**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 |

Table of Contents[**ATIS-1000XXX** i](#_Toc39068360)

[ATIS Standard on i](#_Toc39068361)

[**Signature-based Handling of Asserted information using toKENs (SHAKEN): Calling Name and Rich Call Data Handling Procedures** i](#_Toc39068362)

[**Alliance for Telecommunications Industry Solutions** i](#_Toc39068363)

[**Abstract** i](#_Toc39068364)

[Table of Figures iii](#_Toc39068365)

[1 Scope & Purpose 1](#_Toc39068366)

[1.1 Scope 1](#_Toc39068367)

[1.2 Purpose 1](#_Toc39068368)

[2 Normative References 1](#_Toc39068369)

[3 Definitions, Acronyms, & Abbreviations 2](#_Toc39068370)

[3.1 Definitions 2](#_Toc39068371)

[3.2 Acronyms & Abbreviations 2](#_Toc39068372)

[4 Overview 4](#_Toc39068373)

[4.1 SHAKEN CNAM and RCD Model Overview 4](#_Toc39068374)

[5 SHAKEN CNAM and RCD Framework Definition 5](#_Toc39068375)

[5.1 "rcd" claim construction overview 5](#_Toc39068376)

[5.1.1 Traditional CNAM using "nam" 5](#_Toc39068377)

[5.1.2 RCD using "jcd" with an embedded jCard 6](#_Toc39068378)

[5.1.3 RCD using "jcl" with a URL to jCard 7](#_Toc39068379)

[5.1.4 RCD using "crn" to convey call reason 7](#_Toc39068380)

[5.1.5 Integrity Protection of Rich Call Data 8](#_Toc39068381)

[5.2 RCD Authentication and Verification Procedures 8](#_Toc39068382)

[5.2.1 RCD Authentication 8](#_Toc39068383)

[5.2.2 RCD Verification 9](#_Toc39068384)

# Table of Figures

# 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> >.

## 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:** Either a canonical Address-of-Record (AoR) SIP Uniform Resource Identifier (URI) employed to reach a user (such as ’sip:alice@atlanta.example.com’), or a telephone number, which commonly appears in either a TEL URI [RFC 3966] or as the user portion of a SIP URI. See also Caller ID [RFC 8224].

**National/Regional Regulatory Authority (NRRA):** A governmental entity responsible for the oversight/regulation of the telecommunication networks within a specific country or region.

NOTE: Region is not intended to be a region within a country (e.g., a region is not a state within the US).

**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].

**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 URI or a TEL URI) from which a telephone number can be derived.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| AoR | Address-of-Record |
| 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 |
| JWA | JSON Web Algorithms |
| JWK | JSON Web Key |
| JWS | JSON Web Signature |
| JWT | JSON Web Token |
| NNI | Network-to-Network Interface |
| OCN | Operating Company Number |
| PASSporT | Personal Assertion Token |
| PSTN | Public Switched Telephone Network |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| RCD | Rich Call Data |
| REST | Representational State Transfer |
| SP | Service Provider |
| STI | Secure Telephone Identity |
| STIR | Secure Telephone Identity Revisited |
| TN | Telephone Number |
| URI | Uniform Resource Identifier |
| VoIP | Voice over Internet Protocol |

# Overview

This document introduces a set of procedures for the use of calling name (CNAM) and Rich Call Data (RCD) in the SHAKEN framework [ATIS-1000074] and [ATIS-1000080] and with TN certificates using certificate delegation [ATIS delegate-cert document]. 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 more traditional CNAM data, typically in the form of a string, of the name of the calling party displayed to the called party. 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 is various ways CNAM 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 show 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. This traditional CNAM is generally either passed through the call signaling or is inserted into the call at the terminating communications service provider (CSP) via a dip to a CNAM database.

Note: The 15-character string was derived 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 additional data in one or more Call-Info headers.

As the industry moves away from string and text-based displays to more modern display of calling party information like mobile phone displays, Caller-ID to the TV services, and other enhanced displays capable of displaying more and different types of data like 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 the SHAKEN framework and extend it to provide both a model that can support both the security of traditional CNAM and eCNAM calling name strings transported in SIP as well as both the transport and security of RCD in an extensible way to 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 CNAM 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 CNAM and RCD data to the calling party.

# SHAKEN CNAM and RCD Framework Definition

This section 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. If the “rcd” claim does not contain any URLs, then the “rcdi” claim is not required. Otherwise, the “rcdi” claim must be included.

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 sections 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 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: “Alice” <sip:+12155551212@atlanta.com; user=phone>;tag=1928301774

Call-ID: a84b4c76e66710@pc33.atlanta.com

CSeq: 314159 INVITE

Date: Sat, 13 Nov 2015 23:29:00 GMT

Contact: <sip:alice@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":1443208345,

 "orig":{“tn”:"12155551212"},

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

 "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"}

 "rcdi":"sha256-u5AZzq6A9RINQZngK7T62em8M"

}

### 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":1443208345,

 "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":1443208345,

 "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 “rcd” PASSporT “orig”, “dest”, and “iat” claims with the same procedures as specified for the "shaken" PASSporT defined 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. 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).

When constructing an “rcd” PASSporT, the Protected Header “x5u” parameter shall reference either a delegate end entity certificate as defined in [ATIS delegate-cert document], or a SHAKEN end entity certificate as specified in [ATIS-1000080]. The RCD authentication service shall sign the “rcd” PASSporT with the private key of the end-entity certificate referenced by the “x5u” parameter.

When adding "rcd” PASSporT claims to a “shaken” PASSporT, the RCD authentication service must sign the “shaken” PASSporT with a SHAKEN certificate as defined in [ATIS-1000074].

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 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 with the restriction that 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 a delegate certificate held by the non-SHAKEN VoIP Entity.

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]. The OSP may verify an "rcd" PASSporT received in an originating INVITE request as described in clause 5.2.2, and use the verification results to augment the [ATIS-1000074] shaken attestation criteria; i.e., the presence of a valid "rcd" PASSPorT can be used as evidence that the shaken "A" attestation criteria are met. If the received "rcd" PASSporT is valid, then the OSP should include the "rcd" PASSporT claims in the "shaken" PASSporT.

If the received "rcd" PASSporT is valid, then it is recommended that the OSP include the "rcd" PASSporT in an Identity header field of the INVITE request sent to the TSP. Based on local policy agreement with the TSP, the OSP may optionally remove the "rcd" PASSporT from the INVITE sent to the TSP, in which case the OSP shall include the "rcd" PASSporT claims in the "shaken" PASSporT.

#### RCD Authentication provided by OSP

Based on local policy, an OSP may provide RCD authentication services for its originating customers. As described in clause 5.2.1 the OSP RCD authentication service can either construct an "rcd" PASSporT or place the "rcd" PASSporT claims in a "shaken" PASSporT. 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 delegate cert spec].

### 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]. In addition, the RCD verification service shall verify that the value of the “orig”, “dest”, and “iat” claims are as specified in [ATIS-1000074] and [ATIS-1000085].

When verifying an “rcd” PASSporT, the RCD verification service shall determine the validity of the certificate referenced in the “x5u” field in the “rcd” PASSporT protected header as specified in section 5.3.1 of [ATIS-1000074], with the following modifications:

* Verify that the certificate is a valid delegate end entity certificate, as specified in [ATIS delegate-cert document]; i.e., both the certificate and its parent certificate contain a TNAuthList object.
* Verify that the “orig” claim TN belongs to the set of TN(s) identified by the TNAuthList of the certificate referenced by the “x5u” parameter.
* Verify that the scope of each delegate CA certificate in the certification path encompasses the scope of its child certificate, as described in clause 6.2 of [ATIS delegate cert spec].

If the certificate referenced by the "x5u" field contains a JWTClaimConstraints extension, and 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 information could be conveyed 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). Any unprotected rich call data contained in the INVITE request (e.g., display name information contained in the From or P-Asserted-Identity header fields, or any information contained in the Call-Info header field) that doesn’t match the information in the "shaken" or "rcd" PASSporT shall be removed from the terminating INVITE request before it is sent to the called endpoint.
2. Alternatively, the rich call data contained in a valid "shaken""rcd" PASSPorT can be carried unprotected to the called endpoint in the following header field components of the terminating INVITE request as per [RFC 3325] and [draft-wendt-sipcore-callinfo-rcd-01]:
* The calling name is conveyed in the display name portion of the P-Asserted-Identity and/or From header field, and
* The URI referencing additional rich call data is carried in the Call-Info header field (purpose = "jcard").
* The "crn" call reason text string is carried in the "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.

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)