ATIS-1000085

ATIS Standard on Signature-based Handling of Asserted information using ToKENs (SHAKEN):

SHAKEN Support of "div" PASSporT

JOINT STANDARD

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.

The SIP Forum is a leading IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations; interoperability testing events and special workshops, educational activities, and general promotion of IP communications standards, services, and technology for service provider, enterprise, and governmental applications. The SIP Forum is also the producer of the annual SIPNOC conferences (for SIP Network Operators Conference), focused on the technical requirements of the service provider community. One of the Forum's technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation that provides detailed guidelines for direct IP peering and interoperability between IP PBXs and SIP-based service provider networks, and the SIPconnect Certification Testing Program, a unique certification testing program that includes a certification test suite and test platform, and an associated "SIPconnect Certified" logo program that provides an official "seal of certification" for companies products and services that have officially achieved conformance with the SIPconnect specification. Other important Forum initiatives include work in security, SIP and IPv6, and IP-based Network-to-Network Interconnection (IP-NNI). For more information about all SIP Forum initiatives, please visit:

< http://www.sipforum.org/ >

ATIS-1000085, ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN): SHAKEN Support of "div" PASSporT

Is an ATIS & SIP Forum Joint Standard developed by the **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **Technical Working Group (TWG)** under the **SIP Forum**.

Published by

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

SIP Forum LLC
733 Turnpike Street, Suite 192
North Andover, MA 01845

ATIS-1000085

ATIS Standard on

Signature-based Handling of Asserted information using toKENs (SHAKEN):
SHAKEN Support of "div" PASSporT

Alliance for Telecommunications Industry Solutions

Approved February 27, 2019

Abstract

The base SHAKEN specification provides replay-detection mechanisms to identify cases where a malicious entity attempts to masquerade as another user by replaying parts of a legitimate INVITE request. However, these mechanisms don't cover cases where the INVITE is replayed within the short Date freshness window. This technical report describes how the mechanisms defined by [draft-ietf-stir-passport-divert] can be integrated within the SHAKEN framework to close this replay attack window.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, 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 SIP Forum is an IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations, the SIPit, SIPconnect-IT, and RTCWeb-it interoperability testing events, special workshops, educational seminars, and general promotion of SIP in the industry. The SIP Forum is also the producer of the annual SIP Network Operators Conference (SIPNOC), focused on the technical requirements of the service provider community. One of the Forum's notable technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation for direct IP peering and interoperability between IP Private Branch Exchanges (PBXs) and SIP-based service provider networks. Other important Forum initiatives include work in Video Relay Service (VRS) interoperability, security, Network-to-Network Interoperability (NNI), and SIP and IPv6.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005, and/or to the SIP Forum, 733 Turnpike Street, Suite 192, North Andover, MA, 01845.

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.

The **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **SIP Forum Technical Working Group (TWG)** was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

ATIS Standard on –

Signature-based Handling of Asserted information using toKENs (SHAKEN): SHAKEN Support of "div" PASSporT

1 Scope & Purpose

1.1 Scope

This document describes how the PASSporT "div" extension defined in [draft-ietf-stir-passport-divert] can be utilized within the SHAKEN framework to provide end-to-end SHAKEN authentication for calls that are retargeted by features such as call-forwarding.

1.2 Purpose

The SHAKEN authentication service in an originating network asserts two telephone numbers (TNs) in the "shaken" PASSporT; the number identifying the originator of the call in the "orig" claim, and the number identifying the destination of the call in the "dest" claim. The originating number is included to cryptographically assert that the calling TN identifies the calling user. The destination TN is included to provide protection from replay attacks where a man-in-the-middle replays a valid Identity header in a new INVITE sent to a different destination TN. In addition, PASSporT contains an "iat" claim that specifies the timestamp that the PASSporT was created. Including the "iat" claim further limits the time associated with a potential replay of the specific "orig" and "dest" claims, to prevent a potential malicious flood of validated calls to the same destination TN.

There are a number of call features that can legitimately retarget an INVITE request to a new destination. Examples include the various forms of call forwarding, where a call is diverted from the original destination to a new forward-to destination, simultaneous ringing, where a call to the dialed TN is simultaneously offered to additional TN(s), and toll-free number routing, where the dialed toll-free TN is replaced with its assigned routing TN. These features break the end-to-end call authentication model of SHAKEN/STIR since the verification service in the terminating network is unable to distinguish between an INVITE that has been legitimately retargeted, and an INVITE that has been maliciously replayed within the "iat" freshness window.

This document describes how the mechanisms defined in [draft-ietf-stir-passport-divert] enable SHAKEN to authenticate each retargeted leg of the call, so that a terminating network verification service has sufficient information to distinguish between an INVITE that has been legitimately retargeted, and an INVITE that has been maliciously replayed within the "iat" freshness window.

1.2.1 Document Organization

Clause 4 provides an informative overview of the PASSporT "div" extension, and how it enables end-to-end delivery of SHAKEN authentication information for retargeted calls.

Clause 5 specifies the normative requirements to add support [draft-ietf-stir-passport-divert] to SHAKEN.

Annex A describes how the normative requirements in Clause 5 can be applied to a sample of real-world deployment use cases.

Annex B shows an example of a SIP Identity header containing a "div" PASSporT.