**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 mechanisms for authentication, verification, and transport of Conventional Calling Name (CNAM), Rich Call Data (RCD) and how they are 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 |
| 11/27/2020 | 0.6 | IPNNI-2020-00167R000 and  IPNNI-2020-00168R000 | D. Hancock |

Table of Contents

[**Alliance for Telecommunications Industry Solutions** i](#_Toc55463346)

[Table of Figures iii](#_Toc55463347)

[1 Scope & Purpose 1](#_Toc55463348)

[1.1 Scope 1](#_Toc55463349)

[1.2 Purpose 1](#_Toc55463350)

[2 Normative References 1](#_Toc55463351)

[3 Definitions, Acronyms, & Abbreviations 2](#_Toc55463352)

[3.1 Definitions 2](#_Toc55463353)

[3.2 Acronyms & Abbreviations 2](#_Toc55463354)

[4 Overview 4](#_Toc55463355)

[4.1 SHAKEN CNAM and RCD Model Overview 4](#_Toc55463356)

[5 SHAKEN CNAM and RCD Framework Definition 5](#_Toc55463357)

[5.1 "rcd" PASSporT claim construction overview 5](#_Toc55463358)

[5.1.1 Traditional CNAM using "nam" 5](#_Toc55463359)

[5.1.2 RCD using "jcd" with an embedded jCard 6](#_Toc55463360)

[5.1.3 RCD using "jcl" with a URL to jCard 7](#_Toc55463361)

[5.1.4 RCD using "crn" to convey call reason 7](#_Toc55463362)

[5.1.5 Integrity Protection of Rich Call Data 8](#_Toc55463363)

[5.2 RCD Authentication and Verification Procedures 8](#_Toc55463364)

[5.2.1 RCD Authentication 8](#_Toc55463365)

[5.2.2 RCD Verification 9](#_Toc55463366)

[5.2.3 OSP Procedures when Originating INVITE contains "rcd" PASSporT 10](#_Toc55463367)

[5.2.4 Including RCD PASSporT in retargeted INVITE Request 10](#_Toc55463368)

# 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-1000092 SHAKEN: 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 7095, *jCard: The JSON Format for vCard*.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> >.

## Definitions

The following provides some key definitions used in this document. Refer to IETF RFC 4949 for a complete Internet Security Glossary, as well as tutorial material for many of these terms.

**Caller ID:** The originating or calling party’s telephone number used to identify the caller carried either in the P-Asserted-Identity or From header fields in the Session Initiation Protocol (SIP) [RFC 3261] messages.

**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.

**Secure Telephone Identity (STI) Certificate:** A public key certificate used by a service provider to sign and verify the Personal Assertion Token (PASSporT).

**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.

**VoIP Entity:** A non-STI-authorized end user entity or other calling entity that purchases (or otherwise obtains) delegated telephone numbers from a Telephone Number SP (TNSP).

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| 3GPP | 3rd Generation Partnership Project |
| ATIS | Alliance for Telecommunications Industry Solutions |
| CNAM | Conventional Caller Name |
| eCNAM | Enhanced Caller Name |
| HTTPS | Hypertext Transfer Protocol Secure |
| IETF | [Internet Engineering Task Force](http://www.ietf.org/rfc.html) |
| JSON | JavaScript Object Notation |
| JWT | JSON Web Token |
| NNI | Network-to-Network Interface |
| OSP | Originating SP |
| PASSporT | Personal Assertion Token |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| RCD | Rich Call Data |
| SP | Service Provider |
| STI | Secure Telephone Identity |
| STIR | Secure Telephone Identity Revisited |
| TN | Telephone Number |
| TNSP | Telephone Number SP |
| TSP | Terminating SP |
| UE | User Equipment |
| URI | Uniform Resource Identifier |
| VoIP | Voice over Internet Protocol |

# 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 Telephone Number (TN) certificates using certificate delegation [ATIS-1000092]. 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. 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 information that may be extended in the future to enable the secure, verified transport of data relevant to the calling party that can be passed to the called party device and displayed to the called user.

There are various ways the calling name data is transmitted to the called party device today. This document will discuss how the SHAKEN framework can be extended to provide validation of this calling name data before it is conveyed to the called party device. Additionally, similar transmission and verification models will be discussed for newer RCD types of data.

## 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 the SS7 network and from 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 header fields.

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 extend SHAKEN 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 JavaScript Object Notation (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 clauses 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.

# SHAKEN CNAM and RCD Framework Definition

This clause describes the procedures associated with the addition the "rcd" PASSporT or inclusion of the "rcd" claim into a "shaken" PASSporT. Both of these procedures are used for supporting different service provider specific CNAM and RCD scenarios.

## "rcd" PASSporT claim construction overview

[draft-ietf-stir-passport-rcd] defines three new PASSporT claims; the "rcd", “crn", and "rcdi" claims. There are two main key values possible as part of the "rcd" claim. They are; (1) "nam" which is a minimally required key value as part of the "rcd" claim value JSON object; and (2) either "jcd" which is the optional key value that represents the direct inclusion of a jCard string in the "rcd" claim, or "jcl" which is the key value that represents an HTTPS URL link to a jCard file hosted on an HTTPS server. The “nam” key value is the only mandatory element of the "rcd" claim. Both the "jcd" and "jcl" key values of the "rcd" claim are optional, can only be included a maximum of one time in a "rcd" claim, and are mutually exclusive where you cannot have both key values. URLs contained in the “rcd” claim or contained in resources referenced by the “rcd” claim must use HTTPS. The “rcdi” claim protects the contents of resources referenced by "rcd" claim from being inadvertently or maliciously modified to unauthorized values. The “rcdi” claim is included if the “rcd” claim contains URLs, or if mandated by a JWTClaimConstraints extension contained in the signing certificate.

The “crn” claim contains a call reason phrase that describes the intent of the call. It is optional but recommended for enhancing usefulness to call recipients.

The following clauses provide more details on how the "rcd" JSON object is constructed.

### Traditional CNAM using "nam"

The "rcd" claim must contain a "nam" key with a value that identifies the display name of the originating entity. If the originating entity does not have a display name, the "nam" key value must be the empty string.

Example, for the following SIP INVITE

INVITE sip:+12155551213@biloxi.com SIP/2.0

Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds

Max-Forwards: 70

To: “Bob” <sip:+12155551213@biloxi.com; user=phone>

From: “Dentist Office” <sip:+12155551212@atlanta.com; user=phone>;tag=1928301774

Call-ID: a84b4c76e66710@pc33.atlanta.com

CSeq: 314159 INVITE

Date: Wed, 03 Dec 2020 12:58:14 GMT

Contact: <sip:dentist@pc33.atlanta.com>

Content-Type: application/sdp

Content-Length: 142

This is an example of an "rcd" extension PASSporT

Protected Header

{

"alg":"ES256",

"typ":"passport",

“ppt”:”rcd”,

"x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

"dest":{“tn”:["12155551213"]}

"iat": 1607000294,

"orig":{“tn”:"12155551212"},

"rcd":{"nam":"Dentist Office"}

}

This is an example of a "shaken" extension PASSporT that includes an "rcd" claim

Protected Header

{

"alg":"ES256",

"typ":"passport",

“ppt”:”shaken”,

"x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

“attest”:”A”

"dest":{“tn”:["12155551213"]}

"iat":1607000294,

"orig":{“tn”:"12155551212"},

“origid”:”123e4567-e89b-12d3-a456-426655440000”,

"rcd":{"nam":"Dentist Office"}

}

### RCD using "jcd" with an embedded jCard

A "jcd" key value for a "rcd" claim should be constructed with the value being equal to a jCard string. At a minimum the jCard should include a “fn” and one “tel” objects for SHAKEN. Note: Additional objects are optional but may be ignored or disregarded by the receiving entity depending on the rendering capabilities of the device and/or network local policy.

This is an example of an "rcd" extension PASSporT with "jcd"

Protected Header

{

"alg":"ES256",

"typ":"passport",

“ppt”:”rcd”,

"x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

"dest":{“tn”:["12155551213"]}

"iat":1607000294,

"orig":{“tn”:"12155551212"},

"rcd":{"nam":"Dentist Office","jcd":["vcard",[["logo",{},"uri",

"https://logo.service-provider.com/DentistLogo.jpg"]]]}}

"rcdi":"sha256-u5AZzq6A9RINQZngK7T62em8M

}

This is an example of an "shaken" extension PASSporT that includes an "rcd" claim

Protected Header

{

"alg":"ES256",

"typ":"passport",

“ppt”:”shaken”,

"x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

“attest”:”A”

"dest":{“tn”:["12155551213"]}

"iat":1607000294,

"orig":{“tn”:"12155551212"},

“origid”:”123e4567-e89b-12d3-a456-426655440000”,

"rcd":{"nam":"Dentist Office","jcd":["vcard",[["logo",{},"uri",

"https://logo.service-provider.com/DentistLogo.jpg"]]]}}

"rcdi":"sha256-u5AZzq6A9RINQZngK7T62em8M"

}

Whenever the logo resource is updated, the new logo must be stored in a new file referenced by a new logo URL.

### RCD using "jcl" with a URL to jCard

A "jcl" key value for a "rcd" claim should be constructed with the value being equal to an HTTPS URL of a file hosted on an HTTPS server containing a jCard string. At a minimum the linked jCard file should include a “fn” and one “tel” objects for SHAKEN. Note: Additional objects are optional but may be ignored or disregarded by the receiving entity depending on the rendering capabilities of the device and/or network local policy.

This is an example of an "rcd" extension PASSporT with "jcl"

Protected Header

{

"alg":"ES256",

"typ":"passport",

“ppt”:”rcd”,

"x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

"dest":{“tn”:["12155551213"]}

"iat":1443208345,

"orig":{“tn”:"12155551212"},

"rcd":{"nam":"Dentist Office","jcl":"https://example.org/dentist.json"}

"rcdi":"sha256-u5AZzq6A9RINQZngK7T62em8M"

}

This is an example of an "shaken" extension PASSporT that includes an "rcd" claim

Protected Header

{

"alg":"ES256",

"typ":"passport",

“ppt”:”shaken”,

"x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

“attest”:”A”

"dest":{“tn”:["12155551213"]}

"iat":1443208345,

"orig":{“tn”:"12155551212"},

“origid”:”123e4567-e89b-12d3-a456-426655440000”,

"rcd":{"nam":"Dentist Office","jcl":"https://example.org/dentist.json"}

"rcdi":"sha256-u5AZzq6A9RINQZngK7T62em8M"

}

Whenever the jCard resource is updated, the new jCard must be stored in a new file referenced by a new jCard URL.

### RCD using "crn" to convey call reason

The "rcd" PASSporT can include a "crn" claim to convey the reason for the call, as shown in the following example:

Protected Header

{

"alg":"ES256",

"typ":"passport",

“ppt”:”rcd”,

"x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

"dest":{“tn”:["12155551213"]}

"iat":1443208345,

"orig":{“tn”:"12155551212"},

"rcd":{"nam":"Dentist Office","jcl":"https://example.org/dentist.json"}

"rcdi":"sha256-u5AZzq6A9RINQZngK7T62em8M"

"crn":"Dentist Appointment Reminder"

}

### Integrity Protection of Rich Call Data

[draft-ietf-stir-passport-rcd] specifies how the "rcdi" claim of the "rcd" PASSporT is used to protect the integrity of the rich call data from being maliciously modified. The "rcdi" claim contains a digest that is calculated across all of the rich call data; i.e., the input to the digest calculation is the “rcd” claim contents, plus any resources referenced by the "rcd" claim contents, plus any resources referenced by the referenced resources, and so on. Consider the case where the "rcd" claim contains a "nam" key value, and "jcl" key value that references a jCard, and the jCard in turn contains a "logo" key value referencing a jpg image of the company logo. The input to the digest algorithm will include the "rcd" key values, the referenced jCard key values, and the referenced logo image.

When the “rcdi” claim is included, the RCD authentication service must use the crypto algorithm sha-256 to generate the digest; i.e., the first part of the "rcdi" value must contain the string "SHA256".

## RCD Authentication and Verification Procedures

### RCD Authentication

The RCD authentication service shall perform RCD authentication, either by constructing an "rcd" PASSporT or by adding "rcd" PASSporT claims to a "shaken" PASSporT, as specified in [draft-ietf-stir-passport-rcd].

When constructing an "rcd" PASSporT, the RCD authentication service shall populate the protected header as specified in [draft-ietf-stir-passport-rcd]. The "alg" parameter value shall be "ES256". The payload "orig", "dest", and "iat" claims shall be populated as specified in [ATIS-1000074].

When adding "rcd" PASSporT claims to a "shaken" PASSporT, the RCD authentication service must populate the base shaken claims as specified in [ATIS-1000074].

The RCD authentication service shall include an "rcd" claim. The "rcd" claim must contain a "nam" key value pair and may contain the additional optional key value pairs defined for the "rcd" claim in [draft-ietf-stir-passport-rcd]. The RCD authentication service shall populate the values of the key value pairs of the "rcd" claim based on information obtained from an authoritative database.

The RCD authentication service must include an "rcdi" claim if the "rcd" claim directly or indirectly references external resources, or if inclusion of the "rcdi" claim is mandated by the JWTClaimConstraints extension contained in the signing certificate. The RCD authentication service may include a "crn" claim.

If the calling user requests privacy (e.g., the Privacy header field contains a privacy type of "id"), then the RCD authentication service may anonymize the user’s identity in the "rcd" claim, but the remaining claims shall be set as specified in [ATIS-1000074] (specifically, the "orig" claim shall contain the actual calling TN).

The "rcd" PASSporT shall be signed with the credentials of either a delegate certificate as defined in [ATIS-100092], or an STI certificate as defined in [ATIS-100074]. When signing with a delegate certificate, the authentication service must ensure that the certificate scope, as specified by the certificate’s TNAuthList, includes the "orig" claim of the "rcd" PASSporT. The Protected Header "x5u" parameter shall reference the signing certificate.

When adding "rcd" PASSporT claims to a "shaken" PASSporT, the RCD authentication service must sign the "shaken" PASSporT with the credentials of an STI certificate as defined in [ATIS-1000074].

The JWTClaimConstraints extension defined in [RFC 8226] may be used to constrain the rcd information that can be signed by an RCD authentication service hosted by a non-shaken entity. For example, an STI-SCA (as defined in [ATIS-1000092]) may include a JWTClaimConstraints extension in the delegate certificate issued to a non-shaken Voice over Internet Protocol (VoIP) entity in order to constrain the RCD authentication service to include an "rcdi" claim in the "rcd" PASSporT for a specific value or set of values (see clause 5.1.5).

The Identity header field of the originating INVITE request shall be populated with the full form of the resulting "rcd" or "shaken" PASSporT.

RCD authentication can be performed either by the originating customer’s CPE (i.e., a non-SHAKEN VoIP Entity such as an enterprise SIP-PBX) or by a SHAKEN-approved Originating SP (OSP), as described in the following sub-clauses.

#### RCD Authentication provided by non-SHAKEN VoIP Entity

A non-SHAKEN VoIP entity shall perform RCD authentication as described in clause 5.2.1 with the restriction that it must construct an "rcd" PASSporT (i.e., the option to populate "rcd" PASSporT claims in a "shaken" PASSporT must not be used by non-SHAKEN entities). The resulting "rcd" PASSporT must be signed with the credentials of a delegate certificate held by the non-SHAKEN VoIP Entity.

#### RCD Authentication provided by OSP

Based on local policy, an OSP may provide RCD authentication services for its originating customers. The OSP shall perform RCD authentication only if the criteria for "A" attestation are met, either as specified in [ATIS-1000074] or based on receiving a valid base PASSporT from the originating customer as described in clause 6.1 of [ATIS-1000092].

### RCD Verification

The RCD verification service shall verify a received “rcd” PASSporT, or a “shaken” PASSporT containing “rcd” PASSporT claims, as specified in [draft-ietf-stir-passport-rcd], with the following additions or modifications:

1. In the case of a "shaken" PASSporT containing "rcd" PASSporT claims, the verification procedures defined in [ATIS-1000074] and [ATIS-1000085] shall be applied.
2. In the case of an "rcd" PASSporT, the verification procedures are based on the type of certificate referenced by the Protected Header "x5u" parameter, as follows:
   * If the "x5u" parameter references an STI certificate, then the "shaken" PASSporT verification procedures defined in [ATIS-1000074] and [ATIS-1000085] shall be applied to the "rcd" PASSporT.
   * If the "x5u" parameter references a delegate certificate, then the base PASSporT verification procedures defined in [ATIS-1000092] shall be applied. (Note, [ATIS-1000092] refers to the base SHAKEN verification procedures in [ATIS-1000074], with specific modifications for delegate certificates such as stricter scope encompassing rules.)

If the certificate referenced by the "x5u" field contains a JWTClaimConstraints extension, then the verification service shall verify that the constraints are satisfied as specified in [RFC 8226]. If the RCD verification service does not support JWTClaimConstraints, then it should fail verification with response code 437 ‘Unsupported credential’. Note, this verification failure case should not cause the call to fail.

If the “rcdi” claim is included, then the RCD verification service must verify it as specified in [draft-ietf-stir-passport-rcd].

#### Conveying Rich Call Data to the Called Endpoint

This document does not mandate a specific mechanism for conveying rich call data to the called endpoint. For example, the Terminating SP (TSP) could convey this information in SIP signaling, or via some out-of-band mechanism. Two possible ways to convey this information in SIP are as follows:

1. The rich call data contained in a valid "shaken" or "rcd" PASSporT can be conveyed to the called endpoint protected in the PASSporT itself (contained in an Identity header field of the terminating INVITE request sent to the called User Equipment (UE)). In this case, the TSP shall ensure that any unprotected rich call data contained in the INVITE request does not conflict with the protected rich call data. Specifically, the TSP shall set the display name component in the From header field (and, if present, in the P-Asserted-Identity header field) to match the "rcd" claim "nam" key value. If the INVITE request contains a Call-Info header field, then the TSP shall ensure that any rich call data item (e.g., company logo) that is contained in both the Call-Info header field and the "shaken" or "rcd" PASSporT match.
2. Alternatively, the rich call data contained in a valid "shaken" or "rcd" PASSporT can be carried unprotected to the called endpoint in the following header field components of the terminating INVITE request as per [RFC 3261], [RFC 3325] and [draft-wendt-sipcore-callinfo-rcd]:

* The calling name is conveyed in the display name portion of the P-Asserted-Identity and/or From header field,
* The URI referencing additional rich call data is carried in the Call-Info header field (purpose = "jcard") and,
* The "crn" call reason text string is carried in the "call-reason" parameter of the Call-Info header field.

The actual method used to convey rich call data to the called endpoint is based on local policy and the capabilities of the called endpoint.

If the TSP receives a "shaken" PASSporT and an "rcd" PASSporT that are both valid but contain different rich call data information, then the rich call data information delivered to the called endpoint shall be based on local policy.

The TSP shall not convey any rich call data to the called UE if the calling user has requested privacy (e.g., the received terminating INVITE request contains a Privacy header field with a privacy type of "id").

### OSP Procedures when Originating INVITE contains "rcd" PASSporT

As described in this clause, an OSP can use the presence of an "rcd" PASSporT received in an originating INVITE request for two things; to determine the attestation level during SHAKEN authentication, and as a source of rich call date that is conveyed to the TSP. The OSP handling of rcd PASSporTs received in originating INVITE requests is based entirely on local policy; i.e., the OSP can apply a policy to perform these functions always, selectively based on some criteria, or never.

On receiving an originating INVITE request containing an Identity header field with an "rcd" PASSporT, the OSP shall perform SHAKEN authentication as specified in [ATIS-1000074] (i.e., an OSP will always generate a “shaken” PASSporT, even though the received INVITE request already contains an "rcd" PASSporT). As described in [ATIS-1000092], an OSP may use the presence of a valid "rcd" PASSporT signed with the credentials of a delegate certificate as evidence that SHAKEN Full attestation criteria 2 and 3 are satisfied.

If local policy dictates that the OSP accepts the received “rcd” PASSporT, then it shall verify the PASSporT as described in clause 5.2.2. If the passport is valid, and local policy dictates that the OSP sends rich call data to this particular destination[[4]](#footnote-4), then the OSP shall either include the "rcd" PASSporT in the INVITE request sent toward the TSP, or include the "rcd" PASSporT claims in the "shaken" PASSport and discard the "rcd" PASSporT.

If the received "rcd" PASSporT is invalid, then it shall be discarded by the OSP.

### TSP Procedures when received INVITE contains "rcd" PASSporT

As with the OSP, the TSP handling of rich call data contained in a terminating INVITE request is based entirely on local policy.

If the INVITE request contains a "shaken" PASSporT with rcd claims, then the TSP shall include the rcd claims in the PASSporT signature validation procedure, but otherwise may either use or ignore these rcd claims based on local policy.

If the INVITE request contains an "rcd" PASSporT, then the TSP shall either accept or discard the "rcd" PASSporT, based on local policy. If local policy dictates that the TSP accepts the received “rcd” PASSporT, then it shall verify the PASSporT as described in clause 5.2.2. If verification passes, the TSP shall convey the verification results to the called endpoint as described in clause 5.2.2.1.

If verification fails, the TSP shall discard the “rcd” PASSporT.

If a TSP retargets a terminating INVITE request containing an "rcd" PASSporT (e.g., as a result of a terminating feature such as call forwarding), then the retargeting TSP shall either include the "rcd" PASSPorT in the retargeted INVITE request or discard the "rcd" PASSporT, based on local policy.

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)
4. The most straightforward policy is to send the validated rich call data to all destinations. However, there may be cases, especially during the initial rollout of RCD, where some destinations can’t handle the additional data (e.g., the inclusion of rich call data causes the message size to exceed some implementation-imposed threshold). [↑](#footnote-ref-4)