



ATIS-100096

ATIS Standard on -

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



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

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

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

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.

Published by

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

Copyright © 2021 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

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

Alliance for Telecommunications Industry Solutions

Approved July 15, 2021

Abstract

The Signature-based Handling of Asserted information using toKENs (SHAKEN) framework enables an authorized Voice over Internet Protocol (VoIP) service provider to deliver a cryptographically protected assertion that the calling user is authorized to use the calling telephone number to a called user via Session Initiation Protocol (SIP) signaling that the calling user is authorized to use the calling telephone number. This specification extends the SHAKEN framework to enable service providers using Time Division Multiplexing (TDM) signaling to participate in the SHAKEN ecosystem without placing any new requirements on authorized SHAKEN service providers.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. International Telecommunication Union Telecommunication Sector (ITU-T) and U.S. ITU Radiocommunication Sector (ITU-R) Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

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

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

At the time it approved this standard, the PTSC had the following leadership:

M. Dolly, PTSC Chair

V. Shaikh, PTSC Vice Chair

Table of Contents

1	SCOPE, PURPOSE, & APPLICATION	1
1.1	SCOPE.....	1
1.2	PURPOSE & APPLICATION	1
2	NORMATIVE REFERENCES	2
3	DEFINITIONS, ACRONYMS, & ABBREVIATIONS	2
3.1	DEFINITIONS.....	3
3.2	ACRONYMS & ABBREVIATIONS	4
4	OUT-OF-BAND PASSPORT TRANSMISSION INVOLVING TDM NETWORKS	6
5	STI-OOBS	6
6	STI-IWF	7
7	STI-CPS	7
7.1	HEALTH CHECK	7
7.1.1	<i>HTTP Request</i>	8
7.1.2	<i>Success HTTP Response</i>	8
7.1.3	<i>Error HTTP Response</i>	8
7.2	PUBLISH PASSPORT(S)	8
7.2.1	<i>HTTP Request</i>	11
7.2.2	<i>Success HTTP Response</i>	12
7.2.3	<i>Error HTTP Response</i>	12
7.3	RETRIEVE PASSPORT(S)	12
7.3.1	<i>HTTP Request</i>	14
7.3.2	<i>Success HTTP Response</i>	14
7.3.3	<i>Error HTTP Response</i>	15
8	CALL SCENARIO EXAMPLES	15
8.1	TRANSIT PROVIDER PUBLISH – TRANSIT PROVIDER RETRIEVE.....	15
8.2	TRANSIT PROVIDER PUBLISH – VOIP SERVICE PROVIDER RETRIEVE.....	16
8.3	TRANSIT PROVIDER PUBLISH – TDM SWITCH RETRIEVE	16
8.4	VOIP SERVICE PROVIDER PUBLISH - TRANSIT PROVIDER RETRIEVE	17
8.5	VOIP SERVICE PROVIDER PUBLISH - VOIP SERVICE PROVIDER RETRIEVE	17
8.6	VOIP SERVICE PROVIDER PUBLISH - TDM SWITCH RETRIEVE	18
8.7	TDM SWITCH PUBLISH - TRANSIT PROVIDER RETRIEVE	18
8.8	TDM SWITCH PUBLISH - VOIP SERVICE PROVIDER RETRIEVE	19
8.9	TDM SWITCH PUBLISH - TDM SWITCH RETRIEVE	19
9	CROSS-BORDER	20
9.1	SIP SIGNALING.....	20
9.2	TDM SIGNALING.....	21

Table of Figures

FIGURE 7-1:	STI-CPS PROCESSING LOGIC.....	11
FIGURE 8-1:	TRANSIT PROVIDER PUBLISH – TRANSIT PROVIDER RETRIEVE	15
FIGURE 8-2:	TRANSIT PROVIDER PUBLISH – VOIP SERVICE PROVIDER RETRIEVE.....	16
FIGURE 8-3:	TRANSIT PROVIDER PUBLISH – TDM SWITCH RETRIEVE.....	16
FIGURE 8-4:	VOIP SERVICE PROVIDER PUBLISH – TRANSIT PROVIDER RETRIEVE.....	17
FIGURE 8-5:	VOIP SERVICE PROVIDER PUBLISH – VOIP SERVICE PROVIDER RETRIEVE	17
FIGURE 8-6:	VOIP SERVICE PROVIDER PUBLISH – TDM SWITCH RETRIEVE	18
FIGURE 8-7:	TDM SWITCH PUBLISH – TRANSIT PROVIDER RETRIEVE.....	18
FIGURE 8-8:	TDM SWITCH PUBLISH – VOIP SERVICE PROVIDER RETRIEVE	19

ATIS-1000096

FIGURE 8-9: TDM SWITCH PUBLISH – TDM SWITCH RETRIEVE 19
FIGURE 9-1: TDM NETWORK WITH OUTGOING CROSS-BORDER SIP SIGNALING 20
FIGURE 9-2: TDM NETWORK WITH INCOMING CROSS-BORDER SIP SIGNALING 21
FIGURE 9-3: TDM NETWORKS WITH CROSS-BORDER SIP SIGNALING 21
FIGURE 9-4: TDM SIGNALING FOR CROSS-BORDER TRAFFIC..... 22
FIGURE 9-5: TDM SIGNALING FOR CROSS-BORDER TRAFFIC FROM “B” TO “A” 22
FIGURE 9-6: TDM SIGNALING FROM A SIP NETWORK 23
FIGURE 9-7: TDM SIGNALING BETWEEN SIP NETWORKS 23

ATIS Standard on –

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

Out-of-Band PASSporT Transmission Involving TDM Networks

1 Scope, Purpose, & Application

1.1 Scope

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

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

Within the specification, cryptographically signed PASSporT(s) are exchanged out-of-band, that is, separate from the telephone network signaling. The mechanism of exchanging PASSporT(s) out-of-band is based on draft-ietf-stir-servprovider-oob-01, *Out-of-Band STIR for Service Providers*.

It is recommended that ATIS-1000097, *Technical Report on Alternatives for Caller Authentication for Non-IP Traffic*, evaluating the viability of implementing this call authentication mechanism for TDM networks, be considered along with this document.

1.2 Purpose & Application

The SHAKEN framework provides a set of tools that enable verification of the calling party's legitimate right to use a calling telephone number for a call. The SHAKEN protocol specification ATIS-1000074.v002, *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)*, describes an authentication mechanism that can be invoked by the Originating Service Provider (OSP) to authenticate itself at a transit switch as the service provider responsible for the call origination and to "attest" to the legitimacy of the calling telephone number associated with a call. A cryptographic signature across the call parameters protects the integrity of the SIP parameters and the OSP's call markings. In the SHAKEN framework, the OSP's Secure Telephone Identity Authentication Service (STI-AS) creates a PASSporT and inserts this PASSporT in a SIP Identity header per RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol*. The SIP INVITE is then routed over the network-to-network interface (NNI) through the standard inter-domain routing configuration.

TDM switching elements, in today's public switched telephone networks, do not support the Identity header necessary to interwork with SIP. Thus, the Identity header may fail to arrive at the Terminating Service Provider (TSP) network's transit switch for verification by their Secure Telephone Identity Verification Service (STI-VS) because the call may not be transmitted using SIP signaling end to end. *Out-of-Band PASSporT Transmission Involving TDM Networks* may remedy this problem by enabling service providers to exchange PASSporT(s) through a Secure Telephone Identity Call Placement Service (STI-CPS). However, this is predicated on certain TDM interworking functions as identified later in this document. SHAKEN authentication, verification, and Public Key Infrastructure (PKI) operation remains the same.