant SIP networks that do not use TDM interconnects.
- **SHAKEN compatibility**: This approach identifies the appropriate level of attestation within the TDM domain and converts this into a "shaken" PASSporT at the TDM-to-SIP boundary. The "shaken" PASSporT generated is a fully standards-compliant "shaken" PASSporT, but it is signed by the service provider converting TDM-to-SIP rather than by the originating service provider, while preserving the level of attestation. Direct visibility to the originating service provider is not provided in an end-to-end fashion unless CDR traceback mechanisms or the optional procedures to carry originating servicer provider information in ISUP signaling are used. If CDR traceback is used, it is only needed for the TDM portions of the connection. Standard SHAKEN mechanisms can still be used for the SIP portions of the connection path, e.g., if signature validation fails at the SIP-to-TDM boundary then originating service provider information can be used for locating the source of the problem. In addition to "shaken" PASSporTs, this approach supports other PASSporTs (e.g., "div", "rcd", and "rph").
- **International**: Fully supports cross border SHAKEN.
- **Dependencies**:
    - Existing networks use the ISUP Screening Indicator in a manner that is broadly consistent with this approach, but not necessarily identical. TDM connections using this approach require bilateral agreements between both service providers and in some tandem/transit use cases multilateral agreements between service providers whose values are sent transparently over multiple hops, and the connections are required to be correctly provisioned and screened to maintain the transitive trust relationship. In addition, if the ISUP Screening Indicator method is used, it is recommended that the ISUP links from untrusted entities (i.e., those without the required bilateral agreements) be monitored to ensure the ISUP Screening Indicator is set to "user provided, not verified". Monitoring the ISUP Screening Indicator is not required if separate trunk groups are used to convey attestation levels, but in that case the trunk groups are required to be correctly provisioned and configured to ensure they only include calls with the appropriate level of attestation.
    - The ISUP UUI parameter is reserved for use by the end user, and therefore the optional encoding specified in ATIS-1000095 [Ref 2] differs from the standard. The intent is that the use of the UUI parameter by the end user will take precedence.
    - This approach describes several options for carrying call authentication in TDM signaling. Therefore, the bilateral agreements between service providers are required to specify exactly which options are supported to ensure interoperability.
    - This approach specifies the mapping between TDM and SIP at the TDM/SIP boundary but does not explicitly address the functionality required at an originating or terminating TDM switch. In SHAKEN, the STI-AS determines the appropriate level of attestation and generates a PASSporT. To provide equivalent functionality with this approach, the Originating Service Provider's TDM switch would need to determine the appropriate level of attestation and either set the ISUP Screening Indicator or groom the traffic into the correct trunk group. In addition, the ISUP/SIP interworking function determines the appropriate level of attestation from the ISUP Screening Indicator, or from the trunk group, and passes this to an STI-AS function to create a "shaken" PASSporT. The intermediate provider performing the interworking function and generating the PASSporT is required to have an STI certificate. Finally, if an ISUP trunk terminates directly on a TDM switch, the switch determines the appropriate level of attestation from the ISUP Screening Indicator or from the trunk group.

The following apply if the optional mechanism to encode STIR/SHAKEN PASSporT claims and signatures in the ISUP UUI parameter, as described in ATIS-1000095 [Ref 2] Clause 4.11, is used:

- Additional functionality is required at the SIP/ISUP and ISUP/SIP boundaries to implement this encoding.
- If an ISUP trunk terminates on a TDM end office that does not support the mechanism, there is a risk that STIR/SHAKEN PASSporT claims and signatures could be passed across a Primary Rate Interface (PRI) to the terminating subscriber. This functionality uses a dedicated UUI Protocol Discriminator value which could be used by entities consuming UUI but not supporting this mechanism to ignore UUI content.
- If the OSP does not support the mechanism, and if the ISUP UUI parameter in the PRI from the originating enterprise contains encoded STIR/SHAKEN PASSporT claims and signatures, as described in ATIS-1000095 [Ref 2], then it is possible that the STIR/SHAKEN PASSporT claims and signatures could be passed into the network in the UUI parameter in ISUP signaling.
- It is possible that the receipt of a UUI parameter containing an encoded PASSporT by a network not supporting this mechanism could result in a charge to the calling or called party for the delivery/transport of the UUI parameter. Accordingly, this UUI mechanism should not be used for any call where this could occur.
- This specification covers scenarios where a call goes between two switches (inter-switch), but it does not cover the case for calls within a single switch (intra-switch). Many legacy networks have experienced significant central office consolidation which increases switch size and therefore increases the number of intra-switch calls.

Summary: ATIS-1000095 [Ref 2] is structured to take advantage of existing ISUP signaling parameters to minimize the impact on existing TDM switches. It uses TDM switch provisioning and configuration capabilities, where possible, to identify and communicate attestation levels to the terminating service provider over TDM interconnects. As a result, this approach provides a degree of call authentication (i.e., attestation level) for TDM switches with TDM interconnects while minimizing the impact on existing TDM equipment. Call authentication information is included in the call signaling and does not introduce the possibility of the incorrect PASSporT being retrieved or the possibility of the PASSporT not being available, nor expose any new information about calling patterns. It does not place any requirements on pure SIP networks (i.e., SIP switching and all-SIP interconnects) although it does introduce new requirements on intermediate networks that convert from TDM-to-SIP and on SIP switches with TDM interconnects.

The approach described in ATIS-1000095 [Ref 2] is designed to be flexible, allowing service providers to choose the option that is best suited to each situation. But as a result, bilateral agreements are required between service providers, for each interconnection, to fully specify the exact configuration and to maintain the integrity of the transitive trust.

Finally, ATIS-1000095 [Ref 2] provides an approach to provide call authentication for inter-switch calls, but does not address intra-switch calls (i.e., calls that originate and terminate on the same switch). In some networks, central office consolidation has dramatically increased the size of switches, especially legacy TDM switches, and as a result a significant portion of calls can be intra-switch.