ATIS-1000094

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 April 12, 2021

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 calling name and other enhanced caller identity information (e.g., images, logos) and call reason, and describing how they are handled in various call origination and termination scenarios.

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

ATIS Standard on –

SHAKEN: Calling Name and Rich Call Data Handling Procedures

1 Scope & Purpose

1.1 Scope

This specification expands the SHAKEN framework, introducing mechanisms for authentication, verification, transport of calling name and other enhanced caller identity information (e.g., images, logos), and call reason and describing how they are handled in various call origination and termination scenarios.

1.2 Purpose

To provide a framework and a set of procedures that enable the delivery of authenticated calling name and enhanced caller metadata for display to the called party using the "rcd" PASSporT extension defined in draft-ietf-stir-passport-rcd, *PASSporT Extension for Rich Call Data* [Ref 7].

2 References

2.1 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.

[Ref 1] ATIS-1000074-E, *Errata on ATIS Standard on Signature-based Handling of Asserted Information using toKENs (SHAKEN).*[1]

[Ref 2] ATIS-1000067, *IP NGN Enhanced Calling Name (eCNAM)*.[1]

[Ref 3] ATIS-1000080, *SHAKEN: Governance Model and Certificate Management*.[1]

[Ref 4] ATIS-1000085, *SHAKEN: SHAKEN Support of "div" PASSporT*.[1]

[Ref 5] ATIS-1000092, *SHAKEN: Delegate Certificates.*[1]

[Ref 6] draft-wendt-sipcore-callinfo-rcd, *SIP Call-Info Parameters for Rich Call Data*.[2]

[Ref 7] draft-ietf-stir-passport-rcd, *PASSporT Extension for Rich Call Data.*[2]

[Ref 8] RFC 3261, *SIP: Session Initiation Protocol.*[2]

[Ref 9] RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks.*[2]

[Ref 10] RFC 7095, *jCard: The JSON Format for vCard*.[2]

[Ref 11] RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol*.[2]

[Ref 12] RFC 8225, *Personal Assertion Token (PASSporT)*.[2]

[Ref 13] RFC 8226, *Secure Telephone Identity Credentials: Certificates.*[2]

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://www.atis.org/docstore/product.aspx?id=28297 >.

[2] This document is available from the Internet Engineering Task Force (IETF) at: < https://tools.ietf.org/ >.

[Ref 14] 3GPP TS 22.173, *IMS Multimedia telephony communication service and supplementary services*.[3]

[Ref 15] 3GPP TS 24.196, *Enhanced Calling Name (eCNAM)*.[3]

2.2 Informative References

[Ref 101] RFC 4949, *Internet Security Glossary, Volume 2.*[4]

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 >.

3.1 Definitions

The following provides some key definitions used in this document. Refer to IETF RFC 4949 [Ref 101] 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) [Ref 8] message.

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 needed by a service provider to sign or verify the Personal Assertion Token (PASSporT).

Secure Telephone Identity Subordinate Certificate Authority (STI-SCA): An SCA that gets its certificate directly from an STI-CA.

Subordinate CA (SCA): A Certificate Authority whose public-key certificate is issued by another (superior) CA [Ref 8].

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 leases (or otherwise obtains) telephone numbers from a Telephone Number SP.

VoIP Entity Subordinate Certificate Authority (V-SCA): An SCA that gets its certificate from an STI-SCA or from another V-SCA.

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
ATIS	Alliance for Telecommunications Industry Solutions
CA	Certificate Authority
CNAM	Calling Name

[3] This document is available from 3rd Generation Partnership Project (3GPP) at: < https://www.3gpp.org >.

[4] This document is available from the Internet Engineering Task Force (IETF) at: < https://tools.ietf.org/ >.

eCNAM	Enhanced Calling Name
HTTPS	Hypertext Transfer Protocol Securep
IETF	Internet Engineering Task Force
JSON	JavaScript Object Notation
JWT	JSON Web Token
OSP	Originating SP
PASSporT	Personal Assertion Token
PBX	Private Branch Exchange
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
RCD	Rich Call Data
SCA	Subordinate Certificate Authority
SP	Service Provider
STI	Secure Telephone Identity
STI-SCA	Secure Telephone Identity Subordinate Certificate Authority
STIR	Secure Telephone Identity Revisited
TN	Telephone Number
TSP	Terminating SP
UE	User Equipment
URI	Uniform Resource Identifier
V-SCA	VoIP Entity Subordinate Certificate Authority
VoIP	Voice over Internet Protocol

4 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-E, *Errata on ATIS Standard on Signature-based Handling of Asserted toKENs* [Ref 1], and ATIS-1000080, *SHAKEN: Governance Model and Certificate Management* [Ref 3] [Ref 5]. The terms "rich" or "enhanced" data generically refer to the delivery of additional or metadata about the caller. That metadata may be made available to the end user through a multitude of services, such as Enhanced Calling Name (eCNAM) and Rich Call Data (RCD). This document describes the functional requirements for RCD while ATIS-1000067, *IP NGN Enhanced Calling Name (eCNAM)* [Ref 2], 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, *Personal Assertion Token (PASSporT)* [Ref 12]; RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol* [Ref 11]; and RFC 8226, *Secure Telephone Identity Credentials: Certificates* [Ref 13] – 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 authentication of the calling party name and other caller identity information displayed to the called party, typically in the form of a string. It also discusses the use of draft-ietf-stir-passport-rcd [Ref 7] which defines a PASSporT [Ref 12] extension for enhanced calling party data such as name, address, photos, logos, and other information that may be provided in the future. draft-ietf-stir-passport-rcd [Ref 7] enables the secure, verified transport of data relevant to the calling party to be passed to the called party device and displayed to the called party. In addition to the PASSporT extension, RFC 8226 [Ref 13] and draft-ietf-stir-passport-rcd [Ref 7] define a certificate extension and specific rcd-PASSporT-related values to bind sets of vetted calling party name and enhanced caller identity information that may be asserted by the PASSporT signer to a signing certificate.

There are various ways the calling name data is transmitted to the called party device today. This document discusses 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 are discussed for newer RCD types of data.

> NOTE: This specification does not incorporate the third-party service model described in draft-ietf-stir-passport-rcd [Ref 7], but recognizes it as a future consideration.

4.1 SHAKEN CNAM and RCD Model Overview

Calling Name (CNAM), which has been in use for many years in the public 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 (or other information about the caller) corresponding to the calling party.

> 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 [Ref 2], 3GPP TS 22.173, *IMS Multimedia telephony communication service and supplementary services* [Ref 14], and 3GPP TS 24.196, *Enhanced Calling Name (eCNAM)* [Ref 15]. eCNAM extends the ability to provide a longer name with 35 characters in the display-name SIP parameter plus the delivery of metadata 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, such as mobile phone and tablet/laptop displays, and home entertainment displays that support Caller ID to the TV services, it becomes possible to render images, graphics and fonts to a called party that are adapted to the display capabilities of the called party's device. Service Providers can take advantage of these new display capabilities to provide the called party with additional information about the identity of the caller and the reason for the call. This requires a framework for the transport and authentication/verification of this rich call data.

This extends SHAKEN by providing:

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

Both RCD and eCNAM are intended 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 [Ref 7] which defines the base STIR PASSporT claim "rcd". This claim includes an extensible JavaScript Object Notation (JSON) object that has three specified key values: a "nam" claim for validation of a name string, plus "jcd", and "jcl" key values which are defined to support the jCard, the JSON format or vCard defined in RFC 7095, *jCard: The JSON Format for vCard* [Ref 10] 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, Clause 5 of this document 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.

5 SHAKEN CNAM and RCD Framework Definition

This clause describes the procedures associated with the addition of 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.

5.1 "rcd" PASSporT claim construction overview

draft-ietf-stir-passport-rcd [Ref 7] 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 shall use HTTPS. The "rcdi" claim protects the contents of resources referenced by the "rcd" claim from being inadvertently or maliciously modified. Where a Voice over Internet Protocol (VoIP) Entity or SP populates an "rcdi" claim value with no constraints encoded in the signing certificate, the "rcdi" claim in the PASSporT protects the integrity of the "rcd" claim and referenced URL resources as asserted by the entity that created the PASSporT. In cases where the signing certificate includes constraints on the "rcdi" claim values (and therefore on the contents of the "rcd" claim and associated resources) as described in Clause 5.2.1, the PASSporT is further limited to specific pre-vetted values for the calling name and enhanced caller identity information the signing entity can assert.

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.

5.1.1 CNAM using "nam"

The "rcd" claim shall 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 shall 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: Thu, 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"}

}
```

5.1.2 Integrity Protection of Rich Call Data

draft-ietf-stir-passport-rcd [Ref 7] 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 JPEG 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 shall use the crypto algorithm sha-256 to generate the digest; i.e., the first part of the "rcdi" value shall contain the string "sha256".

5.1.3 RCD using "jcd" with an embedded jCard

A "jcd" key value for an "rcd" claim should be constructed with the value being equal to a jCard string. Note that 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":<computed per draft-ietf-stir-passport-rcd>
}
```

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","jcd":["vcard",[["logo",{},"uri",
         "https://logo.service-provider.com/DentistLogo.jpg"]]]},
   "rcdi":<computed per draft-ietf-stir-passport-rcd>
}
```

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

5.1.4 RCD using "jcl" with a URL to jCard

A "jcl" key value for an "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. Note that 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":1607000294,
   "orig":{"tn":"12155551212"},
   "rcd":{"nam":"Dentist Office","jcl":"https://example.org/dentist.json"},
   "rcdi":<computed per draft-ietf-stir-passport-rcd>
}
```

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","jcl":"https://example.org/dentist.json"},
   "rcdi":<computed per draft-ietf-stir-passport-rcd>
}
```

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

5.1.5 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 (note that the contents of the "rcd" claim have no bearing on the inclusion or value of the “crn" claim):

```
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","jcl":"https://example.org/dentist.json"},
   "rcdi":<computed per draft-ietf-stir-passport-rcd>,
   "crn":"Dentist Appointment Reminder"
```

}

5.2 RCD Authentication and Verification Procedures

5.2.1 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 [Ref 7].

The RCD authentication service shall include an "rcd" claim. The "rcd" claim shall 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 [Ref 7]. The RCD authentication service shall populate the values of the key value pairs of the "rcd" claim based on a source of vetted information as described in Clauses 5.2.1.1 through 5.2.1.3 below.

The RCD authentication service shall include an "rcdi" claim as described in Clause 5.1.2 if the "rcd" claim directly or indirectly references external resources and/or if inclusion of the "rcdi" claim is mandated by the JWTClaimConstraints extension contained in the signing certificate as described in Clause 5.2.1.1.

If the RCD authentication service includes an "rcdi" claim, then the entity generating the PASSporT shall ensure that the content contained in and referenced by the "rcd" claim corresponds to the value of the "rcdi" claim (otherwise, verification will fail).

The RCD authentication service may include a "crn" claim.

If the calling party 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-E [Ref 1] (specifically, the "orig" claim shall contain the actual calling TN).

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 or other VoIP Entity's CPE (e.g., an enterprise SIP-PBX) or by a SHAKEN-approved Originating SP (OSP) with credentials as appropriate to the given entity type, as described in the following sub-clauses.

5.2.1.1 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 shall construct an "rcd" PASSporT (i.e., the option to populate "rcd" PASSporT claims in a "shaken" PASSporT shall not be used by non-SHAKEN entities).

When constructing an "rcd" PASSporT, the RCD authentication service shall populate the protected header as specified in draft-ietf-stir-passport-rcd [Ref 7]. The "alg" parameter value shall be "ES256". The payload "orig", "dest", and "iat" claims shall be populated as specified in ATIS-1000074-E [Ref 1].

The resulting "rcd" PASSporT shall be signed with the credentials of a delegate certificate held by the non-SHAKEN VoIP Entity. The RCD authentication service shall 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. The JWTClaimConstraints extension defined in RFC 8226 [Ref 13] may be used by the delegate certificate issuer (STI-SCA or V-SCA as defined in ATIS-1000092 [Ref 5]) to constrain the "rcd" information that can be signed by an RCD authentication service hosted by a non-SHAKEN VoIP Entity. For example, the issuer may include a JWTClaimConstraints extension in the delegate certificate issued to the VoIP Entity specifying that an "rcdi" claim must be included with one of a set of "permitted values", corresponding to pre-vetted sets of "rcd" claims and associated resources the VoIP Entity may assert in the PASSporT (see RFC 8226 clause 8 [Ref 13] and draft-ietf-stir-passport-rcd [Ref 7]). The "rcd" claims populated by the VoIP Entity in an "rcd" PASSporT shall contain data and resource URLs corresponding to an "rcd" digest value matching the "rcdi" claim digest value that was selected from the set of permitted "rcdi" values. Alternatively, the certificate issuer can include only "permitted values" for the "rcd" claim to provide a vetted value for a "nam"-only "rcd" claim or other "rcd" claim that does not reference external resources.

5.2.1.2 RCD Authentication provided by OSP – "shaken" PASSporT

Based on local policy, an OSP may perform RCD authentication services to populate "rcd"/"rcdi" and optional "crn" claims in a "shaken" PASSporT for its originating customers' calls. The OSP shall perform RCD authentication only if the criteria for "A" attestation are met; e.g., as specified in ATIS-1000074-E [Ref 1] or based on receiving a valid base PASSporT from the originating customer as described in Clause 6.1 of ATIS-1000092 [Ref 5]. The RCD authentication service shall populate the by-value and by-reference contents of the "rcd" claim based on vetted information. The source of the vetted information may be the contents of the "rcd" claim in a verified "rcd" PASSporT that complies with the JWTClaimConstraints of the signing delegate certificate (see Clauses 5.2.1.1 and 5.2.3), or another source currently outside the scope of this document. As an example, the information could be vetted by the SHAKEN SP holding the signing STI certificate. Alternatively, the information could be obtained from a trusted non-SHAKEN entity such as an Authoritative Database as described in ATIS-1000067 [Ref 2]. When adding "rcd" PASSporT claims to a "shaken" PASSporT, the combined SHAKEN and RCD authentication service shall sign the "shaken" PASSporT with the credentials of an STI certificate as defined in ATIS-1000074-E [Ref 1].

5.2.1.3 RCD Authentication provided by OSP – "rcd" PASSporT

Based on local policy a SHAKEN OSP may also perform RCD authentication to create an "rcd" PASSporT signed with STI certificate credentials. The protected header and base PASSporT claims shall be populated as described in Clause 5.2.1.1. The "rcd"/"rcdi" claims shall be populated based on vetted information as described in Clause 5.2.1.2. The Protected Header "x5u" parameter shall reference the STI signing certificate. The RCD authentication service performed by the OSP shall create an "rcd" PASSporT only if the criteria for "A" attestation are met; e.g., as specified in ATIS-1000074-E [Ref 1] or based on receiving a valid base PASSporT from the originating customer as described in Clause 6.1 of ATIS-1000092 [Ref 5]. An OSP supporting RCD authentication shall populate either an "rcd" PASSporT or "rcd" claims in a SHAKEN PASSporT but not both on a given call.

5.2.2 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 [Ref 7], 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-E [Ref 1] and ATIS-1000085 [Ref 4] 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-E [Ref 1] and ATIS-1000085 [Ref 4] 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 [Ref 5] shall be applied. (Note, ATIS-1000092 [Ref 5] refers to the base SHAKEN verification procedures in ATIS-1000074-E [Ref 1], 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 RCD verification service shall verify that the constraints are satisfied as specified in RFC 8226 [Ref 13] and draft-ietf-stir-passport-rcd [Ref 7]. 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 shall verify it by re-computing the "rcd" digest as specified in draft-ietf-stir-passport-rcd [Ref 7] and comparing it to the "rcdi" claim. The RCD verification service shall fail verification if the digest does not match the "rcdi" claim value or if the "rcdi" claim value is not enumerated in "rcdi" permittedValues in the JWTClaimConstraints extension (if present) of the certificate. Likewise, where only the "rcd" claim is constrained by the certificate (for cases where the "rcd" claims do not reference external resources and no "rcd" digest is used), verification shall fail if the claim itself is not one of the "rcd" permittedValues. Where the values of "rcd"/"rcdi" are not constrained by the certificate, the verification may succeed but the associated claims are only an indication of the integrity of the claims and resources as populated by the PASSporT creator.

Any HTTPS URLs contained in or referenced by an "rcd" claim are not required to be dereferenceable for an interval longer than the expiry of the PASSporT containing the "rcd" claim.

5.2.2.1 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) in 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, *SIP: Session Initiation Protocol* [Ref 8]; RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks* [Ref 9]; and draft-wendt-sipcore-callinfo-rcd, *SIP Call-Info Parameters for Rich Call Data* [Ref 6]:
   - 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 party device if the calling party has requested privacy (e.g., the received terminating INVITE request contains a Privacy header field with a privacy type of "id").

5.2.3 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 purposes; to determine the attestation level during SHAKEN authentication, and as a source of rich call data that is conveyed to the TSP. The OSP decision to process "rcd" PASSporTs received in originating INVITE requests is based 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-E [Ref 1] (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 [Ref 5], 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[5], then the OSP shall either include the "rcd" PASSporT in the INVITE request sent towards the TSP, or include the "rcd" PASSporT claims in the "shaken" PASSporT and discard the "rcd" PASSporT. The OSP may utilize an "rcdi" or "rcd" value specified in JWTClaimConstraints/permittedValues as evidence the "rcd" claims and (if applicable) associated resources have been vetted by the certificate issuer, or per local policy the OSP may utilize other sources of vetted calling name and enhanced caller identity information to determine the validity of the "rcd" claims and associated resources for population in the "shaken" PASSporT.

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

5.2.4 TSP Procedures when received INVITE contains "rcd" PASSporT

As with the OSP, the TSP decision to process 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 may convey the rich call data contained in the "rcd" PASSporT to the called endpoint as described in Clause 5.2.2.1.

If verification fails, then:

- If the INVITE request is not retargeted, the TSP shall discard the "rcd" PASSporT, and shall not convey the rich call data contained in the PASSporT to the called endpoint.
- If the INVITE request is retargeted, then the disposition of the "rcd" PASSporT is based on TSP local policy. For example, the retargeting TSP could decide to include the failed "rcd" PASSporT in the retargeted INVITE request in order to provide information that is useful to analytics and traceback functions performed by the retarget-to TSP.

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.

[5] The most straightforward policy is to always send the validated rich call data. However, there may be cases, especially during the initial rollout of RCD, where some destinations cannot handle the additional data (e.g., the inclusion of rich call data causes the message size to exceed some implementation-imposed threshold).