ATIS-1000106

Viability of Non-IP Call Authentication Standards

TECHNICAL REPORT

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

ATIS-1000106, *Viability of Non-IP Call Authentication Standards*

Published by

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

ATIS-1000106

ATIS Technical Report on

Viability of Non-IP Call Authentication Standards

Alliance for Telecommunications Industry Solutions

Approved December 2, 2024

Abstract

While the standards developed by the Non-IP Call Authentication Task Force may be technically feasible and implementable on a bilateral basis or under controlled conditions, none of the NIPCA approaches can be used ubiquitously in the network without concern. This Technical Report does a deep dive on the viability of implementing specific NIPCA solution options that traverse TDM network elements and coexistence with each other and integration with the SHAKEN solution in IP networks.

.

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

ATIS Technical Report on –

Viability of Non-IP Call Authentication Standards

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

ATIS-1000097, *Alternatives for Call Authentication for Non-IP Traffic* [Ref 5], provides a framework to evaluate the non-IP call authentication standards:

- ATIS-1000095, *Extending STIR/SHAKEN over TDM* [Ref 3],
- ATIS-1000096, *Out-of-Band PASSporT Transmission Involving TDM Networks* [Ref 4], and
- ATIS-1000105, *Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM* [Ref 6]

While these standards may be technically feasible, the purpose of this Technical Report is to help implementers understand the challenges they would face to implement these standards.

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-1000073, *Technical Report on Use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information*.[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-1000097, *Alternatives for Call Authentication for Non-IP Traffic.*[1]

[Ref 6] ATIS-1000105, *Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM.*[1]

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

[Ref 7] IETF RFC 4949, *Internet Security Glossary, Version 2.*[2]

[Ref 8] IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates*.[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.

Authorized Service Provider: A service provider that a Secure Telephone Identity Governance Authority (STI-GA) authorizes to obtain Service Provider Code (SPC) Tokens.

(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 7]). 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 (RFC 4949 [Ref 7]).

Public Key: The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography (RFC 4949 [Ref 7]).

Public Key Infrastructure (PKI): The set of hardware, software, personnel, policy, and procedures used by a Certification Authority (CA) to issue and manage certificates (RFC 4949 [Ref 7]).

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

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

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

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

Signature: Created by signing the message using the private key. It ensures the identity of the sender and the integrity of the data (RFC 4949 [Ref 7]).

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

[2] Available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org/ >.

3.2 Acronyms & Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
CA	Certification Authority
CDR	Call Detail Record
CNAM	Calling Name
CPS	Call Placement Service
CRL	Certificate Revocation List
CVT	Call Validation Treatment
GW	Gateway
HTTP	Hypertext Transfer Protocol
IAM	Initial Address Message
IBCF	Interconnection Border Control Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IN	Intelligent Network
IP	Internet Protocol
ISUP	Integrated Services Digital Network User Part
MFA	Multi-Factor Authentication
MGCF	Media Gateway Control Function
NNI	Network-to-Network Interface
OSP	Originating Service Provider
PASSporT	Personal ASSertion Token
PKI	Public Key Infrastructure
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
RPH	Resource-Priority Header
SBC	Session Border Controller
SCP	Service Control Point
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SP	Service Provider
SPC	Service Provider Code
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-GA	Secure Telephone Identity Governance Authority
STI-IWF	Secure Telephone Identity InterWorking Function
STI-OOBS	Secure Telephone Identity Out-of-Band Service
STI-PA	Secure Telephone Identity Policy Administrator
STI-VS	Secure Telephone Identity Verification Service
STIR	Secure Telephone Identity Revisited
STP	Signal Transfer Point
TDM	Time Division Multiplexing
TN	Telephone Number
TrGW	Transition GateWay
TSP	Terminating Service Provider
URI	Uniform Resource Identifier
UUI	User-to-User Information
VoIP	Voice over Internet Protocol

4 Implementation Viability

The following section describes viability considerations for implementing each of the non-IP call authentication standards. Readers of these subsections are expected to be familiar with the relevant non-IP call authentication standard and ATIS-1000097 [Ref 5].

4.1 ATIS-1000095, Extending STIR/SHAKEN over TDM

4.1.1 Deployment in Existing TDM-based Networks

Implementing either an ISUP-Screening-Indicator-based approach to conveying attestation values or an ISUP User-to-User Information (UUI) parameter approach for encoding and decoding PASSporT information may require software and system updates to existing TDM systems. In many networks, the TDM network elements have been in service for many years and contain older technology. Additional development to such systems may be impractical, or vendor support may not be available. Possible methods of implementation are to replace the existing systems with later-generation TDM-based systems that might be extensible to the new functionality or to route calls received/sent via TDM NNIs through an interworking function that can support the logic. Both these methods would require additional capital and/or operating resources to deploy and support the function.

4.1.2 ISUP Parameters Already in Use

In some networks, the ISUP Screening Indicator and User-to-User Information (UUI) parameters may already be in use and contain values not compatible with ATIS-1000095 [Ref 3]. Therefore, either the existing information contained in the ISUP Screening Indicator and/or UUI parameter must be overwritten to utilize ATIS-1000095 [Ref 3], or ATIS-1000095 cannot be used. See ATIS-1000073, *Technical Report on Use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information* [Ref 1], for additional information.

4.1.3 Bilateral/Multilateral Agreements

The ISUP Screening Indicator parameter is not cryptographically protected. Therefore, to ensure the meaning of the indicator as a conveyor of attestation information across one or more TDM NNI hops, bilateral agreements need to exist between each pair of service providers that interconnect via TDM NNIs or multilateral agreements need to exist among all providers that interconnect through a given tandem network.

4.1.4 Validity of Authentication Information

The use of ISUP Screening Indicator to convey an attestation value across TDM NNIs does not preserve the identity of the Originating Service Provider (OSP) or the OSP's cryptographic signature. The use of ISUP UUI parameter to convey PASSporT information only preserves the identity of the OSP and the OSP's cryptographic signature in the cases where an original "shaken" PASSporT is directly encoded in the UUI parameter. The cases where information from multiple PASSporTs is combined and a new signature is generated with an intermediate provider's credentials does not preserve the identity or original cryptographic signature of the OSP.

4.2 ATIS-1000096, Out-of-Band PASSporT Transmission Involving TDM Networks

4.2.1 Sequential Versus Concurrent Publish

When publishing or republishing PASSporT(s), the STI-OOBS may set a timer and wait for a response from the STI-CPS or the timer to expire before the service provider sends the call downstream. If the timer is non-zero, call setup time may be increased. If the timer is zero or the timer expires, it is possible for a service provider to attempt to retrieve the PASSporT(s) from an STI-CPS before the PASSporT(s) have been published to that STI-CPS. This could result in the call that was authenticated appearing as if it was unauthenticated (which is no different than how the call appears without Out-of-Band SHAKEN).

4.2.2 PASSporTs Accessible by Any Authorized Service Provider

STI-CPS access is restricted to only Authorized Service Providers. However, an Authorized Service Provider could query an STI-CPS to access the PASSporT(s) for a call that the service provider is not processing. To minimize the risk of a service provider accessing PASSporTs for calls that the service provider is not processing, the STI-CPS API requires the service provider to provide both the calling number and called number of the call, to make the request within a short time window of when the call occurs, and to sign the request with their STI certificate. These requirements provide a record of a service provider's access and make it more difficult for rogue service providers to query an STI-CPS to access the PASSporT(s) for a call they are not processing. However, these requirements do not fully mitigate malicious or abusive treatment of the retrieved PASSporT information.

4.2.3 PASSporT Collisions

If there are two calls with the same calling number and called number that occur within the STI-CPS PASSporT retention window, it is possible for the wrong PASSporT to be returned for a given call. The security mitigations suggested in ATIS-1000097 [Ref 5], analysis of call volume with same calling and called number and retaining PASSporT(s) for as short a time as practical, are not robust for situations with two entities known to have frequent calls (e.g., between a bank branch and its headquarters). To induce a collision, an attacker may not need to place a volume of calls that could be reliably detected by volumetric traffic monitoring.

ATIS-1000096 [Ref 4] leaves collision handling to STI-CPS local policy, which raises the potential for inconsistent local policies in STI-CPS implementations. Because PASSporTs are replicated to each STI-CPS, the overall STI-CPS network may be impacted by a single STI-CPS with a weak local policy.

To mitigate the risk of an attacker's call retrieving a PASSporT with a higher attestation level than it should, STI-CPS local policy needs to be to retain the PASSporT with the lowest attestation. Meaning that if an attacker is able to cause a collision, the attacker would not be elevating the attestation level of the attacker's call but decreasing the attestation level of the legitimate call.

4.3 ATIS-1000105, Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM

4.3.1 Ubiquitous Implementation

ATIS-1000105 [Ref 6] must be implemented by every service provider with TDM NNIs in the call path of a given call for the PASSporT(s) associated with that call to be delivered to the terminating service provider.

4.3.2 Increased Call Setup Time

When publishing or retrieving PASSporT(s), the STI-OOBS sets a timer and waits for a response from the STI-CPS or the timer to expire before the service provider sends the call downstream. Call setup time may be increased.

4.3.3 PASSporT Collisions

ATIS-1000105 [Ref 6] describes a procedure for an STI-CPS to disambiguate multiple PASSporT publishes received in close proximity with the same calling and called number. In some cases, an STI-CPS may not be able to determine the authentication information that corresponds to a retrieve request initiated by an STI-OOBS when receiving a specific call at a TDM interface. Per the procedure in this case, no PASSporTs are retrieved and the PASSporT(s) are not passed end-to-end from the originating network to the terminating network. While this can occur only under specific call routing or attack conditions, the frequency of these conditions is not yet known.

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.