Telecommunications Standards Advisory Committee (TSAC)

Technical Specification

Calling Name Service (CNS)

IMDA TS CNS
Issue 1 Rev 1, December 2025

Info-communications Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Acknowledgement

The Info-communications Media Development Authority (IMDA) and the Telecommunications Standards Advisory Committee (TSAC) would like to acknowledge the following members of the TSAC Task Force (TF) for their invaluable contributions to the preparation of this Technical Specification:

List of TSAC TF Members (2025)

TF Chairman:

Mr Harin S Grewal	Infocomm Media Development Authority (IMDA)

TF Members:

Mr Lim Wai Yean	Infocomm Media Development Authority (IMDA)
Mr Sim Bak Chor	Infocomm Media Development Authority (IMDA)
Ms Christina Goh	M1 Limited
Mr Walter Klomp	MyRepublic Group Limited
Mr Benjamin Tan	Simba Telecom Pte. Ltd.
Mr Hng Sze Hong	Simba Telecom Pte. Ltd.
Ms Adeline Lee	Singapore Telecommunications Ltd (Singtel)
Mr Tan Wee Tiong	Singapore Telecommunications Ltd (Singtel)
Mr Abdullah Bin OTHMAN	StarHub Ltd
Ms Janet Aw Lay Kuan	StarHub Ltd
Mr Nathan Steele	Supernet Limited
Ms Wing-yan Louey	Supernet Limited
Ms Airika Takeguchi	The Government Technology Agency of Singapore (GovTech)
Mr Paul Hong	The Government Technology Agency of Singapore (GovTech)
Mr Au Yeong Pak Wai	Verizon Communications Singapore Pte Ltd.
Mr Dong Jae Kum	Verizon Communications Singapore Pte Ltd.

Telecommunications Standards Advisory Committee (TSAC)

The TSAC advises IMDA on the setting of ICT standards as well as on the development and recommendation of specifications, standards, information notes, guidelines and other forms of documentation for adoption and advancement of the standardisation effort of the Singapore ICT industry (hereafter termed "IMDA Standards").

Telecommunications standards-setting in Singapore is achieved with the assistance of TSAC, where professional, trade and consumer interest in telecommunications standards is represented on the TSAC with representatives from network and service operators, equipment suppliers and manufacturers, academia and researchers, professional bodies and other government agencies.

List of TSAC Members (2024-2027)

TSAC Chairman:

Dr Chin Woon Hau	Director (Technology and Standards) Infocomm Media Development Authority (IMDA)

TSAC Members:

Mr George Choo	President Association of Telecommunications Industry of Singapore (ATIS)
Mr Andy Phang	Assistant Director, Technology and Standards Infocomm Media Development Authority (IMDA)
Mr Marcus Tan Cheng Lin	Head of Cybersecurity Department Institute for Infocomm Research (I2R)
Mr Denis Seek	CTO M1 Limited
Mr Ng Thian Khoon	Head, Broadcast Engineering/ Broadcast Engineering (Technology) Mediacorp Pte Ltd
Associate Professor Chau Yuen	Associate Professor, School of Electrical & Electronic Engineering Provost's Chair in Wireless Communications Nanyang Technological University (NTU)
Dr Biplab Sikdar	Head of Department, Electrical and Computer Engineering, & Area Director (Communications & Networks) National University of Singapore (NUS)
Mr Gao Peng	Head of Radio Planning Simba Telecom Pte. Ltd.
Professor Susanto Rahardja	Professor, Engineering Cluster Singapore Institute of Technology (SIT)
Mr Lim Yu Leong	Vice President, Group Strategy, Engineering & Innovation Singapore Telecommunications Ltd (Singtel)
Professor Tony Quek	Head of Information Systems and Technology Design Pillar; Cheng Tsang Man Chair Professor Singapore University of Technology and Design (SUTD)
Mr Heng Hwee Tong	Head of Engineering and Corporate IT SP Telecomunications (SPTel) Pte. Ltd.

Mr Eddie Teo Soo Kwok	Assistant Vice President, Radio Technology StarHub Ltd

Contents

NOTICE

The Info-communications Media Development Authority (“IMDA”) makes no representation or warranty of any kind with regard to the material provided herein and excludes any express or implied warranties or conditions of non-infringement, merchantability, satisfactory quality and fitness for a particular purpose. Subject to the maximum extent permitted under law, IMDA shall not be responsible or liable to you or any third party for any errors and/or omissions contained herein or for any losses or damages (including any loss of profits, business, goodwill or reputation, and/or any special, incidental or consequential damages) in connection with the use of this material.

IMDA reserves the right to change, modify or add to any part of this document. Nothing herein is intended to create or impose any binding legal obligations or liability whatsoever on IMDA, whether expressed or implied, and whether contractual or otherwise. Without prejudice to the foregoing, nothing in this document shall bind IMDA to adopt any particular course of action. Consequently, nothing herein shall be construed as granting any expectation, whether procedural or substantive in nature, that IMDA will take or not take any particular course of action in the future, arising from or due to anything in this document or in the exercise of its discretion as a public authority.

IMDA draws attention to the possibility that ANY practice or implementation of this Standard/Specification may involve the use of Intellectual Property Rights and takes no position concerning the existence, validity and/or applicability of any such Intellectual Property Rights, whether asserted by TSAC members or any third party.

As of the date of issuance of this Standard/Specification, IMDA has not received written notice of any patent rights which may be relevant in relation to the implementation of this Standard/Specification. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to check with the relevant database in ITU, ISO, IEC or the relevant Standards Development Organisation for information of intellectual property rights. Implementers are advised to obtain their own professional, technical and/or legal advice and conduct all necessary due diligence, including but not limited to making such investigations or seeking clarifications as may be appropriate, in regard to any decision or action that they intend to take, or prior to the implementation of any Standard/Specification as may be required.

Technical Specification for Calling Name Service

1 Scope

This specification establishes the requirements and recommendations for the call authentication, verification and display mechanisms for the implementation of calling name service (CNS) and thus provide assurance for calls to consumers in Singapore.

It provides requirements and recommendations for the following entities:

1. Originating Service Providers (OSP):
    a. Authentication/attestation of calls originating from their calling name subscribers
    b. Generation and insertion of authentication data
    c. Association and insertion of pre-registered call information for the authenticated calls

2. Intermediary Network Carriers (INC):
    a. Transparent transmission of authentication data throughout the call path
    b. Preservation of call information integrity during transit

3. Terminating Service Providers (TSP):
    a. Verification of incoming calls using received authentication data
    b. Validation of call information authenticity
    c. Processing and delivery of authenticated call information to the recipient's display device

This specification is applicable to:

- OSP that offers CNS to their subscribers
- INC that provides domestic call-routing
- TSP that terminates domestic calls to their subscribers

2 References

For the technical requirements captured in this Specification, reference has been made to the following standards. Where versions are not indicated, implementation of this Specification shall be based on current and valid versions of these standards published by the respective Standards Development Organisations.

1. IETF RFC 8224: “Authenticated Identity Management in the Session Initiation Protocol (SIP) Description: Defines the PASSporT (Personal Assertion Token) format for conveying cryptographically-signed information about the caller.”

2. IETF RFC 8225: “PASSporT: Personal Assertion Token Description: Specifies the PASSporT format in detail, including how to create and validate these tokens.”

3. IETF RFC 8226: “Secure Telephone Identity Credentials: Certificates Description: Outlines the certificate policies and management procedures for the X.509 certificates used in STIR.”

4. IETF RFC 8588: “Based on ATIS 1000074, Personal Assertion Token (PASSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN) Description: Defines how PASSporT is used within the SHAKEN (Signature-based Handling of Asserted information using toKENs) framework.”

5. IETF RFC 9795: “PASSporT Extension for Rich Call Data: Defines how to authenticate and include Rich Call Data in PASSporT tokens. Specifies methods for signing and verifying additional caller information. Enables secure transmission of caller names, logos, and other display data.”

6. IETF RFC 9796: “SIP Call-Info Parameters for Rich Call Data: Specifies how to carry Rich Call Data in SIP signaling using Call-Info headers. Defines the format and parameters for transmitting RCD in SIP messages. Provides the transport mechanism for delivering authenticated caller display information.”

7. IETF RFC 8946: “Personal Assertion Token (PASSporT) Extension for Diverted Calls Description: Defines a PASSporT extension ("div") to handle call forwarding scenarios Enables verification of call authentication when calls are redirected. Maintains the chain of trust across multiple forwarding events.”

8. ATIS-1000074: “Signature-based Handling of Asserted information using toKENs (SHAKEN)", is a framework that defines the protocols and procedures for implementing STIR/SHAKEN call authentication and verification services.”

9. ATIS-1000080: “SHAKEN: Governance Model and Certificate Management Description: Outlines the governance model and certificate management procedures for the SHAKEN ecosystem.”

10. ATIS-1000085: “SHAKEN Support of "div" PASSporT Extension Description: Specifies how the "div" PASSporT extension for diverted calls is supported in SHAKEN.”

11. ATIS-1000094: “Calling name and RCD handling procedures: Introduces mechanisms for authentication, verification, transport of calling name and other enhanced caller identity information (e.g., images, logos), and call reason.”

3 Abbreviations

AS	Application Server
ATIS	Alliance for Telecommunications Industry Solutions
CNS	Calling Name Service
CR	Certificate Repository
ID	Identity
IETF	Internet Engineering Task Force
INC	Intermediary Network Carrier
OSP	Originating Service Provider
PASSporT	Personal Assertion Token
RCD	Rich Call Data
RFC	Request for Comments
S-CSCF	Serving Call Session Control Function
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiated Protocol
STIR	Secure Telephone Identity Revisited
TSP	Terminating Service Provider
URI	Uniform Resource Identifier

4 System architecture

4.1 This informative section introduces a generic system architecture for CNS.

4.2 Call authentication in integrated CNS provides a robust mechanism for validating call origins and delivering verified caller identification information. Figure 1 depicts a typical system architecture of CNS, actual implementation may differ. The solid red arrows depict the scope of this specification.

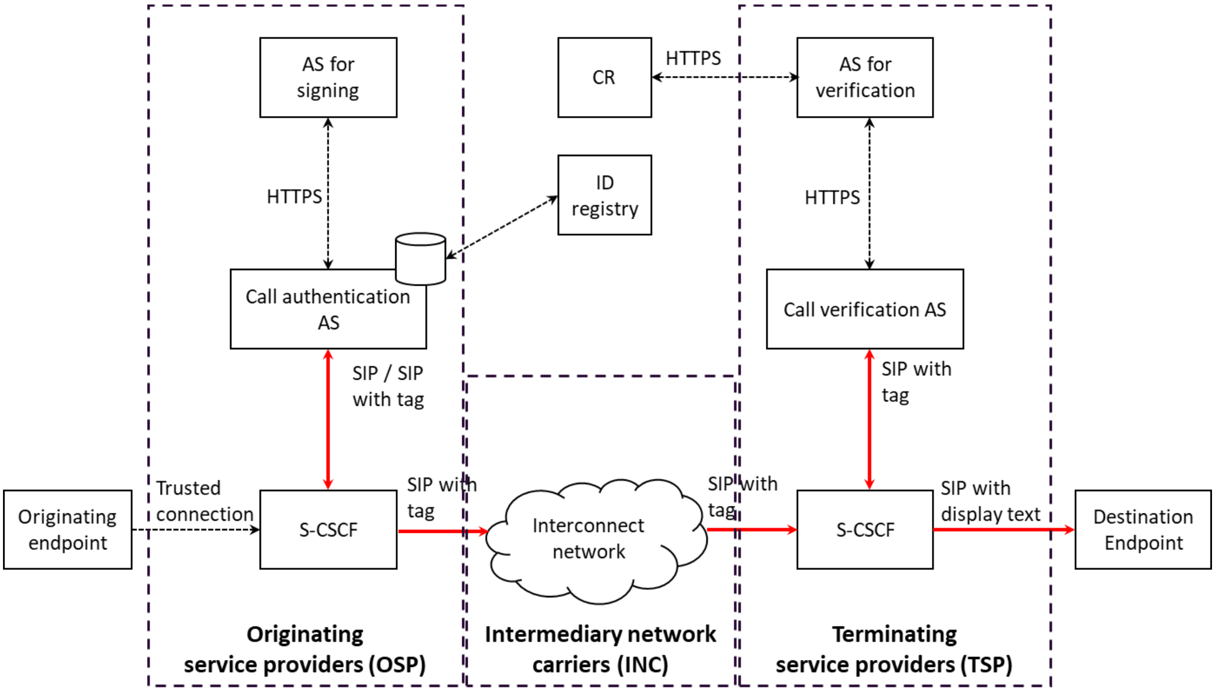

Figure 1. Typical CNS system architecture

4.3 The authentication process initiates at the Originating Service Provider (OSP), where two key operations occur:

a. Call authentication using the STIR/SHAKEN framework

b. Calling name enrichment provided by the ID registry

4.4 On reception of the call from the originating endpoint, over trusted connection, the OSP “call authentication application server (AS)” function authenticates the call based on pre-defined rules, not defined by this specification.

4.5 OSP can associate the trusted connection with its customer, an organisation whose unique calling names are pre-registered with the authoritative ID registry. OSP references an internal database for the bindings between calling names and calling numbers.

4.6 This bound calling name, along with the authentication data, is cryptographically signed by the “AS for signing” function and encoded into a PASSporT (Personal Assertion Token). The token is then embedded in the SIP signalling message using an Identity header.

4.7 During call routing, intermediary network carriers (INC) maintain the integrity of both the authentication token and calling name information by ensuring transparent transmission of all SIP signalling elements, particularly preserving the Identity header containing the PASSporT.

4.8 Upon receiving the call, the Terminating Service Provider (TSP) executes a two-stage verification:

a. "AS for verification" function validates the PASSporT signature against the certificate from the certificate repository (CR)

b. "Call verification AS" function verifies the authenticity of the embedded calling name information

4.9 Following successful verification, the TSP "call verification AS" function processes the authenticated calling name information and presents it to the destination endpoint. This provides recipients with assurance of the call's origin and verified calling party identification from the authoritative source.

4.10 Note that this specification assumes end-to-end SIP connectivity.

5 Existing standards and their relationships

5.1 This informative section introduces the relationships between the existing standards referenced by this specification. Figure 2 below depicts the simplified relationship between the existing standards.

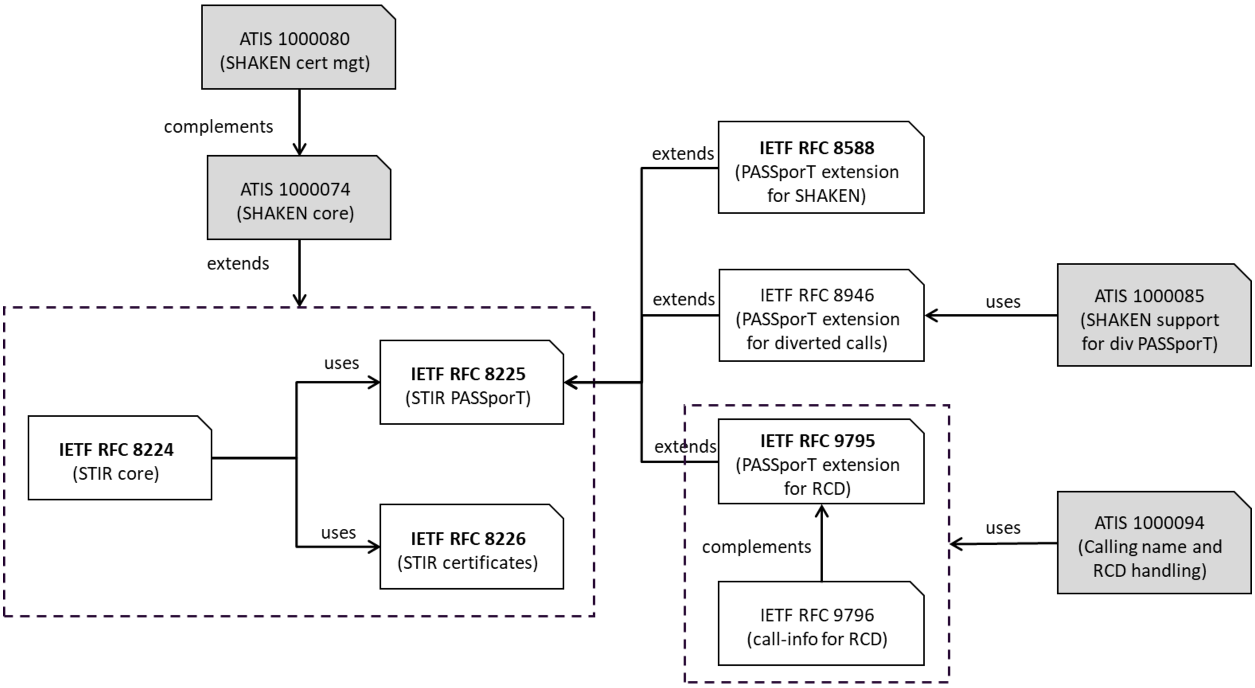
ATIS 1000080 (SHAKEN cert mgt)
complements
ATIS 1000074 (SHAKEN core)
extends
uses
IETF RFC 8225 (STIR PASSporT)
IETF RFC 8224 (STIR core)
uses
IETF RFC 8226 (STIR certificates)
extends
IETF RFC 8588 (PASSporT extension for SHAKEN)
extends
IETF RFC 8946 (PASSporT extension for diverted calls)
uses
ATIS 1000085 (SHAKEN support for div PASSporT)
extends
IETF RFC 9795 (PASSporT extension for RCD)
complements
IETF RFC 9796 (call-info for RCD)
uses
ATIS 1000094 (Calling name and RCD handling)

Figure 2. Existing standards and their relationships

5.2 Call authentication and verification, are standardised by RFC 8224, RFC 8225, and RFC 8588, which form the core of the authentication process:

- RFC 8224 defines how to use PASSporT tokens within SIP for authenticating caller identity.

- RFC 8225 specifies the detailed structure of PASSporT tokens.

- RFC 8588 tailors the use of PASSporT specifically for the SHAKEN framework.

5.3 ATIS-1000074 provides the SHAKEN framework and additional guidance for implementation of the STIR standard.

5.4 The overall STIR/SHAKEN standardised process works as follows:

a. When a call is initiated, the originating service provider creates a PASSporT token containing call details.

b. This token is cryptographically signed using certificates as specified in RFC 8226.

c. The signed PASSporT is then embedded in the SIP signaling (as per RFC 8224) and transmitted with the call.

d. The terminating service provider receives the call, extracts the PASSporT, verifies its signature and validate caller information using the public key infrastructure defined in RFC 8226 and ATIS-1000080.

5.5 Caller name display is enhanced through several of these standards:

- RFC 8588 allows for the inclusion of attestation levels in the PASSporT, which can influence how the caller ID is displayed.

- IETF RFC 9795 extends PASSporT to include Rich Call Data (RCD), which can contain caller names and other display information. This extended PASSporT is verified by the terminating service provider at network level.

- IETF RFC 9796 complements IETF RFC 9795 to allows RCD to be carried in Call-info headers for delivery to end-devices.

5.6 For call diversion/forwarding scenarios, RFC 8946 and ATIS-1000085 is needed:

- RFC 8946 defines the "div" PASSporT extension for representing diverted calls.

- ATIS-1000085 specifies how this extension is implemented within the SHAKEN framework.

This allows the authentication and caller name display to work correctly even when calls are diverted or forwarded.

5.7 For certificate management, RFC 8226 and ATIS-1000080 work together to manage the certificates used in the authentication process:

- RFC 8226 defines the structure and policies for the certificates.
- ATIS-1000080 outlines how these certificates are managed within the SHAKEN ecosystem, including issuance, revocation, and governance.

6 General requirements

6.1 The following standards shall be supported:

S/N	Standard	Description
1	IETF RFC 8224	Main document for STIR.
2	IETF RFC 8225	Specifies the PASSporT format in detail, including how to create and validate these tokens.
3	IETF RFC 8226	Outlines the certificate policies and management procedures for the X.509 certificates used in STIR.
4	IETF RFC 8588	PASSporT extension for SHAKEN.
5	IETF RFC 9795	Defines how to authenticate and include Rich Call Data in PASSporT tokens.

6.2 The following standards may be supported:

S/N	Standard	Description
1	IETF RFC 9796	Specifies how to carry Rich Call Data in SIP signaling using Call-Info headers.
2	IETF RFC 8946	Defines a PASSporT extension ("div") to handle call forwarding scenarios.
3	ATIS-1000074	Main document for SHAKEN
4	ATIS-1000080	Outlines the governance model and certificate management procedures for the SHAKEN ecosystem.
5	ATIS-1000085	Specifies how the "div" PASSporT extension for diverted calls is supported in SHAKEN.
6	ATIS-1000094	Introduces mechanisms for authentication, verification, transport of calling name and other enhanced caller identity information (e.g., images, logos), and call reason.

6.3 OSP shall authenticate and validate the identity of CNS subscribers and their calling numbers, using a “Know Your Customer” (KYC) process and trusted connection, not defined by this specification.

6.4 OSP shall check against ID registry for the caller information associated with its CNS subscribers.

6.5 OSP shall map caller information to numbers and number-ranges, owned by its CNS subscriber.

6.6 OSP shall digitally sign the following elements:

a. The validated caller number

b. The associated caller information

6.7 OSP shall modify the SIP INVITE request to include:

a. The caller information

b. The full form PASSporT

6.8 OSP shall ensure authentication data and caller information is formatted, according to the clause 7.

6.9 For domestic call routing, INC shall forward all authentication data and caller information without modification

6.10 TSP shall perform the following verification steps for incoming SIP INVITE requests that include authentication data:

a. Validate the signing credentials, include certificate path validation, ensuring certificate is valid and not expired/revoked

b. Verify the authenticity of the digital signature, using the public key from the certificate

c. Check the integrity of the authentication data, e.g. ensuring timestamp has not expired, originating number matches calling number and terminating number matches called number

d. Check the integrity of the caller information, also known as RCD verification

6.11 For successful SIP INVITE requests validation, TSP shall:

a. Process the authenticated caller information

b. Update the relevant authentication-related SIP INVITE headers for display, according to clause 8.

c. Deliver the updated SIP INVITE requests to the recipient's device

TSP may implement local policy that helps protect against incorrect or rogue implementation of STIR/SHAKEN standard.

6.12 TSP shall implement display mechanisms that:

a. Present caller information in a standardised format

b. Ensure consistent display across different recipient devices

7 Data structure-related requirements

7.1 The enhanced “SHAKEN” PASSporT, with “rcd” claim, shall consist of:

- Attestation level (attest)
- Terminating number (dest)
- Timestamp (IAT)
- Originating number (orig)
- Origination ID (origid)
- Caller information (rcd)

The caller information shall also include a “rcdi” claim, when the “rcd” claim contains URIs referencing external content.

An example of a "SHAKEN" extension PASSporT that includes "rcd" claim and “rcdi” claim:

```
Protected Header
{
"alg":"ES256",
"typ":"passport",
"ppt":"shaken",
"x5u":"https://biloxi.example.org/biloxi.cer"
}
Payload
{
"attest":"A"
"dest":{"tn":[“8123 4567"]},
"iat":1607000294,
"orig":{"tn":“6377 3800"},
"origid":"123e4567-e89b-12d3-a456-426655440000",
"rcd":{"nam":“IMDA", "jcl":"https://example.org/imda.json" },
"rcdi":<computed per IETF RFC 9795>
}
```

An example of a full form PASSporT in Identity header:

```
Identity: eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1I \
joiaHR0cHM6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ \
kZXN0Ijp7InVyaSI6WyJzaXA6YWxpY2VAZXhhbXBsZS5jb20iXX0sImlhdC \
I6IjE0NDMyMDgzNDUiLCJvcmlnIjp7InRuIjoiMTIxNTU1NTEyMTIifX0.r \
q3pjT1hoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjpjlk-cpFYpFYs \
ojNCpTzO3QfPOlckGaS6hEck7w;info=<https://biloxi.example.org \
/biloxi.cert>;ppt="shaken"
```

8 Display-related requirements

8.1 TSP shall support the following display mechanisms:

a. Use of SIP "from" header for calling name; and

b. Use of SIP "p-asserted-identity" header for calling name

TSP shall use the SHAKEN PASSporT "nam" claim to populate the supported display mechanisms for delivery to the recipient's device.

8.2 In addition to clause 8.1, TSP shall support the use of 3GPP "verstat" parameter to indicate the verification status of the calling number in "from" header and "p-asserted-identity" header.

Example usage of "verstat" in SIP headers:

```
From: "IMDA" <sip:+6563773800@imda.gov.sg>;verstat=TN-Validation-Passed
P-Asserted-Identity: "IMDA" <sip :+6563773800@imda.gov.sg>;verstat=TN-Validation-Passed
```

8.3 In addition to clause 8.1, TSP may support the use of call-info parameters for RCD, according to "IETF RFC 9796".

Example usage of "Call-Info" in SIP headers:

```
From: "IMDA" < sip:+6563773800@imda.gov.sg; user=phone>;tag=1928>
Call-ID: a84b4c76e66710
Call-Info: <data:>;purpose=jcard;verified="true"
Call-Info: <https://imda.gov.sg/photos/q-
256x256.png>;purpose=icon;verified="true";integrity="sha256-RojgWwU6xUtI4q82+kHPyHm
1JKbm7+663bMvzymhkl4"
```

9 Authentication-related requirements

9.1 OSP shall include an enhanced "SHAKEN" PASSporT, according to clause 7, into SIP INVITE requests to support the implementation of CNS.

9.2 OSP shall populate the "Identity" header field of the originating SIP INVITE message with the full form of the resulting "SHAKEN" PASSporT.

9.3 OSP shall generate and provision a unique origination ID (origID), in the enhanced "SHAKEN"

PASSporT, to assist in traceback.

9.4 OSP shall provide “A” attestation signing to support the implementation of CNS, i.e. the customer is authenticated and its right to its right to use the calling number is verified.

9.5 OSP shall provision the “rcd” claim with a “nam” key value that holds the ID registry pre-registered name of the caller.

9.6 OSP shall add the “rcd” PASSporT claims to an enhanced “SHAKEN” PASSporT.

9.7 OSP shall set the “alg” parameter to “ES256”, for signing algorithm.

9.8 OSP shall set the “iat” parameter to current time and use NumericDate format (i.e. Unix timestamp).

9.9 OSP shall set the "x5u" parameter, in the protected header in the “SHAKEN” PASSporT, to reference the signing credentials.

10 Verification-related requirements

10.1 TSP shall verify the enhanced “SHAKEN” PASSporT containing “rcd” PASSporT claims, when it is present.

10.2 TSP shall re-compute the “rcd” digest and compare it against the “rcdi” claim, when it is present.

10.3 TSP shall verify that “iat” parameter is within recommended tolerance, +/- 60 seconds from current time.

10.4 As highlighted in clause 8.2, TSP shall use the SHAKEN PASSporT “nam” claim to populate the supported display mechanisms for delivery to the recipient’s device.

10.5 For failed signature validation, including missing/erroneous/conflicting parameters, TSP shall log failure reason, remove all forms of rich call data and proceed the call with calling name set as “”, according to clause 8.

10.6 For unauthenticated calls, including those with attestation “B” or lower, TSP shall remove all forms of rich call data and replace calling names with “” if present, according to clause 8.

11 Exclusions

11.1 This specification does not specify:

a. how OSP identify and validate its subscriber

b. what and how caller information is pre-registered into the ID registry

c. the implementation of the credential infrastructure

12 Additional information

12.1 For diverted or forwarded calls, CNS requires the support of PASSporT extension for diversion.

12.2 For roaming callers and callees, CNS requires the transparent transmission of SIP authentication headers over foreign networks.