ATIS-1000097.v003

ATIS Standard on -

Alternatives for Call Authentication for Non-IP Traffic

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-1000097.v003

ATIS Technical Report on

Alternatives for Call Authentication for Non-IP Traffic

Alliance for Telecommunications Industry Solutions

Approved December 2, 2024

Abstract

The SHAKEN framework, governance model, and certificate management enable 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.

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

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

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

At the time it approved this 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)* [Ref 2], 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 2] 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* [Ref 11]. 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-0500046, *Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services*.[1]

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

[Ref 3] ATIS-1000095, *Extending STIR/SHAKEN over TDM.*[1]

[Ref 4] ATIS-1000096, *Out-of-Band PASSporT Transmission Involving TDM Networks.*[1]

[Ref 5] ATIS-1000098, *Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling*.[1]

[Ref 6] ATIS-1000628, *Emergency Calling Service*.[1]

[Ref 7] ATIS-1000105, *Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM*.[1]

[Ref 8] IETF RFC 3261, *SIP: Session Initiation Protocol.*[2]

[Ref 9] IETF RFC 3966, *The tel URI for Telephone Numbers.*[2]

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

[Ref 11] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*[2]

[Ref 12] IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates.*[2]

[Ref 13] ITU Q.763 (12/1999), *Signalling System No. 7 – ISDN user part formats and codes.*[3]

[Ref 14] J-STD-036-C-2, *Enhanced Wireless 9-1-1 Phase II.* [4]

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* [Ref 10]). 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 10].

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

---

[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/ >.

[4] Available from Telecommunications Industry Association (TIA) at: < https://tiaonline.org/ >.

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 10].

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

Secure Telephone Identity (STI) Certificate: A public key certificate needed by a service provider to sign or verify a PASSporT (RFC 8226, *Secure Telephone Identity Credentials: Certificates* [Ref 12]).

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 10].

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 [IETF RFC 3966, *The tel URI for Telephone Numbers* (Ref 9)]) from which a telephone number can be derived.

3.2 Acronyms & Abbreviations

ALI	Automatic Location Identification
ANI	Automatic Number Identification
ATIS	Alliance for Telecommunications Industry Solutions
CA	Certification Authority
CAMA	Centralized Automated Message Accounting
CDR	Call Detail Record
CNAM	Calling Name
CPE	Customer Premises Equipment
CPS	Call Placement Service
CRL	Certificate Revocation List
CVT	Call Validation Treatment
E9-1-1	Enhanced 9-1-1
E-MF	Enhanced Multi-Frequency
ESRK	Emergency Services Routing Key
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
LCR	Least Cost Routing
LNG	Legacy Network Gateway
LPG	Legacy PSAP Gateway
LSRG	Legacy Selective Router Gateway
MF	Multi-Frequency
MFA	Multi-Factor Authentication
MGCF	Media Gateway Control Function
MSC	Mobile Switching Center
NG9-1-1	Next Generation 9-1-1
NNI	Network-to-Network Interface
NPA	Numbering Plan Area
NPD	Numbering Plan Digit
OSP	Originating Service Provider
PASSporT	Personal ASSertion Token
PKI	Public Key Infrastructure
PRI	Primary Rate Interface
PSAP	Public Safety Answering Point
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
SR	Selective Router
SS7	Signaling System No. 7
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
WCM	Wireline Compatibility Mode

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 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.

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?
- **Impact on non-participants:** Are changes required in networks that would not otherwise participate in call authentication, to convey call authentication information between networks that do, or for other reasons?
- **Impact on call routing:** Are changes required to existing TDM Least Cost Routing (LCR) systems, such that support of call authentication by potential downstream networks is considered?
- **Co-existence**: Can the approach co-exist with other non-IP call authentication approaches?
- **Discovery**: Is a priori knowledge required to support the approach? If so, identify where it is required, and how it is obtained. Examples of network knowledge that might be required include:
  - Assuming that in the North American voice network multiple non-IP Call Authentication approaches are implemented, how is the approach to use for a given egress TDM route, determined?
  - 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.
- **Scalability**: Does the approach lend itself to the creation of separate "instances" (defined for example by a set of shared STI-CPS servers)? If so, how big can an instance be and what factors limit its size? In such a (multi-instance) scenario, how is the instance to use for a given call, determined? In the event that an approach does not lend itself to creation of instances, are there limits on its scalability?
- **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 [Ref 2], rather than duplicate or compete? This would include things like:
    - Does it use a standard "shaken" PASSporT?
    - Can the approach interwork with SHAKEN [Ref 2]?
    - What is the impact on existing SIP networks that have deployed SHAKEN [Ref 2]? Ideally any approach would be transparent to SIP networks that have implemented SHAKEN [Ref 2] 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.

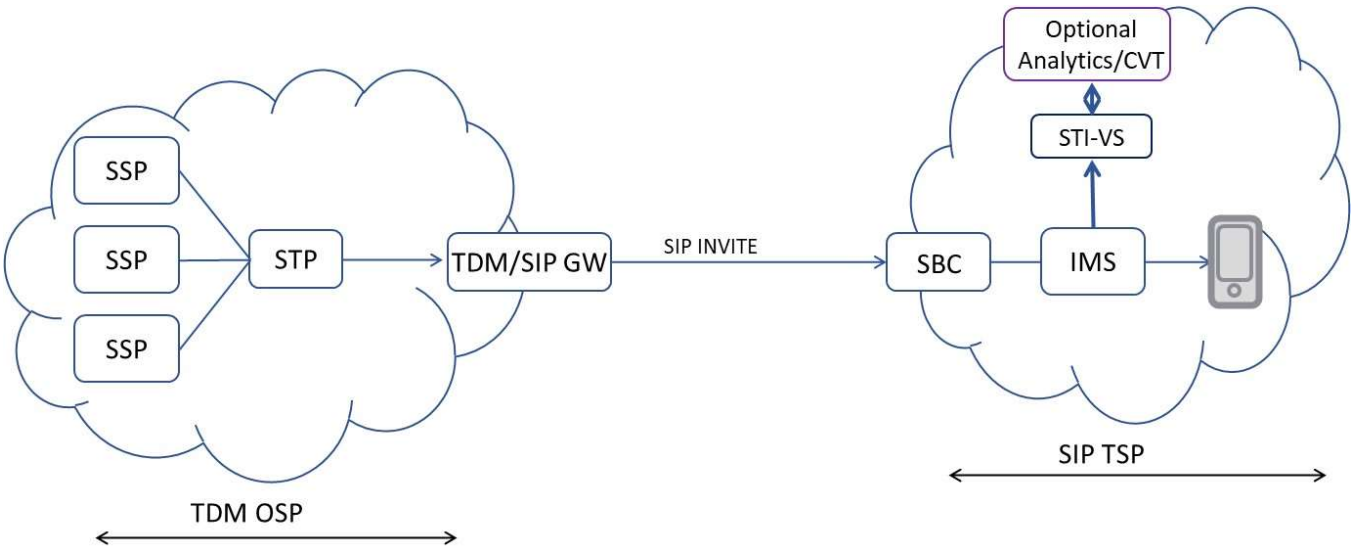

Figure 5-1: TDM → SIP

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.

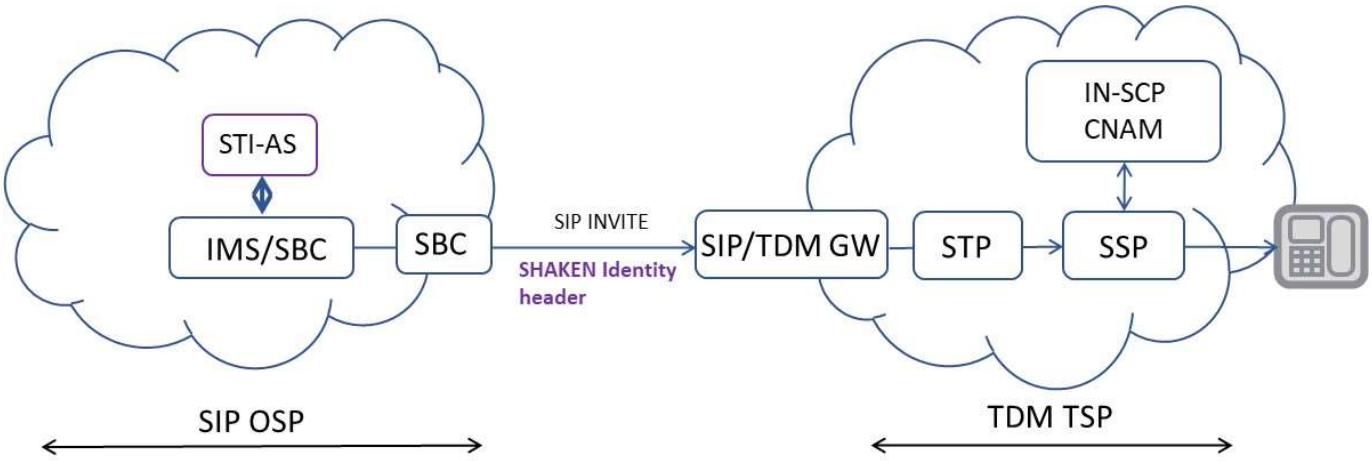

Figure 5-2: SIP → TDM

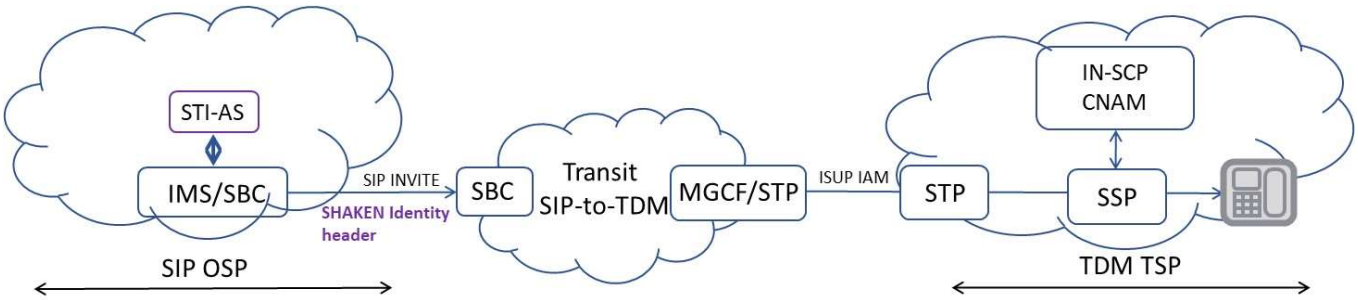

Figure 5-3: SIP → TDM With Conversion in the Transit Network

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.

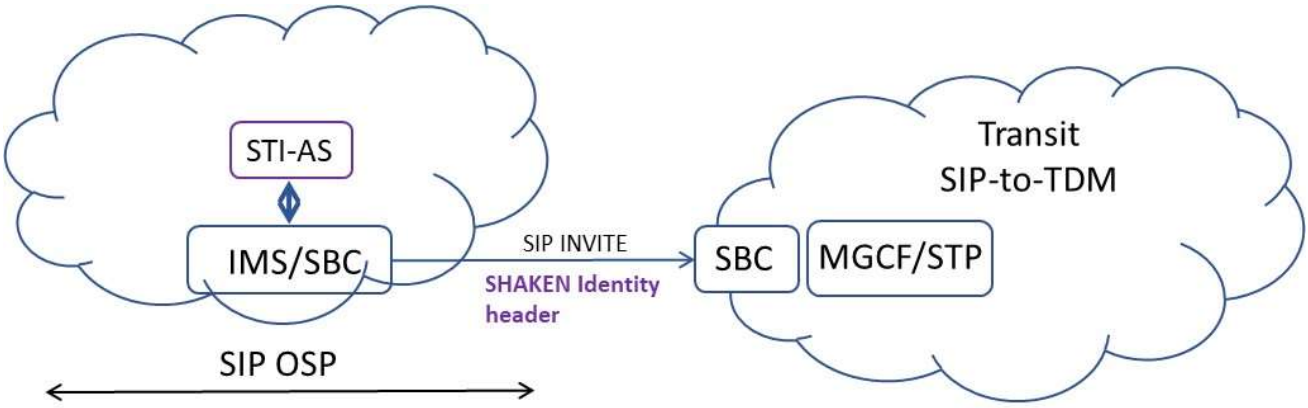

Figure 5-4: SIP → TDM Transit Network

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.

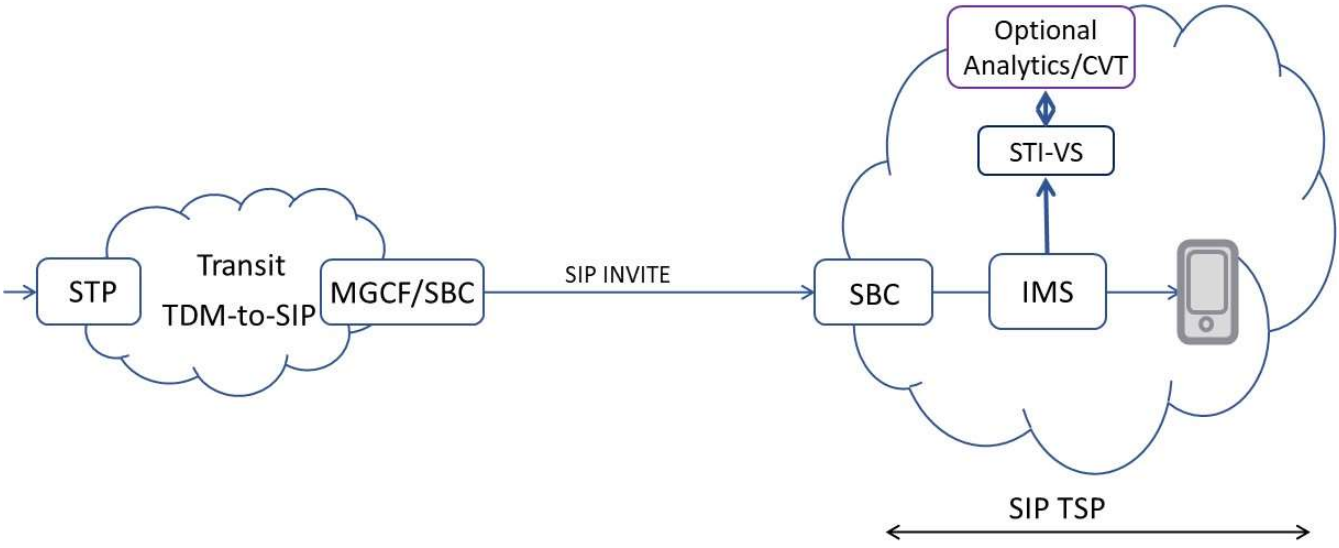

Figure 5-5: TDM → SIP

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.

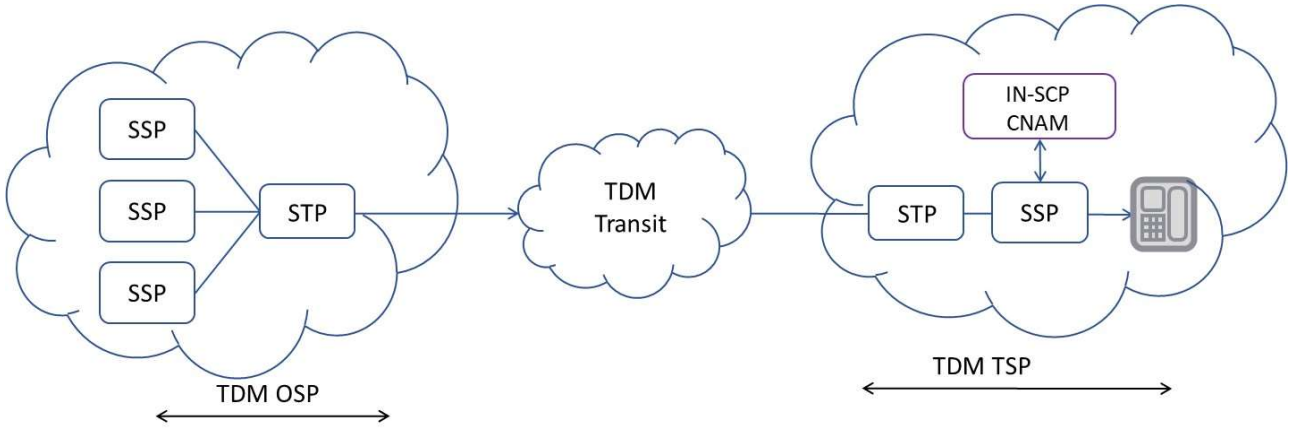

Figure 5-6: TDM → TDM

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.

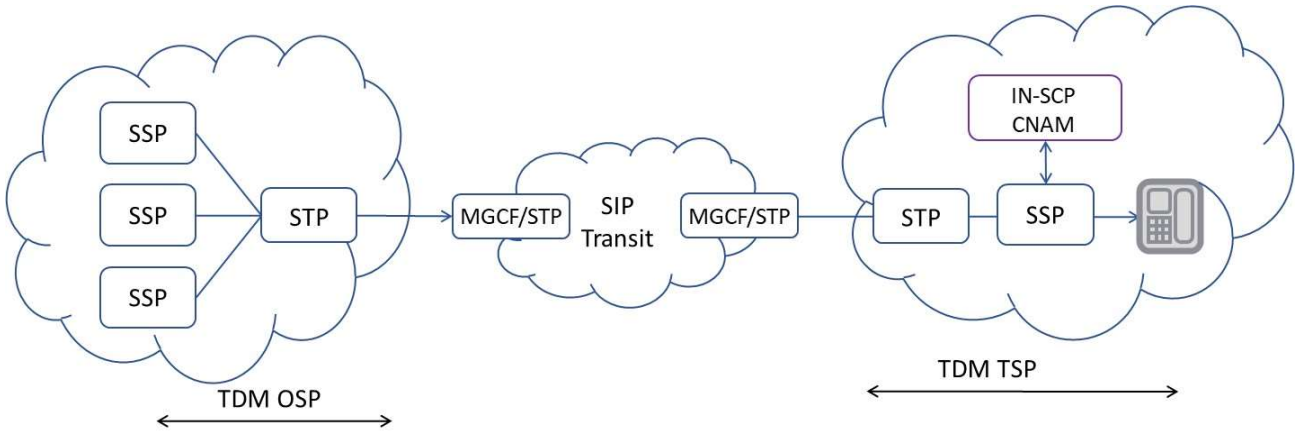

Figure 5-7: TDM → TDM with SIP Transit Network

6 Assessment

This Technical Report identifies non-IP call scenarios where standard SHAKEN [Ref 2] 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 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: Non-IP Call Authentication Approaches (Informative)identifies the key attributes of each approach, based on the factors identified in Clause 4.3 to provide a better understanding of each scenario.

The approaches described in Annex A: Non-IP Call Authentication Approaches (Informative)can be utilized in the call path of a single call.

The approaches may be used independently by different service providers in the call path, as shown in Figure 6-1. At minimum, service providers need to support configuration of approach per TDM interface and implement an approach that is supported by the service providers they interconnect with. This may require some service providers to implement more than one approach for call authentication to be transmitted end-to-end.

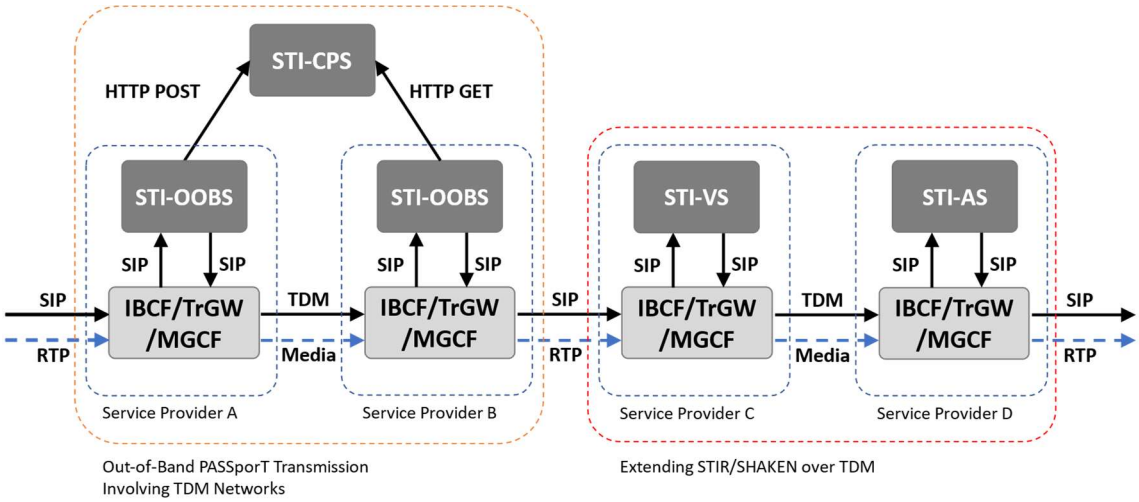

Figure 6-1: Independent Usage of Approaches

The 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 NNI between each other would need to agree on one of the approaches for transmitting attestation levels over the TDM NNI.

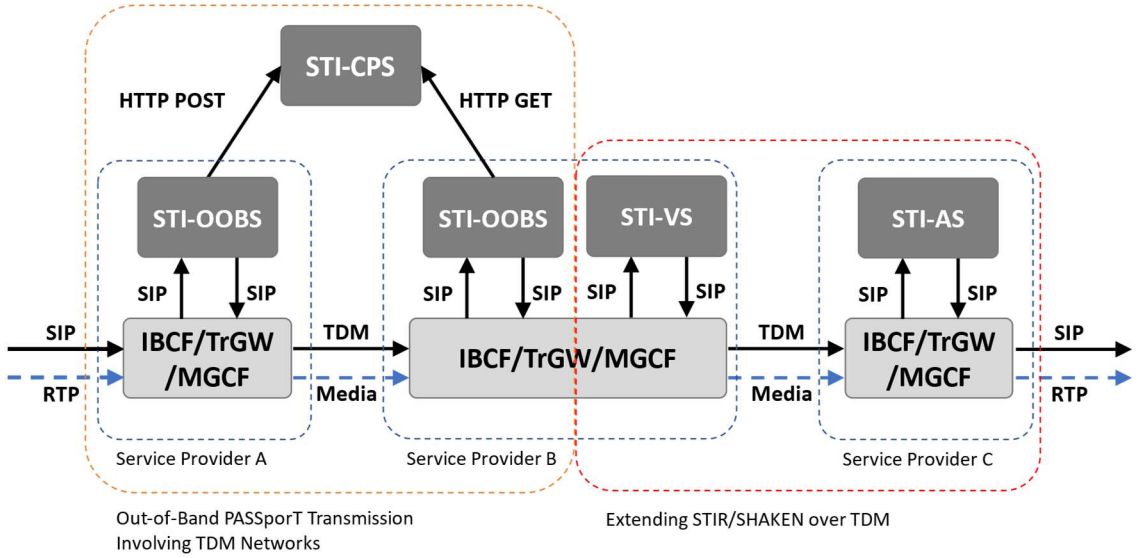

Figure 6-2: Boundary Point Usage of Approaches

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

A.1 Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM

ATIS-1000105, *Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM* [Ref 7], extends the currently defined SHAKEN [Ref 2] framework, governance model, and certificate management to enable the transmission of PASSporTs for calls that use TDM signaling and/or TDM switches during origination, termination, and/or transit.

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 [Ref 2] trust model for STI-CPS access control. An STI-CPS has a standardized interface for service provider's Secure Telephone Identity Out-of-Band Service (STI-OOBS) to publish and retrieve PASSporT(s).

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

A service provider network that converts a call from SIP signaling to TDM signaling invokes an STI-OOBS to publish all associated PASSporT(s) received in the SIP signaling to the agreed STI-CPS before the call is sent downstream. If no PASSporT(s) are received, the service provider's STI-AS generates the applicable PASSporT(s) and then the STI-OOBS publishes the generated PASSporT(s) to the agreed STI-CPS before the call is sent downstream. An OSP network that sends a call via a TDM NNI invokes an STI-AS to generate the applicable PASSporT(s) and then invokes an STI-OOBS to publish the generated PASSporT(s) to the agreed STI-CPS before the call is sent downstream.

A service provider network that converts a call from TDM signaling to SIP signaling invokes an STI-OOBS to retrieve all PASSporT(s) associated with the call from the agreed STI-CPS and then inserts the retrieved PASSporT(s) into the SIP signaling in Identity header(s) as described in RFC 8224 [Ref 11]. A TSP network that receives a call via a TDM NNI invokes an STI-OOBS to retrieve all PASSporT(s) associated with the call from the agreed STI-CPS and then inserts the retrieved PASSporT(s) into the SIP signaling in Identity header(s) for delivery to the TSP's STI-VS function.

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

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. 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 NNIs.

- **Network topology**: The STI-OOBS of a service provider performing a publish is provisioned with the mutually agreed STI-CPS for each TDM NNI. The STI-OOBS of a service provider performing a retrieve is provisioned with the mutually agreed STI-CPS for each TDM NNI and the SPC of the service provider from which the call was received. Each service provider whose network includes TDM NNIs needs to establish a relationship for STI-CPS access with every STI-CPS that is mutually agreed with one or more of its TDM peers. For each TDM NNI that a call traverses, the PASSporT(s) associated with the call are published to and retrieved from an agreed STI-CPS. The PASSporT(s) related to a given call may be published to and retrieved from an STI-CPS multiple times, once for each TDM NNI that the call traverses. The same or a different STI-CPS may be used at each TDM NNI. Unlike ATIS-1000096, *Out-of-Band PASSporT Transmission Involving TDM Networks* [Ref 4], in which a call transiting from one TDM NNI directly to another TDM NNI does not trigger the need for any additional interaction with an STI-CPS, with this standard a service provider network that receives a call via a TDM NNI always invokes an STI-OOBS to retrieve any available PASSporT(s) from an STI-CPS, and then in the case where it also sends that call via a TDM NNI it invokes an STI-OOBS to publish the successfully retrieved PASSporT(s), or generated PASSporT(s) if no PASSporT(s) were successfully retrieved, to the STI-CPS agreed to with the next-hop TDM peer.
- **Use cases**: Supports call forwarding, call forking, and crankback.
- **Security considerations**: Leverages the extensive security analysis performed in the IETF (RFC 8816, *Secure Telephone Identity Revisited (STIR) Out-of-Band Architecture and Use Cases* [Ref 102]). Drastically simplifies the security requirements by limiting access to only Secure Telephone Identity Policy Administrator (STI-PA)-approved service providers. An attacker could cause a legitimate call that was authenticated to appear unauthenticated (which is no different than how the legitimate call appears without Out-of-Band SHAKEN). The attacker must 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 attacker's call must traverse at least one of the same service provider networks as the original call (note that the attacker does not control this behavior nor have any way of knowing it is occurring). If some publish requests are accepted and some publish requests fail, the STI-CPS may be unable to accurately determine if there are multiple calls with the same calling and called number occurring in close proximity, which could result in the STI-CPS returning the wrong PASSporT for a call when it should have returned no PASSporTs.
- **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 NNIs.
- **SHAKEN compatibility**: This approach complements SHAKEN [Ref 2] by transparently extending PASSporTs into the TDM domain:
    - Uses standard PASSporTs.
    - Interworks transparently with SHAKEN [Ref 2].
    - Does not require any changes to SHAKEN-compliant SIP networks that do not use TDM NNIs.
    - Fully supports "shaken", "div", "rcd", and "rph" PASSporTs.
    - Should support future PASSporT extensions without changes to standards or functional elements.
- **International**: Fully supports SHAKEN [Ref 2] applied across country boundaries.
- **Dependencies**: This approach:
    - Requires each service provider with a TDM NNI to have an STI certificate.
    - Requires each pair of service providers with a TDM NNI to agree to use a particular STI-CPS for each call that traverses that TDM NNI. A given service provider may need to interface with multiple STI-CPSs to exchange PASSporTs with all its TDM peers.

Summary: ATIS-1000105 [Ref 7] is structured to maximize alignment with SHAKEN, as specified in ATIS-1000074 [Ref 2]. 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 NNIs). 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, softswitches that use TDM NNIs) although it does place new requirements on intermediate TDM networks. 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 softswitches.

ATIS-1000105 [Ref 7] requires deployment of an STI-CPS (STI Call Placement Service) to allow service providers to publish and retrieve PASSporTs.

ATIS-1000105 [Ref 7] 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 associated call authentication information to the called party.

A.2 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 [Ref 4] framework to enable the transmission of PASSporTs for calls that use TDM signaling and/or TDM switches during origination, termination, and/or transit.

Due to the security considerations with this specification, documented below, use of ATIS-1000105 [Ref 7] may be preferrable.

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 [Ref 2] 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* [Ref 8], (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 NNIs. 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 4] 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 the PASSporT(s) to an STI-CPS.
- **Security considerations**: Leverages the extensive security analysis performed in the IETF [Ref 102]. 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, *PASSporT: Personal Assertion Token* [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 4]) 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 NNIs.
- **SHAKEN compatibility**: This approach complements SHAKEN [Ref 2] by transparently extending PASSporTs into the TDM domain:
    - Uses standard PASSporTs.
    - Interworks transparently with SHAKEN [Ref 2].
    - Does not require any changes to SHAKEN-compliant SIP networks that do not use TDM NNIs.
    - Fully supports "shaken", "div", "rcd", and "rph" PASSporTs.
    - Should support future PASSporT extensions without changes to standards or functional elements.
- **International**: Fully supports SHAKEN [Ref 2] applied across country boundaries.
- **Dependencies**: This approach:
    - Requires the STI-CPS to have an STI certificate 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).
- 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* [Ref 5]).
- To validate authentication tokens, the STI-CPS is required to interface with the STI-PA(s) to retrieve the trusted Secure Telephone Identity Certification Authority (STI-CA) list and Certificate Revocation List (CRL).

Summary: ATIS-1000096 [Ref 4] is structured to maximize alignment with SHAKEN, as specified in ATIS-1000074 [Ref 2]. 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 NNIs). 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, softswitches that use TDM NNIs) 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 softswitches.

ATIS-1000096 [Ref 4] 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 4].

A.3 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* [Ref 3], extends the SHAKEN [Ref 2] framework to enable conveying of verified attestation levels over TDM NNIs, 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 NNIs. 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 NNI. The terminating side of the STIR/SHAKEN relationship (i.e., the originating side of the TDM NNI) signals the verified attestation level via the TDM NNI to the terminating side of the TDM NNI (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 3] 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 [Ref 2] 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, ITU Q.763 (12/1999), *Signalling System No. 7 – ISDN user part formats and codes* [Ref 13], 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 3] 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 3] (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 3], the remainder of this annex includes an assessment of the mechanisms defined in Clause 4.2 of ATIS-1000095 [Ref 3] 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 3] 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 the relevant information can be expressed in an ISUP Initial Address Message (IAM) message.
- **Non-IP calls**: All non-IP call scenarios over ISUP/SS7 interfaces are supported.

- **Network impact**: No changes or additional equipment are required for SIP networks that do not use TDM NNIs. 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 Clause 4.11 [Ref 3] 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 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, 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 NNIs.
- **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 [Ref 2] 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 SHAKEN [Ref 2] applied across country boundaries.
- **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 3] 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 ISUP and SIP at the ISUP/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.
    - ATIS-1000095 [Ref 3] is only applicable when the signaling protocol used on the non-IP interface is ISUP/SS7.

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 Clause 4.11 [Ref 3], 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 3], 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.

Summary: ATIS-1000095 [Ref 3] 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 NNIs. As a result, this approach provides a degree of call authentication (i.e., attestation level) for TDM switches with TDM NNIs 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 NNIs) although it does introduce new requirements on intermediate networks that convert from TDM-to-SIP and on softswitches with TDM NNIs.

The approach described in ATIS-1000095 [Ref 3] 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.

Annex B: Applicability of Non-IP Call Authentication Solutions to 9-1-1 Calls

ATIS-0500046, *Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services* [Ref 1], discusses call authentication in the context of emergency services offered using legacy Enhanced 9-1-1 (E9-1-1) and transitional Next Generation 9-1-1 (NG9-1-1) architectures. Specifically, it considers the applicability and impacts of the *Signature-based Handling of Asserted information using toKENs (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks* [SHAKEN OOB] solution described in ATIS-1000096 [Ref 4], and the *Extending STIR/SHAKEN Over TDM* solution described in ATIS-1000095 [Ref 3], on the processing of 9-1-1 calls in all-TDM and mixed TDM/IP environments. These solutions assume that TDM networks support the ability to obtain caller identity attestation level and verification status information either by implementing new functional elements and/or interfaces to support the acquisition of such information, or by using mappings between SIP headers and Signaling System No. 7 (SS7) signaling parameters or specific trunk groups to convey such information with the call. In assessing the applicability of these approaches to 9-1-1 calls, the unique architecture and signaling characteristics of E9-1-1 and transitional NG9-1-1 environments must be considered. The material in this clause highlights key considerations described in detail in ATIS-0500046 [Ref 1]. It is important to note that, while ATIS-0500046 [Ref 1] did not consider the Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM mechanism addressed in ATIS-1000105 [Ref 7], the same considerations regarding the applicability of this non-IP call authentication solution to 9-1-1 calls apply as for the SHAKEN OOB solution described in ATIS-1000096 [Ref 4].

B.1 Considerations for 9-1-1 Call Authentication in an E9-1-1 Environment

In E9-1-1 architectures, specially equipped switching systems referred to as Selective Routers (SRs) typically receive emergency calls over dedicated Multi-Frequency (MF) or SS7-supported trunk groups from wireline end offices and Mobile Switching Centers (MSCs). They use information received in incoming signaling to identify the Public Safety Answering Point (PSAP) that serves the area in which the call originated. SRs deliver the emergency call to the PSAP, typically over traditional Centralized Automated Message Accounting (CAMA)-like (i.e., Traditional MF) or Enhanced MF (E-MF) interfaces. Traditional MF is still in use in certain areas today and supports the delivery of a 7-digit number, along with a single Numbering Plan Digit (NPD) that can be used to derive the Numbering Plan Area (NPA) and to indicate whether the Automatic Number Identification (ANI) information should be displayed using a steady or flashing display[5]. E-MF is a Feature Group D-like signaling scheme that is more commonly used between SRs and PSAPs. It supports the delivery of either one or two 10-digit numbers to the PSAP with the call, along with an ANI II value that tells the PSAP Customer Premises Equipment (CPE) whether to display the information using a steady or flashing display. The MF signaling stream includes a key that the PSAP will use to query an Automatic Location Identification (ALI) database for the caller's location information. Having retrieved the location information, the PSAP can support the dispatch of emergency personnel to the incident location.

The application of the SHAKEN OOB solution to an E9-1-1 architecture would be most closely addressed by the end-to-end TDM call scenario illustrated in Figure 8-9 of ATIS-1000096 [Ref 4]. Since the SHAKEN OOB mechanism assumes that all TDM networks support SS7, this non-IP call authentication solution would not apply to E9-1-1 architectures that currently use MF signaling to legacy SRs. The SHAKEN OOB call authentication mechanism requires additional functional elements and interfaces to be accessible to switches in the TDM originating network and, in the case of an E9-1-1 architecture, SRs in a legacy Emergency Services Network. For example, the application of the SHAKEN OOB call authentication mechanism to 9-1-1 calls in an E9-1-1 environment would require that end offices/MSCs route calls to an interworking function (i.e., STI-IWF) rather than being routed directly over a dedicated trunk group to an SR. The STI-IWF would be responsible for interacting with an STI-AS to obtain a "shaken" PASSporT for the call, and with an STI-OOBS to have that PASSporT published to an STI-CPS. The SHAKEN OOB solution would also expect there to be an STI-IWF in the legacy Emergency Services Network. The STI-IWF would be responsible for retrieving the "shaken" PASSporT (via the STI-OOBS) and interacting with the STI-VS to verify it. There would be impacts on existing SR call processing and interfaces to support interactions between an SR and an STI-IWF and the handling of verification status information by the SR.

There are unique challenges associated with defining a mechanism to convey attestation and verification status information to legacy PSAPs with 9-1-1 calls. For legacy PSAPs, the ability to convey attestation or verification status information is significantly limited using legacy MF interfaces for call delivery and legacy ALI interfaces for the delivery of location and some non-location information. For legacy PSAPs that support E-MF interfaces, it might be possible to use spare "II" values to convey attestation and verification information associated with the caller identity, but this would require modifications to the call processing supported by the SR to correctly populate the "II" value in the outgoing E-MF signaling based on attestation and verification status information received from the STI-IWF. There would also be impacts on PSAP Operating Procedures to support the interpretation of the new "II" values by PSAP call takers. For legacy PSAPs that support Traditional MF interfaces, there is no practical MF signaling-based option for conveying attestation and verification status information with a 9-1-1 call due to the significant signaling limitations associated with such interfaces.

Special consideration should also be given to the relevance of the SHAKEN OOB non-IP call authentication solution to wireless 9-1-1 calls that support the Wireline Compatibility Mode (WCM) approach defined in J-STD-036-C-2, *Enhanced Wireless 9-1-1 Phase II* [Ref 14]. When the WCM approach is used for 9-1-1 calls, an Emergency Services Routing Key (ESRK) is conveyed via the SS7 Calling Party Number parameter rather than the callback number; the callback number is provided to the PSAP via the ALI system using a separate data interface. While there may still be value in authenticating the ESRK to ensure that it was populated by the legacy wireless originating network, and not one that was spoofed by a bad actor, authenticating, and verifying the ESRK does not communicate anything about the legitimacy of the callback information.

In considering the application of the Extending STIR/SHAKEN Over TDM call authentication solution to 9-1-1 calls in an E9-1-1 environment, the mappings between Screening Indicator values (or trunk groups) and attestation levels described in ATIS-1000095 [Ref 3] assume that at least one network involved in processing the call is SHAKEN-capable, and that interworking between SS7 and SIP will need to be performed at some point in the call path. In an

[5] A flashing display is intended to alert the PSAP call-taker to special conditions related to call treatment.

E9-1-1 environment, neither the originating network nor the Emergency Services Network is SHAKEN/SIP-capable, so the Extending STIR/SHAKEN Over TDM mechanism may not directly apply. However, the mappings defined between Screening Indicator values (for legacy originating networks that interconnect to SRs using SS7 trunks) and attestation levels could be used as a basis for determining the attestation level and verification status associated with the information signaled in the SS7 Calling Party Number parameter. Based on standards related to E9-1-1 (i.e., ATIS-1000628, *Emergency Calling Service* [Ref 6]), an SS7 Calling Party Number parameter will be populated with a network-provided number (i.e., Screening Indicator set to "network provided"), unless the call originates from an ISDN interface, the originating switch allows user-provided numbers from ISDN interfaces to be used as calling party numbers, and the user-provided number passes screening. In the latter case, the Screening Indicator associated with the Calling Party Number will have the value "user provided, screening passed". Per ATIS-1000628 [Ref 6], a user-provided number that fails screening shall not be sent toward the SR; instead, the main (i.e., network-provided) number shall be sent toward the SR as the calling party number. According to ATIS-1000095 [Ref 3], both a Screening Indicator value of "network provided" and a Screening Indicator value of "user provided, verified and passed" would be associated with an attestation level of "A" and a "verstat" value of "TN-Validation-Passed".

Since, based on ATIS-1000095 [Ref 3], all allowable Screening Indicator parameter values associated with 9-1-1 originations from legacy originating networks will map to an attestation level of "A" and a "verstat" value of "TN-Validation-Passed", it may be sufficient just to know that the call originated in a legacy wireline or wireless network to associate an "A" attestation and a verification status of "TN-Validation-Passed" with the information signaled as the calling number. The type of network that the call originated from is known by the SR based on the incoming trunk group but cannot be determined by the legacy PSAP based on MF signaling associated with a 9-1-1 call. The same issue related to conveyance of attestation and verification status information to legacy PSAPs via MF call setup interfaces applies as for the SHAKEN OOB call authentication mechanism.

The UUI-based mechanism defined in ATIS-1000095 [Ref 3] does not apply in a legacy E9-1-1 environment because standards and existing implementations do not support the delivery of the UUI parameter in an SS7 IAM associated with a 9-1-1 call. If an SR were able to receive a UUI parameter containing a "shaken" PASSporT, it is not clear what it would do with it, or how it could be used to convey attestation level and verification status information to a legacy PSAP over an MF interface.

Applying either the SHAKEN OOB or Extending STIR/SHAKEN Over TDM solutions to an E9-1-1 Service architecture would have an impact on the signaling and call processing supported by legacy SRs. Since suppliers of SR equipment are no longer implementing enhancements to those systems, call authentication solutions that require support for new call processing or modifications to signaling interfaces at an SR cannot be viewed as technically feasible. In addition, even if an SR could obtain attestation level and verification status information associated with a 9-1-1 call based on information received via existing SS7 interfaces (or the incoming trunk group), the ability to deliver this information to legacy PSAPs is limited by the MF call delivery interfaces typically supported by legacy PSAPs today. ATIS-0500046 [Ref 1] describes an alternative approach for supporting caller authentication in an E9-1-1 environment that uses the ALI interface to deliver information that will allow a legacy PSAP to determine the caller identity attestation level and verification status for a 9-1-1 call.

B.2 Considerations for 9-1-1 Call Authentication in a Transitional NG9-1-1 Environment

During the transition to end-state NG9-1-1, NG9-1-1 Emergency Services Networks will be required to support emergency calls that originate in legacy (circuit-switched) wireline and wireless networks and must be able to support the delivery of emergency calls to legacy PSAPs that they serve. As a result, gateway functionality will be a required part of transitional NG9-1-1 architectures. A high-level overview of the types of gateways that may be included in a transitional NG9-1-1 architecture is provided below.

- Legacy Network Gateways (LNGs) – An LNG logically resides between a legacy/TDM originating network and an IP/SIP-based NG9-1-1 Emergency Services Network and allows PSAPs served by the NG9-1-1 Emergency Services Network to receive emergency calls from legacy originating networks. The LNG interworks the SS7 or MF signaling received from a legacy originating network to the SIP signaling used in the NG9-1-1 Emergency Services Network and uses NG9-1-1-specific processing to support the routing of emergency calls to the appropriate element in the appropriate NG9-1-1 Emergency Services Network.
- Legacy PSAP Gateway (LPG) – An LPG is a signaling and media interconnection point between an NG9-1-1 Emergency Services Network and a legacy PSAP. In a transitional NG9-1-1 architecture that includes an LPG, the LPG will receive the same signaling associated with a 9-1-1 call from the NG9-1-1

Emergency Services Network as an NG9-1-1 PSAP would receive. In addition, the LPG is required to deliver 9-1-1 calls and associated data to legacy PSAPs using the same MF call delivery interfaces and ALI interfaces as the PSAP would use in an E9-1-1 environment.

- Legacy Selective Router Gateway (LSRG) – An LSRG is a signaling and media interconnection point between a legacy SR and an NG9-1-1 Emergency Services Network. An ingress LSRG allows emergency originations routed via a legacy SR to terminate on an NG9-1-1 PSAP, as well as allowing calls routed via an NG9-1-1 Emergency Services Network to terminate to a legacy PSAP that is served by an LPG or egress LSRG. An egress LSRG allows emergency calls that are routed via an NG9-1-1 Emergency Services Network to be delivered to a legacy PSAP that is connected to a legacy SR. The LSRG also facilitates transfers of calls between PSAPs that are served by legacy SRs and PSAPs that are served by NG9-1-1 Emergency Services Networks, regardless of the type of network from which the 9-1-1 call originated.

B.2.1 Transitional NG9-1-1 Architectures Involving Legacy PSAPs

During transition, NG9-1-1 architectures may include LPGs or egress LSRGs to support the delivery of 9-1-1 calls to legacy PSAPs. The SIP signaling delivered to an LPG or egress LSRG by an NG9-1-1 Emergency Services Network will contain the same information as the SIP signaling that is delivered to an NG9-1-1 PSAP, including location information (by reference or by value) and callback information. In the case of an LPG, the SIP signaling will be interworked to the Traditional MF or E-MF signaling that is appropriate for the interface over which the call will be delivered to the legacy PSAP. Location information and other non-location information received by the LPG will be provided to the legacy PSAP outside of the call setup process via a legacy ALI interface. In transitional architectures involving LPGs, an attestation level of “A”, “B”, or “C” and a verification status of “TN-Validation-Passed”, “TN-Validation-Failed”, or “No-TN-Validation” may be received by the LPG in incoming SIP signaling. Since, by design, an LPG will interface to a legacy PSAP for 9-1-1 call delivery in the same way as an SR does, the same considerations apply to delivering attestation level and verification status information over MF call delivery interfaces using this transitional architecture as for a legacy E9-1-1 architecture. ATIS-0500046 [Ref 1] describes the use of the legacy ALI interface between the LPG and the legacy PSAP as a viable option for delivering attestation level and verification status information to legacy PSAPs associated with 9-1-1 calls that are routed via LPGs.

An egress LSRG takes the SIP signaling received from an NG9-1-1 Emergency Services Network and generates SS7 signaling associated with 9-1-1 calls toward a legacy SR. An egress LSRG must also be capable of processing location queries steered to it by an ALI system. If the NG9-1-1 Emergency Services Network and other upstream networks support call authentication, it is expected that the SIP signaling delivered to an egress LSRG will include an Identity header containing attestation information, and a P-Asserted-Identity or From header containing a “verstat” parameter. If the egress LSRG supports the SHAKEN OOB call authentication mechanism then, strictly speaking, it would be responsible for passing the SIP INVITE to an STI-OOBS so that the PASSporT information can be published to an STI-CPS, and the legacy SR would be responsible for also interacting with an STI-OOBS via an STI-IWF to retrieve the PASSporT from the STI-CPS. However, the SHAKEN OOB mechanism does not consider architectures like those involving egress LSRGs, where the verification is performed by an upstream network (i.e., the NG9-1-1 Emergency Services Network) and it is the role of an element in the terminating network (in this case the E9-1-1 Network) to pass the SHAKEN information through a TDM network to the called party over an MF interface. Although the egress LSRG may receive a PASSporT and “verstat” information via SIP signaling from the NG9-1-1 Emergency Services Network, and is responsible for interworking between SIP and SS7, there is no value in having the egress LSRG publish PASSporT information to an STI-CPS because it will not be possible to enhance SR functionality to support the retrieval of PASSporTs from an STI-CPS, or to enhance the MF call delivery interface to support the delivery of attestation and verification status information to a legacy PSAP.

The Extending STIR/SHAKEN Over TDM call authentication mechanism will allow an egress LSRG to map the attestation level and “verstat” information received in the SIP signaling from the NG9-1-1 Emergency Services Network to an appropriate Screening Indicator value for conveyance to the SR. However, once the call is delivered to the SR, the same issues apply as for the E9-1-1 architecture regarding delivering attestation level and verification status information to the legacy PSAP with the call using MF signaling.

Similarly, an egress LSRG could encode the “shaken” PASSporT information received in an Identity header in an SS7 UUI parameter, but even if the SR was capable of receiving and processing that information (which would likely require updates to the processing at the SR), the same issues would apply regarding the ability to deliver attestation level and verification status information to the legacy PSAP over an MF call delivery interface. ATIS-0500046 [Ref

1] describes a mechanism by which responses to location requests steered to an egress LSRG by an ALI system can provide a viable means of conveying attestation level and verification status information to legacy PSAPs.

B.2.2 Transitional NG9-1-1 Architectures that include an LNG

In a transitional NG9-1-1 architecture that includes an LNG, the presence of the gateway should not have any impact on the way that the legacy originating network processes a 9-1-1 call. The only difference is that the trunk group over which the call is routed is connected to an LNG rather than an SR. When considering transitional NG9-1-1 architectures that include an LNG, it is necessary to address two scenarios: one where the LNG is operated by the OSP and one where the LNG is operated by the NG9-1-1 Emergency Services Network provider. It is more typical for the NG9-1-1 Emergency Services Network provider to operate the LNG in actual implementations.

If the SHAKEN OOB call authentication solution is applied to an architecture that includes an LNG that is operated by the NG9-1-1 Emergency Services Network provider, the approach would most closely resemble the architecture illustrated in Figure 8-7 of ATIS-1000096 [Ref 4]. The impacts on the legacy originating network would be the same as described for the E9-1-1 architecture, namely that the 9-1-1 call would be routed from a wireline end office or MSC to an STI-IWF. The STI-IWF would be responsible for interacting with an STI-AS, which would create a "shaken" PASSporT for the call and return it to the STI-IWF. The STI-IWF would forward the SIP INVITE with the PASSporT to the STI-OOBS which would publish it to an STI-CPS. Upon receiving the 9-1-1 call from the TDM originating network, the LNG would be responsible for performing all of the expected SS7-SIP interworking and NG9-1-1-specific call processing associated with the 9-1-1 call, but in addition, the LNG would need to be enhanced to interact with an STI-OOBS (by forwarding it the SIP INVITE message prior to sending the INVITE to the NG9-1-1 Emergency Services Network) to support retrieval of the "shaken" PASSporT from the STI-CPS. Since the SIP INVITE message forwarded to it by the LNG would not contain an Identity header with a PASSporT, the STI-OOBS would need to create a JWT, then pass that along with the calling and called party information to the STI-CPS. Upon receiving the "shaken" PASSporT from the STI-CPS, the STI-OOBS would return the SIP INVITE message to the LNG with the "shaken" PASSporT populated in an Identity header. The LNG would then forward the SIP INVITE with the Identity header to the NG9-1-1 Emergency Services Network, which would be responsible for applying SHAKEN verification procedures to the call.

If the LNG is operated by the OSP, the SHAKEN OOB architecture could be modified so that the LNG would replace the STI-IWF in the originating network. Rather than having the STI-IWF interact with the STI-AS, the LNG could instead interact with the STI-AS (after performing all the call processing required of an LNG, but before forwarding the SIP INVITE to the NG9-1-1 Emergency Services Network), by forwarding it the SIP INVITE message. The STI-AS would perform normal SHAKEN authentication and create the "shaken" PASSporT. The STI-AS would then populate the "shaken" PASSporT in an Identity header and return it to the LNG in a SIP INVITE message. While the OOB SHAKEN call authentication mechanism assumes that the STI-IWF will forward the SIP INVITE with the "shaken" PASSporT to the STI-OOBS so that the "shaken" PASSporT can be published to the STI-CPS, the LNG could just pass the SIP INVITE with the Identity header to the NG9-1-1 Emergency Services Network, which is SIP/SHAKEN-capable, without having the PASSporT published to the STI-CPS, since functional elements in the NG9-1-1 Emergency Services Network, NG9-1-1 PSAPs, and any gateway elements on the egress side of the NG9-1-1 Emergency Services Network (i.e., LPG or egress LSRG) would be capable of receiving and processing the PASSporT information provided in the Identity header, and SRs, if present in the call path, would not be capable of retrieving PASSporTs from an STI-CPS.

If the LNG is operated by the NG9-1-1 Emergency Services Network provider, and the Extending STIR/SHAKEN Over TDM call authentication mechanism is applied, then the LNG could be enhanced to map the received Screening Indicator value to an Identity header containing a PASSporT with an attestation level of "A" and include a "verstat" value of "TN-Validation-Passed" in the P-Asserted-Identity header or From header (since all Screening Indicator values associated with legacy 9-1-1 calls will map to these values). Likewise, the LNG could use the trunk group over which it received the 9-1-1 call to determine the attestation level and "verstat", which would accommodate calls delivered to the LNG via MF trunk groups. It is expected that any trunk group over which a 9-1-1 call is delivered by a legacy originating network to the LNG would have an attestation level of "A" and a "verstat" value of "TN-Validation-Passed" associated with it. In addition to populating the attestation level in the Identity header and the "verstat" value, the LNG would also have to include an STI certificate in the Identity header, signing the PASSporT information. In this case the STI certificate would be associated with the NG9-1-1 Emergency Services Network provider. Since, in this scenario, the LNG is operated by the NG9-1-1 Emergency Services Network provider, routing the 9-1-1 call from the LNG to an element in the NG9-1-1 Emergency Services Network

would be viewed as intranetwork routing, so SHAKEN verification (e.g., by having the downstream element in the NG9-1-1 Emergency Services Network interact with the STI-VS) would not need to be performed.

If the Extending STIR/SHAKEN Over TDM approach was in use and the LNG is operated by the OSP, then the processing at the LNG would be the same as described above, with the LNG mapping the Screening Indicator or incoming trunk group to an "A" attestation and "verstat" value of "TN-Validation-Passed". As above, the LNG would then create an Identity header with a signed PASSporT and populate the "verstat" in the P-Asserted-Identity header (or From header, if no P-Asserted-Identity header is to be populated). In this case, the STI certificate in the PASSporT would be associated with the OSP. Routing the call from the LNG to an NG9-1-1 Emergency Services Network would be viewed as internetwork routing, and as a result, any "verstat" information populated by the LNG would be stripped out by the Border Control Function (BCF)/Interconnection Border Control Function (IBCF) on the ingress side of the NG9-1-1 Emergency Services Network, and the NG9-1-1 Emergency Services Network would be expected to interact with an STI-VS to perform SHAKEN verification.

As indicated above, the SS7 signaling associated with a 9-1-1 call is not expected to include a UUI parameter, so it is not expected that the mechanism in which a PASSporT is encoded in an ISUP UUI parameter would apply to a transitional NG9-1-1 architecture that includes an LNG.

B.2.3 Transitional NG9-1-1 Architectures that include an Ingress LSRG

An ingress LSRG has many of the same characteristics as an LNG, except that it receives 9-1-1 calls over SS7 trunk groups from legacy SRs. In considering the application of the SHAKEN OOB call authentication solution to 9-1-1 calls that are routed via ingress LSRGs, the impacts on the legacy originating network would be the same as for the E9-1-1 and LNG scenarios. However, in this case the call would traverse an SR and be delivered to the ingress LSRG over an SS7 trunk group with essentially the same information that the SR received from the end office/MSC. In this scenario, the LSRG would be responsible for performing SS7-SIP interworking and NG9-1-1-specific call processing associated with the 9-1-1 call. In the context of the SHAKEN OOB call authentication solution, the LSRG would need to be enhanced to interact with the STI OOBS (by forwarding it the SIP INVITE message prior to sending it to the NG9-1-1 Emergency Services Network) to support retrieval of the "shaken" PASSporT from the STI-CPS. Since the SIP INVITE message forwarded to it by the LSRG would not contain an Identity header with a PASSporT, the STI-OOBS would need to create a JWT, then pass that along with the calling and called party information to the STI-CPS. Upon receiving the "shaken" PASSporT from the STI-CPS, the STI-OOBS would return the SIP INVITE message to the ingress LSRG with the "shaken" PASSporT populated in an Identity header. The ingress LSRG would then forward the SIP INVITE with the Identity header to the NG9-1-1 Emergency Services Network, which would be responsible for applying SHAKEN verification procedures to the call.

In considering the application of the Extending STIR/SHAKEN Over TDM call authentication mechanism to a transitional architecture involving an ingress LSRG, the LSRG could be responsible for mapping the received Screening Indicator value to an Identity header containing an attestation level of "A" and populating a "verstat" value of "TN-Validation-Passed" (since all Screening Indicator values associated with legacy 9-1-1 calls will map to these values) in the P-Asserted-Identity header or From header. In addition to populating the attestation level in the Identity header and the "verstat" value in the P-Asserted-Identity or From header, the LSRG would also have to include a certificate in the Identity header, signing the PASSporT information. In this case the certificate would be associated with the E9-1-1 System Service Provider (who is assumed to be responsible for operating the ingress LSRG). Any "verstat" information populated by the LSRG would be stripped out by the BCF/IBCF on the ingress side of the NG9-1-1 Emergency Services Network, and the NG9-1-1 Emergency Services Network would be expected to interact with the STI-VS to have SHAKEN verification procedures applied to the PASSporT information in the Identity header.

Considerations related to the use of the call authentication mechanism where a "shaken" PASSporT is embedded in an SS7 UUI parameter are the same for an ingress LSRG scenario as for the LNG scenario. SS7 signaling associated with a 9-1-1 call is not expected to include a UUI parameter.