**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.

Table of Contents[**ATIS-1000XXX** i](#_Toc6869935)

[ATIS Standard on i](#_Toc6869936)

[**Signature-based Handling of Asserted information using toKENs (SHAKEN): Calling Name and Rich Call Data Handling Procedures** i](#_Toc6869937)

[**Alliance for Telecommunications Industry Solutions** i](#_Toc6869938)

[**Abstract** i](#_Toc6869939)

[Table of Figures iv](#_Toc6869940)

[1 Scope & Purpose 1](#_Toc6869941)

[1.1 Scope 1](#_Toc6869942)

[1.2 Purpose 1](#_Toc6869943)

[2 Normative References 1](#_Toc6869944)

[3 Definitions, Acronyms, & Abbreviations 2](#_Toc6869945)

[3.1 Definitions 2](#_Toc6869946)

[3.2 Acronyms & Abbreviations 2](#_Toc6869947)

[4 Overview 4](#_Toc6869948)

[4.1 SHAKEN CNAM and RCD Model Overview 4](#_Toc6869949)

[5 Delegate Certificate Management 5](#_Toc6869950)

[5.1 Delegate Certificate Overview 5](#_Toc6869951)

[5.1.1 Certificate Authority Delegation via Delegate CA Certificates 5](#_Toc6869952)

[5.2 Authorizing Cross-Certificate constraints per TN Provider 7](#_Toc6869953)

[5.3 Certificate Management Architecture 8](#_Toc6869954)

[5.4 Certificate Management Interfaces 8](#_Toc6869955)

[5.5 Certificate Management Procedures 9](#_Toc6869956)

[5.5.1 Subordinate CA obtains an SPC Token 9](#_Toc6869957)

[5.5.2 Subordinate CA obtains a Delegate CA Certificate 10](#_Toc6869958)

[5.5.3 Customer AF obtains a Delegate End-Entity Certificate 10](#_Toc6869959)

[6 SHAKEN CNAM and RCD Framework Definition 15](#_Toc6869960)

[6.1 ‘rcd’ claim construction overview 15](#_Toc6869961)

[6.1.1 Traditional CNAM using ‘nam’ 15](#_Toc6869962)

[6.1.2 RCD using ‘jcd’ with an embedded jCard 16](#_Toc6869963)

[6.1.3 RCD using ‘jcl’ with a URL to jCard 17](#_Toc6869964)

[6.2 RCD Authentication and Verification Scenarios 18](#_Toc6869965)

[6.2.1 Originating/Terminating endpoints support RCD Authentication/Verification 18](#_Toc6869966)

[6.2.2 Originating Network Scenarios 19](#_Toc6869967)

[6.2.3 Terminating Network Scenarios 22](#_Toc6869968)

[6.2.4 Termination side ‘rcd’ authentication 26](#_Toc6869969)

[6.3 Calling Name Authentication and Verification Scenarios – Third-party service ‘rcd’ authentication 26](#_Toc6869970)

[6.4 UE procedures 26](#_Toc6869971)

[6.4.1 Analog or Limited Text display procedures 26](#_Toc6869972)

[6.4.2 SIP enabled enhanced Text display procedures 26](#_Toc6869973)

[6.4.3 Graphical display procedures 26](#_Toc6869974)

[6.4.4 Local address book procedures(?) 27](#_Toc6869975)

[Appendix A – CNAM and RCD Verified Text based Indicator 28](#_Toc6869976)

[Examples 28](#_Toc6869977)

[Appendix B – CNAM and RCD Verified Graphical Indicator 29](#_Toc6869978)

[Graphics 29](#_Toc6869979)

[SVG Source Code 31](#_Toc6869980)

[Examples 31](#_Toc6869981)

# Table of Figures

[Figure 1. STI-CA delegates authority to a TN Provider Subordinate CA 5](#_Toc6870038)

[Figure 2. The STI-PA authorizes cross-certificate constraints 7](#_Toc6870039)

[Figure 3. Delegate Certificate Management Architecture 8](#_Toc6870040)

[Figure 4. RCD Authentication and Verification 18](#_Toc6870041)

[Figure 5. RCD Authentication at the originating endpoint 19](#_Toc6870042)

[Figure 6. SHAKEN “rcd” claim – originating endpoint does supports RCD authentication 20](#_Toc6870043)

[Figure 7. RCD Identity header – originating endpoint does not support RCD authentication 21](#_Toc6870044)

[Figure 8. Two Identity headers – terminating endpoint supports RCD authentication 22](#_Toc6870045)

[Figure 9. Two Identity headers – terminating endpoint does not support RCD verification 23](#_Toc6870046)

[Figure 10. SHAKEN “rcd” claim – terminating endpoint supports RCD verification 24](#_Toc6870047)

[Figure 11. SHAKEN “rcd” claim – terminating endpoint does not support RCD verification 25](#_Toc6870048)

[Figure 0.1 – Examples of Textual validated indicators 28](#_Toc6870049)

[Figure 0.1 – 1024 px x 1024 px white background 29](#_Toc6870050)

[Figure 0.2 – 128 px, 32 px, 16 px white background 30](#_Toc6870051)

[Figure 0.3 – 1024 px x 1024 px white background 30](#_Toc6870052)

[Figure 0.4 – 128 px, 32 px, 16 px white background 31](#_Toc6870053)

# Scope & Purpose

## Scope

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.

## 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)

RFC 3261, *SIP: Session Initiation Protocol.*4

RFC 7515, *JSON Web Signatures (JWS).*4

RFC 7516, *JSON Web Algorithms (JWA).*4

RFC 7517, *JSON Web Key (JWK).*4

RFC 7519, *JSON Web Token (JWT).*4

RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol*.4

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

RFC 8226, *Secure Telephone Identity Credentials: Certificates*4

# 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’ claim construction overview

In [draft-ietf-stir-passport-rcd] there are three main key values possible as part of the ‘rcd’ claim. They are ‘nam’ which is a minimally required key value as part of the ‘rcd’ claim value JSON object, ‘jcd’ which is the key value that represents the direct inclusion of a jCard string in the ‘rcd’ claim, and ‘jcl’ which is the key value that represents an HTTPS URL link to a jCard file hosted on an HTTPS server. Both the ‘jcd’ and ‘jcl’ key values are optional, can only be included a maximum of one time in a ‘rcd’ claim, and are mutually exclusive where you can not have both key values. The following sections provide more details on how the ‘rcd’ JSON object is constructed.

### Traditional CNAM using ‘nam’

If a SIP INVITE contains a display-name parameter in the From or P-Asserted-Identity header field, then the ‘rcd’ claim must contain a ‘nam’ key value that has a value with a string that matches exactly the ASCII values of the display-name parameter.

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":"Alice"}

}

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":"Alice"}

}

### 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":"James Bond","jcd":["vcard",[["version",{},"text","4.0"],

["fn",{},"text", "James Bond"],

["n",{},"text",["Bond","James","","","Mr."]],

["adr",{"type":"work"},"text",

["","","3100 Massachusetts Avenue NW","Washington","DC","20008","USA"]

],

["email",{},"text","007@mi6-hq.com"],

["tel",{"type":["voice","text","cell"],"pref":"1"},"uri",

"tel:+1-202-555-1000"],

["tel",{"type":["fax"]},"uri","tel:+1-202-555-1001"],

["bday",{},"date","19241116"],

["logo",{},"uri",

"https://upload.wikimedia.org/wikipedia/en/c/c5/Fleming007impression.jpg"

]]]}}

}

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":"James Bond","jcd":["vcard",[["version",{},"text","4.0"],

["fn",{},"text", "James Bond"],

["n",{},"text",["Bond","James","","","Mr."]],

["adr",{"type":"work"},"text",

["","","3100 Massachusetts Avenue NW","Washington","DC","20008","USA"]

],

["email",{},"text","007@mi6-hq.com"],

["tel",{"type":["voice","text","cell"],"pref":"1"},"uri",

"tel:+1-202-555-1000"],

["tel",{"type":["fax"]},"uri","tel:+1-202-555-1001"],

["bday",{},"date","19241116"],

["logo",{},"uri",

"https://upload.wikimedia.org/wikipedia/en/c/c5/Fleming007impression.jpg"

]]]}}

}

### 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":"James Bond","jcl":"https://example.org/james\_bond.json"}

}

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":"James Bond","jcl":"https://example.org/james\_bond.json"}

}

### Integrity Protection of Rich Call Data

[draft-ietf-stir-passport-rcd] specifies how the "rcdi" claim of the "rcd" PASSporT and the STI certificate JWTClaimConstraints extension defined in [RFC 8226] can be used to protect the integrity of the rich call data. The data is protected in two ways; from being maliciously spoofed by the calling entity, and from being maliciously modified en-route to the called destination. 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 a Subordinate CA issues a delegate certificate to a VoIP entity, it must ensure that the certificate is populated with a JWTClaimConstraints object as defined in section 5.2 of [draft-ietf-stir-passport-rcd]; i.e., any PASSporT signed by this delegate certificate must include the "rcd" claim, and must include an "rcdi" claim with one or more permitted values. For example, if the signing VoIP Entity is authorized to use three variations of a company logo, then the JWTClaimConstraints would list three permitted values for the "rcdi" claim; one value for each logo. Verifiers can use the JWTClaimConstraints extension to verify that the signing entity is authorized to use the rich call data contained in and referenced by the "rcd" claim, and also verify that the rich call data was not modified by any 3rd-party after the "rcd" PASSporT was signed.

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".

The vetting process whereby the Subordinate CA determines the set of rich call data that the VoIP Entity is authorized to use is outside the scope of this document.

## RCD Authentication and Verification Procedures

### RCD Authentication

The RCD-AS shall perform RCD authentication as specified in [draft-ietf-stir-passport-rcd].

The RCD-AS shall populate the “rcd” PASSporT “orig”, “dest”, and “iat” claims with the same procedures as specified for the ‘shaken’ PASSporT defined in [ATIS-1000074-E].

The RCD-AS shall include an “rcd” claim containing a “nam” key with a “nam” key value that is set as follows:

* The P-Asserted-Identity header field display name parameter value shall be used, if present, otherwise the From header field display name parameter value shall be used.
* If there are two P-Asserted-Identity header fields that contain a display name parameter, then the RCD authentication service shall have logic to choose the most appropriate one based on local service provider policy.
* If there is no display name parameter in either the P-Asserted-Identity or From header fields, then the “nam” key value shall be an empty string.

The RCD-AS shall populate the remaining key value pairs of the “rcd” claim based on provisioned data.

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

The Protected Header “x5u” parameter shall reference a delegate end-entity certificate as defined in [ATIS delegate-cert document]. The RCD-AS shall sign the “rcd” PASSporT with the private key of the delegate end-entity certificate referenced by the “x5u” parameter.

### RCD Verification

The RCD-VS shall verify a received “rcd” PASSporT as specified in [draft-ietf-stir-passport-rcd].

The RCD-VS shall determine the validity of the certificate referenced in the “x5u” field in the “rcd” PASSporT protected header, applying the basic path validation as defined in [RFC 5280]. The basic steps are as follows:

1. The RCD-VS shall retrieve the certificate referenced by the “x5u” field in the “rcd” PASSporT protected header from the STI-CR.
2. The RCD-VS shall verify that the certificate is a delegate end-entity certificate; i.e., both the certificate and its parent certificate contain a TNAuthList object.
3. The RCD-VS shall verify that the TNAuthList of the parent certificate in the certificate path contains a single SPC value, and at least one TN. The RCD-VS shall also verify that the scope of the TNAuthList of the parent certificate encompasses the scope of the child certificate TNAuthList. The RCD-VS shall repeat this verification step for each delegate certificate in the certificate path.
4. The RCD-VS shall follow the basic certificate path processing as described in [RFC 5280], following the chain until the root is reached (i.e., Issuer name=Subject name).
5. The STI-VS shall verify that the root certificate is on the list of trusted STI-CAs.

The RCD-VS shall verify the “orig”, “dest”, and “iat” claims as specified in [ATIS-1000074-E] and [ATIS-1000085]. In addition, the RCD-VS shall 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.

The RCD-VS shall verify the “rcd” claim “nam” key value as follows:

* The P-Asserted-Identity header field display name parameter value shall be checked as the display name to be validated if present, otherwise the display name parameter of the From header field value shall be checked.
* If there are two P-Asserted-Identity display name parameter values, the verification service shall check each of them until it finds one that is valid.
* If there is no display name parameter in the P-Asserted-ID(s) or From header fields, then the RCD-VS shall verify that the “nam” key value is the null string.

## Extension to SHAKEN Authentication and Verification Procedures

### SHAKEN Authentication

If dictated by local policy, the STI-AS shall include an “rcd” claim in the “shaken” PASSporT constructed during SHAKEN authentication. The STI-AS shall populate the key value pairs of the “rcd” claim as specified in section 5.2.1. Otherwise, the STI-AS shall perform SHAKEN authentication as specified in [ATIS-1000074-E].

The STI-AS shall not add an “rcd” claim to a SHAKEN PASSporT if the received originating INVITE request already contains an RCD Identity header.

### SHAKEN Verification

The STI-VS shall verify the “nam” key value of the “rcd” claim received in a “shaken” PASSporT as specified in section 5.2.2. Otherwise, the “shaken” PASSporT is verified as specified in [ATIS-1000074-E].

## RCD Authentication and Verification Scenarios

There are a number of methods that CNAM and RCD authentication and verification scenarios can be implemented in a VoIP network between the originating and terminating telephone service providers as part of a SHAKEN implementation. This section details the procedures involved in some of the common implementations of these scenarios. This isn’t intended to be a complete list, rather illustrating example deployments.

### End-to-End Flow

#### Originating/Terminating Customer AFs support RCD Authentication/Verification

Figure 4 shows the message flow for providing authenticated rich-call-data to the called endpoint for a case where TN-a calls TN-b. At origination time, the TN-a Customer AF hosts an RCD-AS that performs RCD authentication, and adds an RCD Identity header to the originating INVITE request at (1). This Identity header is carried more-or-less transparently across the network, and delivered to the terminating Customer AF RCD-VS at (4). The terminating Customer AF RCD-VS verifies the received “rcd” PASSporT, and displays the received rich-call-data to the user, along with an appropriate indication that the call-data has been authenticated.

On receiving the originating INVITE from the Customer AF, the originating SP STI-AS performs normal SHAKEN authentication, and adds a second Identity header containing a “shaken” PASSporT to the INVITE at (2). Based on local policy, the originating SP may verify the received “rcd” PASSPorT, and use the result to determine the SHAKEN attestation level. Otherwise, SHAKEN proceeds normally. On receiving the terminating INVITE at (3), the terminating SP STI-VS verifies the “shaken” PASSporT, and populates a Vertstat parameter in the P-Asserted-Identity header to convey the SHAKEN verification result to the terminating Customer AF.



Figure 4. RCD Authentication and Verification

The following sub-clauses describes additional scenarios that vary based on the ability of the Customer AFs to support RCD authentication and verification, and vary based on the [draft-ietf-stir-passport-rcd] options chosen by the originating and terminating service providers to provide some level of RCD to endpoints that don’t support the RCD authentication/verification procedures.

### Originating Network Scenarios

#### Originating Customer AF supports RCD Authentication

Figure 5 shows the case where the originating Customer AF supports the RCD authentication procedures, and has obtained a delegate end-entity certificate from its TN Provider, as described in [ATIS-delegate-cert spec]. This scenario shows the case where the originating SP is also the TN Provider; i.e., the originating SP hosts the STI-CR that contains the delegate end-entity certificate.

1. At call origination time, the RCD-AS shall perform RCD authentication as specified in section 5.2.1.
2. On receiving the originating INVITE request from the Customer AF, the originating SP STI-AS shall perform SHAKEN authentication as specified in [ATIS-1000074-E]. Based on local policy, the originating SP may choose to verify the received RCD Identity header, and use the verification results as part of its criteria to determine the value of the SHAKEN “attest” claim. For example, if the originating SP is not authoritative for calling TN-a (e.g., in a multi-hosted PBX case), but it is able to verify that the received “rcd” PASSporT is valid, then it may choose to provide SHAKEN authentication with full attestation. The originating SP adds a second Identity header containing the newly created SHAKEN PASSporT to the INVITE.



Figure 5. RCD Authentication at the originating Customer AF

#### Add SHAKEN “rcd” claim for Originating Customer AF that does not support RCD-AS

Figure 6 shows the case where the originating Customer AF does not support RCD authentication, and local policy at the originating SP dictates that for this customer, the STI-AS must add an “rcd” claim to the “shaken” PASSporT during SHAKEN authentication.

1. On receiving the originating INVITE request from the customer AF, the STI-AS shall add an “rcd” claim to the “shaken” PASSporT as specified in section 5.3.1.



Figure 6. Add SHAKEN “rcd” claim for originating endpoint that does not support RCD authentication

#### Add 2nd RCD Identity Header for Originating Customer AF that does not support RCD-AS

Figure 7 shows the case where the originating Customer AF does not support RCD authentication, and local policy at the originating SP dictates that for this customer, the STI-AS must perform RCD authentication and add a second Identity header.

On receiving the originating INVITE request from the Customer AF:

1. The originating STI-AS shall perform SHAKEN authentication as specified in [ATIS-1000074-E].
2. The RCD-AS shall perform RCD authentication as specified in section 5.2.1.



Figure 7. RCD 2nd Identity header for originating endpoint that does not support RCD authentication

### Terminating Network Scenarios

#### SHAKEN & RCD Identity Headers received – Terminating Customer AF supports RCD-VS

Figure 8 shows the case where the terminating network receives two Identity headers – one SHAKEN and one RCD – and the terminating Customer AF supports the RCD verification.

1. On receiving the terminating INVITE request from the originating SP, the terminating STI-VS shall cache both Identity headers for later traceback. STI-VS shall perform SHAKEN verification as specified in [ATIS-1000084-E]. The terminating SP shall maintain local per-endpoint capabilities data that indicates whether or not each endpoint supports RCD verification. Since in this case the called endpoint *does* support RCD verification, the terminating SP shall ignore the received RCD Identity header, and pass it transparently to the called endpoint in the terminating INVITE request.
2. On receiving the terminating INVITE request containing an RCD Identity header from the terminating SP, the Customer AF RCD-VS shall perform RCD verification, as specified in section 5.3.2.



Figure 8. Two Identity headers – terminating Customer AF supports RCD verification

#### SHAKEN & RCD Identity Headers received – Terminating Customer AF does not support RCD-VS

Figure 9 shows the case where the terminating network receives two Identity headers – one SHAKEN and one RCD – and the terminating Customer AF supports the RCD verification.

On receiving the terminating INVITE request from the originating SP:

1. The STI-VS shall verify the SHAKEN Identity header as specified in section 5.4.3.1.
2. The RCD-VS shall verify the RCD Identity header as specified in section 5.2.2.



Figure 9. Two Identity headers – terminating endpoint does not support RCD verification

#### SHAKEN PASSPporT “rcd” claim received – Terminating Customer AF supports RCD Verification

Figure 10 shows the case where the terminating network receives a single SHAKEN Identity header containing a “shaken” PASSporT with an “rcd” claim, and the terminating Customer AF supports RCD verification.

On receiving the terminating INVITE request from the originating SP:

1. The STI-VS shall verify the SHAKEN Identity header as specified in section 5.4.3.1.
2. The RCD-AS shall construct an “rcd” PASSporT containing an “rcd” claim that matches the “rcd” claim from the received “shaken” PASSporT, sign it with a delegate end-entity certificate, and include it in an RCD Identity header added to the INVITE request sent to the terminating Customer AF.

On receiving the terminating INVITE request from the terminating SP:

1. The Customer AF RCD-VS shall verify the received “rcd” PASSPorT as specified in section 5.2.2



Figure 10. SHAKEN “rcd” claim – terminating endpoint supports RCD verification

#### SHAKEN PASSporT “rcd” claim received – Terminating Customer AF does not support RCD-VS

Figure 11 shows the case where the terminating network receives a single SHAKEN Identity header containing a “shaken” PASSporT with an “rcd” claim, and the terminating Customer AF does not support RCD verification.

On receiving the terminating INVITE request from the originating SP:

1. The STI-VS shall verify the SHAKEN Identity header as specified in section 5.3.2.
2. The terminating SP shall send the rich-call-data information from the “rcd” claim to Customer AF in the terminating INVITE request via TBD.



Figure 11. SHAKEN “rcd” claim – terminating endpoint does not support RCD verification

## UE procedures

Provide basic guidelines for how CNAM and RCD are rendered to user. A framework that only has basic rules to make sure there is consistency in providing identity information to user, to the extent the display is capable of displaying information with different priority levels and clear indication of validation of the CNAM/RCD information.

In the jCard specification there is a large set of different identity information that is available, not all displays have either the ability or screen space to render an unlimited amount of data. The following is a suggested set of prioritized data to display for CNAM/RCD.

First priority: Calling Name

Second priority: Telephone number

Third priority: logo, image, City/State from address, full address, additional telephone numbers, email address

### Analog or Limited Text display procedures

Most analog or textual displays only have the ability to show CNAM information, possibly the telephone number. When the CNAM information is verified, the UE must render the “[V]” string before the Calling Name on the display for as many characters available for the display.

Optionally, UEs that read the CNAM using a text to speech synthesizer may interpret the “[V]” characters as the ability to announce “Verified Caller”.

### SIP enabled enhanced Text display procedures

In the case of future SIP based UEs that have textual displays, the use of “[V]” should follow the procedures defined above in the last section above. Optionally, a SIP enabled UE that understands verstat or can verify the ‘rcd’ claim in the identity header can provide a clear separate “verified” indicator or a dedicated LCD icon corresponding to the graphical display procedures defined in the next section below.

Optionally, UEs that read the CNAM using a text to speech synthesizer may interpret the inclusion of verstat or validation of the ‘rcd’ claim in an identity header directly as the ability to announce “Verified Caller”.

### Graphical display procedures

The CNAM and RCD data should be displayed to the extent possible in priority order. The verified CNAM/RCD icon, defined in Appendix B, should be displayed

If there is any logos or images included in a jCard, the verified icon should not ever be rendered in the same space as the image or logo to prevent any confusion of parts of the image/logo with the verified logo.

### Local address book procedures(?)

Optionally, define rules for providing validation of local/network address book entries based on comparing information passed in CNAM/RCD.

# Appendix A – CNAM and RCD Verified Text based Indicator

## Examples

Below shows photos of example usage of “[V]”

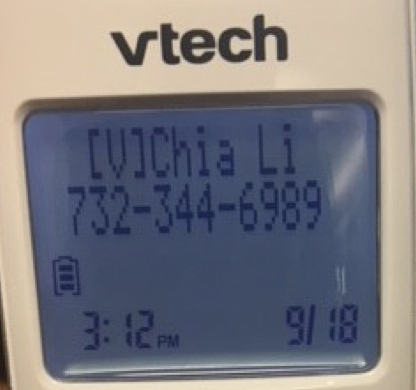
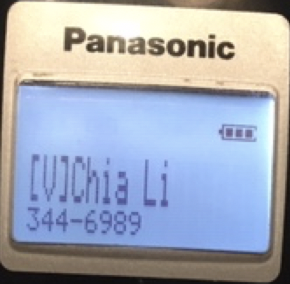
 

Figure 0.1 – Examples of Textual validated indicators

# Appendix B – CNAM and RCD Verified Graphical Indicator

## Graphics

The icon indicating CNAM and RCD information is verified is designed to be used on light and dark background as shown in the below figures. The size of the icons can be modified to be appropriate for the device, so the exact pixel sizes are for example only, however the proportions should remain exact and the icon should remain as consistent as possible to promote recognizability by consumers. The icon MUST not be combined with any other images or graphics where the icon could be spoofed in any way and should stand on its own or combined with reinforcing “verified” words to make a clear impression that the CNAM or RCD information is verified.



Figure 0.1 – 1024 px x 1024 px white background

Figure 0.2 – 128 px, 32 px, 16 px white background



Figure 0.3 – 1024 px x 1024 px white background

Figure 0.4 – 128 px, 32 px, 16 px white background

## SVG Source Code

The SVG representation of the icon is as follows.

<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg width="100%" height="100%" viewBox="0 0 1024 1024" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" xml:space="preserve" xmlns:serif="http://www.serif.com/" style="fill-rule:evenodd;clip-rule:evenodd;stroke-linecap:round;stroke-linejoin:round;stroke-miterlimit:1.5;">

<path id="path" d="M512,13L419.05,134.885L280.103,70.158L254.442,221.277L101.331,228.536L148.838,374.271L16.638,451.853L126.43,558.817L45.427,688.948L192.352,732.637L181.102,885.507L331.501,855.912L392.582,996.5L512,900.401L631.418,996.5L692.499,855.912L842.898,885.507L831.648,732.637L978.573,688.948L897.569,558.817L1007.36,451.853L875.162,374.271L922.669,228.536L769.557,221.277L743.897,70.158L604.95,134.885L512,13Z" style="fill:rgb(61,166,0);fill-rule:nonzero;"/>

<g transform="matrix(0.931161,0,0,0.931161,5.06784,64.0201)">

<path d="M765.35,337.248L459.32,643.279L318.177,502.136" style="fill:none;stroke:white;stroke-width:128.87px;"/>

</g>

</svg>

## Examples

Below shows examples of icon usage on graphical displays

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)