**A****TIS-1000XXX**

ATIS Standard on

**Signature-based Handling of Asserted information using toKENs (SHAKEN):
Calling Name and Rich Call Data Handling Procedures**

**Alliance for Telecommunications Industry Solutions**

Approved Month 00, 2019

**Abstract**

Signature-based Handling of Asserted information using toKENs (SHAKEN) is an industry framework for managing and deploying Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and verification of the telephone identity and other information in an IP-based service provider voice network. This specification expands the SHAKEN framework, introducing a mechanisms for authentication, verification, and transport of CNAM, Rich Call Data and how they a handled in various origination and termination procedures.

**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.

**Revision History (draft spec)**

| **Date** | **Version** | **Description** | **Editor** |
| --- | --- | --- | --- |
| 04/29/2019 | 0.1 | IPNNI-2019-00024R001 (2019 baseline draft)  | D. Hancock |
| 02/04/2020 | 0.2 | IPNNI-2020-00025R001 (2020 baseline draft)  | D. Hancock |
| 03/17/2020 | 0.3 | IPNNI-2020-00052R000 | D. Hancock |
| 04/29/2020 | 0.4 | IPNNI-2020-00080R002 | D. Hancock |
| 06/29/2020 | 0.5 | IPNNI-2020-00095R002 | D. Hancock |

Table of Contents

[**ATIS-1000XXX** i](#_Toc44349970)

[ATIS Standard on i](#_Toc44349971)

[**Signature-based Handling of Asserted information using toKENs (SHAKEN): Calling Name and Rich Call Data Handling Procedures** i](#_Toc44349972)

[**Alliance for Telecommunications Industry Solutions** i](#_Toc44349973)

[**Abstract** i](#_Toc44349974)

[Table of Figures iii](#_Toc44349975)

[1 Scope & Purpose 1](#_Toc44349976)

[1.1 Scope 1](#_Toc44349977)

[1.2 Purpose 1](#_Toc44349978)

[2 Normative References 1](#_Toc44349979)

[3 Definitions, Acronyms, & Abbreviations 2](#_Toc44349980)

[3.1 Definitions 2](#_Toc44349981)

[3.2 Acronyms & Abbreviations 2](#_Toc44349982)

[4 Overview 4](#_Toc44349983)

[4.1 SHAKEN CNAM and RCD Model Overview 4](#_Toc44349984)

[5 SHAKEN CNAM and RCD Framework Definition 5](#_Toc44349985)

[5.1 "rcd" PASSporT claim construction overview 5](#_Toc44349986)

[5.1.1 Traditional CNAM using "nam" 5](#_Toc44349987)

[5.1.2 RCD using "jcd" with an embedded jCard 6](#_Toc44349988)

[5.1.3 RCD using "jcl" with a URL to jCard 7](#_Toc44349989)

[5.1.4 RCD using "crn" to convey call reason 7](#_Toc44349990)

[5.1.5 Integrity Protection of Rich Call Data 8](#_Toc44349991)

[5.2 RCD Authentication and Verification Procedures 8](#_Toc44349992)

[5.2.1 RCD Authentication 8](#_Toc44349993)

[5.2.2 RCD Verification 9](#_Toc44349994)

[5.2.3 Including RCD PASSporT in retargeted INVITE Request 10](#_Toc44349995)

# Table of Figures

**No table of figures entries found.**

# Scope & Purpose

## Scope

This specification expands the SHAKEN framework, introducing mechanisms for authentication, verification, and transport of CNAM, Rich Call Data and how they a handled in various origination and termination procedures.

## Purpose

To provide a framework for delivering authenticated calling name and rich call data for display to the called user.

# Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. 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.

ATIS-1000074, *Signature-based Handling of Asserted Information using Tokens (SHAKEN).*[[1]](#footnote-1)

ATIS-1000067, *IP NGN Enhanced Calling Name (eCNAM)*.1

ATIS-1000080, *SHAKEN: Governance Model and Certificate Management*.1

ATIS-1000085, *SHAKEN: SHAKEN Support of "div" PASSporT*.1

ATIS delegate-cert document, *Delegate Certificates*.1

draft-wendt-sipcore-callinfo-rcd, *SIP Call-Info Parameters for Rich Call Data*.2

draft-ietf-stir-passport-rcd, *PASSporT Extension for Rich Call Data.*2

RFC 3261, *SIP: Session Initiation Protocol.*2

RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks.*2

RFC 3966, *The tel URI for Telephone Numbers*.2

RFC 7095, *jCard: The JSON Format for vCard*.2

RFC 7515, *JSON Web Signatures (JWS).*2

RFC 7516, *JSON Web Algorithms (JWA).*2

RFC 7517, *JSON Web Key (JWK).*2

RFC 7519, *JSON Web Token (JWT).*2

RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol*.2

RFC 8225, *Personal Assertion Token (PASSporT)*.[[2]](#footnote-2)

RFC 8226, *Secure Telephone Identity Credentials: Certificates*2

3GPP TS 22.173, *IMS Multimedia telephony communication service and supplementary services*.3

3GPP TS 24.196, *Enhanced Calling Name (eCNAM)*.[[3]](#footnote-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> >.

# Overview

This document introduces a set of procedures for the delivery of a calling name and potentially other caller data in the SHAKEN framework [ATIS-1000074] and [ATIS-1000080] and with TN certificates using certificate delegation [ATIS delegate-cert document]. The terms “rich” or “enhanced” data generically refer to the delivery of additional or meta data about the caller. That meta data may be made available to the end user through a multitude of services, such as enhanced CNAM (eCNAM) and Rich Call Data (RCD). This document describes the interface for RCD while ATIS-1000067 describes eCNAM.The SHAKEN framework establishes an end-to-end architecture that allows a telephone service provider to authenticate and assert a telephone identity and provides for the verification of this telephone identity by a terminating service provider. The SHAKEN framework defines a profile, using protocols standardized in the IETF Secure Telephone Identity Revisited (STIR) Working Group (WG), providing recommendations and requirements for implementing these IETF specifications, [RFC 8225], [RFC8224], and [RFC 8226], to support management of Service Provider-level certificates within the SHAKEN framework.

This document extends the SHAKEN framework beyond authentication of only the telephone number identity to include the name of the calling party displayed to the called party, typically in the form of a string. It also discusses the use of draft-ietf-stir-passport-rcd which defines a PASSporT [RFC8225] extension for enhanced calling party data such as name, address, photos, logos, and other extensible information that may be extended in the future to enable the secure, verified transport of data relevant to the calling party that can be displayed or passed to the called party.

There are various ways the calling name data is transmitted to the called party device today. These methods will be discussed and how the SHAKEN framework can provide validation of that data for each of these models. Additionally, for newer RCD types of data similar transmission and verification models will be discussed. Finally, a set of guidelines around how this data should be presented to the called party will be defined.

## SHAKEN CNAM and RCD Model Overview

Traditional CNAM which has been in use for many years in the telephone network from analog to digital telephones has provided the ability to display a 15-character string to the called party in a telephone call. The 15-character string is used to display a caller or company name corresponding to the calling party. In the United States, all CNAM data is retrieved from CNAM databases. In Canada, some, but not the majority of CNAM data, results from passing the name through ISUP signaling along with the calling party number.

Note: The 15-character string resulted from a limitation of SS7 Network and telephone user equipment limitations. However, recently, in ATIS and 3GPP, eCNAM was defined and described in [ATIS-1000067], [3GPP TS 22.173] and [3GPP TS 24.196]. eCNAM extends the ability to provide a longer name with 35 characters in the display-name SIP parameter plus the delivery of meta data about the caller, including text and images (e.g., logos) in one or more Call-Info headers.

As the industry moves to more modern displays of calling party information like mobile phone displays, Caller-ID to the TV services, and different images, graphics at different sizes, using fonts and font sizes adapted to the device being displayed, a framework for the transport and authentication/verification of this rich data is required.

This document provides a model and framework to use SHAKEN and extend it to provide

1. a model that can support the security of calling name strings transported in SIP, as well as
2. the transport and the security of RCD

Both RCD and eCNAM can support current and future needs and applications that want to pass identity and other information related to the calling party to the called party.

IETF has defined the "rcd" PASSporT extension in [draft-ietf-stir-passport-rcd] which defines the base STIR PASSporT claim "rcd". This claim includes an extensible JSON object that has two specified key values. A "nam" claim for validation of a name string as well as a "jcd" key value which is defined to support the jCard, the JSON format or vCard defined in [RFC7095] which is itself an extensible JSON object for the transport of personal identifiable types of information.

Using the "rcd" PASSporT extension, and specifically the "rcd" claim, the following sections of this document will detail the use of "rcd" claim depending on the call model either independently or as part of the "shaken" PASSporT to validate the data to the called party.

1. This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < <https://www.atis.org/docstore/product.aspx?id=28297> >. [↑](#footnote-ref-1)
2. This document is available from the Internet Engineering Task Force (IETF) at: < <https://tools.ietf.org/> >. [↑](#footnote-ref-2)
3. This document is available from 3rd Generation Partnership Project (3GPP) at: < https://www.3gpp.org >. [↑](#footnote-ref-3)