**ATIS IPNNI Task Force**

**May 11, 2021**

**Virtual**

**Contribution**

**TITLE: Baseline Text for Draft ATIS Standard on SIP RPH Signing using PASSPorT Tokens (Revised)**

**SOURCE\*: Peraton Labs and CISA ECD**

**ISSUE NUMBER:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Abstract**

This contribution revised baseline text for Draft ATIS standard on SIP RPH Signing using PASSPorT Tokens. It incorporates the agreements at the May 11-13, 2021 meeting shown as revision marks against IPNNI-2021-00056R000.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following is a summary of global changes:

1. Addressed editor’s note with global replacement of “TN PASSPorT” with “shaken” PASSPorT,
2. Consistent use of “PASSPorT,” “rph” PASSPorT,” “shaken” PASSPorT instead of token throughout the document,
3. Consistent use of “NS/EP Priority Service”, and
4. Consistent use of “RPH.”

The following is a summary of changes:

1. Abstract: Text was clarified to explicitly indicate NS/EP Priority Services calls (i.e., with the “ETS” and “WPS” namespace parameter values).
2. Updated Table of Contents
3. Clause 1.1: Text clarification of the scope to explicitely indicate that the scope is limited to calls with the “ETS” and/or “WPS” namespaces. Addition of text to indicate that signing and verifying attestations of the caller ID of NS/EP calls is covered in [ATIS-1000074] and not in the present document.
4. Clause 1.2: General text clarifications.
5. Clause 1.3: The list of assumptions in clause 1.3 was updated and redundant items covered in the body of the document deleted.
6. Clause 2: Updates to reference list.
7. Clause 3: minor edits.
8. Clause 4 (Overview): General clarifications. Addition of text changes to allow signing of a SIP re-INVITE when the RPH is added for the first time in an exising SIP dialogue.
9. Clause 4.1: Text clarification of the scope to explicitely indicate that the scope is limited to calls with the “ETS” and/or “WPS” namespaces.
10. Clause 4.1.1: Change “Service Provider Identifier” to “SPC” and deletion of the note.
11. Clause 4.1.2: addition of a NOTE to link IETF RFC 8224 to the SHAKEN descriptions of the STI-AS and STI-VS.
12. Clause 4.1.3: minor edits
13. Clause 4.1.4: Deletion of clause 4.1.4 on Diverted Calls.
14. Clause 4.2: Clause 4.2 text on call validation treatment and Display was modified and moved to clause 5.3.
15. Clause 4.3: Text clarifications.
16. Clause 4.4: General clarification of the architecture. Text addition to indicate that the reference architecture is a logical model and does not impose any restrictions on implementations.
17. Clause 4.5: Clarification edits to the example call flow.
18. Clause 5: Added clarifications and edits.
19. Subclause 5.1: Deletion of redundant [IETF RFC 8225] information.
20. Subclause 5.2.1: Text replacement for redundant [IETF RFC 8443] information
21. Subclause 5.2.2: Deletion of redundant [IETF RFC 8443] information and added clarifications
22. Subclause 5.2.3: Replace redundant [IETF RFC 8443] information with procedure descriptions
23. Subclause 5.2.4: Replace redundant [IETF RFC 8443] information with procedure descriptions
24. Subclause 5.3: deletion of redundant [IETF RFC 8443] information
25. Clause 6: This entire clause is deleted to remove requirements on NS/EP NGN-PS Service Providers, and limiting the document scope to procedures for signing and verifying “rph” claims only.
26. Annex A: All informative material including call flow examples are deleted to keep the document simple and focused only on logical functions for RPH signing and verifying.

**ATIS-10000XX**

ATIS Standard on

**National Security / Emergency Preparedness Priority Service Session Initiation Protocol Resource-Priority Header (SIP RPH) Signing and Verifying using PASSPorT**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This standard defines how an extension to the IETF PASSporT [IETF RFC 8443] and the associated Secure Telephone Identity Revisted (STIR) mechanisms are used to sign the Session Initiation Protocol-Resource Priority Header (SIP RPH) field of National Security / Emergency Preparedness (NS/EP) Priority Services calls (i.e., calls containing the “ETS” and/or “WPS” namespace parameter values) and convey assertions of authorization for Resource-Priority. Specifically, this standard provides a mechanism for an originating Service Provider to cryptographically-sign the SIP RPH field of an authorized NS/EP Priority Service call and allow a receiving Service Provider to verify the validity of the authorization for Resource-Priority and act on the information with confidence (i.e., verifying that the RPH information has not been spoofed or compromised).

**Foreword**

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [**COMMITTEE NAME**] Committee [**INSERT MISSION**]. [**INSERT SCOPE**].

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 a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, [**COMMITTEE NAME**], 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, [**COMMITTEE NAME**], which was responsible for its development, had the following leadership:

[**LEADERSHIP LIST**]

The **[SUBCOMMITTEE NAME]** Subcommittee was responsible for the development of this document.

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
|  |  |  |  |

# Table of Contents

[1 Scope & Purpose 1](#_Toc69483254)

[1.1 Scope 1](#_Toc69483255)

[1.2 Purpose 1](#_Toc69483256)

[1.3 General Assumptions 2](#_Toc69483257)

[2 Normative References 2](#_Toc69483258)

[3 Definitions, Acronyms, & Abbreviations 3](#_Toc69483259)

[3.1 Definitions 3](#_Toc69483260)

[3.2 Acronyms & Abbreviations 3](#_Toc69483261)

[4 Overview 4](#_Toc69483262)

[4.1 SIP RPH Signing Protocols Overview 5](#_Toc69483263)

[4.1.1 Personal Assertion Token (PASSporT) 5](#_Toc69483264)

[4.1.2 Authenticated Identity Management in the Session Initiation Protocol 5](#_Toc69483265)

[4.1.3 PASSporT Extension for Resource-Priority Authorization 5](#_Toc69483266)

[4.2 Governance Model and Certificate Management 6](#_Toc69483271)

[4.3 Reference Architecture for SIP RPH Signing 6](#_Toc69483272)

[4.4 SIP RPH Signing Call Flow for NS/EP NGN-PS 8](#_Toc69483273)

[5 Procedures for SIP RPH Signing 10](#_Toc69483274)

[5.1 PASSporT Token Overview 10](#_Toc69483275)

[5.2 Token Constuction and Procedures 10](#_Toc69483276)

[5.2.1 PASSporT & Identity Header Construction 10](#_Toc69483277)

[5.2.2 PASSporT Extension “rph” 10](#_Toc69483278)

[5.2.3 STI-AS (RPH-AS) Procedures 11](#_Toc69483279)

[5.2.4 STI-VS (RPH-VS) Procedures 11](#_Toc69483280)

[5.2.5 Verification Error Conditions 12](#_Toc69483281)

[5.2.6 Use of the Full Form of PASSporT 12](#_Toc69483282)

[5.3 Other Considerations 12](#_Toc69483283)

[5.3.1 Call Validation Treatment (CVT) 12](#_Toc69483284)

[5.3.2 Display 12](#_Toc69483285)

# Table of Figures

[Figure 1 – Architecture for Signing and Verifying SIP RPH of NS/EP Calls 7](#_Toc69483298)

# Scope & Purpose

## Scope

[IETF RFC 4412] specifies use of the SIP 'Resource-Priority' Header (SIP RPH) field for communications Resource-Priority. As specified in [IETF RFC 4412], the SIP RPH field may be used by SIP user agents, including Public Switched Telephone Network (PSTN) gateways and terminals, and SIP proxy servers to influence prioritization afforded to communication sessions, including PSTN calls.

The SIP RPH “ETS” and “WPS” namespace parameters are defined and used to support National Security / Emergency Preparedness (NS/EP) Priority Service calls which includes Wireless Priority Service (WPS), Government Emergency Telecommunication Service (GETS) and Next Generation Network Priority Services (NGN-PS) calls in IP-based networks. However, the SIP RPH field could be spoofed and abused by unauthorized entities impacting NS/EP Priority Service communications. For example, NS/EP Service Providers receiving SIP RPHs across IP Network-to-Network Interconnections (IPNNIs) have difficulty determining whether the SIP RPH was populated by an authorized NS/EP Service Provider, or whether it was spoofed or inserted by an unauthorized entity.

This ATIS standard describes a framework leveraging the Signature-based Handling of Asserted information using toKENs (SHAKEN) model specified in [ATIS-1000074] to cryptographically sign and verify the SIP RPH field of NS/EP Priority Service calls using the “rph” PASSPorT extension defined in [IETF RFC 8443] and the associated Secure Telephone Identity (STI) protocols. There are some cross relationships between caller ID signing and verifying using a “shaken” PASSPorT and SIP RPH signing and verifying using the “rph” PASSPorT extension defined in [IETF RFC 8443]. However, caller ID signing and verifying using SHAKEN is not a NS/EP Priority Service requirement per se; it is only discussed in this standard to highlight cross relationships.

This ATIS standard is intended to provide a framework and guidance on how to use the “rph” PASSPorT extension defined in [IETF RFC 8443] and the associated STI protocols to cryptographically sign and verify the SIP RPH field in support of a trust mechanism for NS/EP Priority Service calls crossing IPNNI boundaries.

The scope of this ATIS standard is limited to cryptographic signing and verifying the SIP RPH field of NS/EP Priority Service calls with the “ETS” and “WPS” namespace parameters using the “rph” PASSporT extension defined in [IETF RFC 8443] and the associated STI protocols. The scope of this standard does not include cryptographic signing and verifying attestation of the caller ID of NS/EP Priority Service calls. The procedures to sign and verify attestations of the caller ID in a NS/EP Priority Service call using “shaken” PASSporTs are specified in [ATIS-1000074].

Editor’s note: Change SHAKEN to “shaken”; add quotes around “rph” (both global changes).

## Purpose

Illegitimate spoofing of the SIP RPH with “ETS” and/or “WPS” namespace parameters that are used to support NS/EP Priority Service calls is a concern for NS/EP Service Providers. NS/EP Service Providers have difficulty in determining whether a call with a SIP RPH received over IPNNIs with multiple service providers should be trusted and admitted with the SIP RPH. The purpose of this standard is to provide a framework to cryptographically sign and verify SIP RPH field containing “ETS” and/or “WPS” namespace parameters that can be used as a trust mechanism to mitigate against unauthorized spoofing or tampering of the SIP RPH field. The framework provided in this ATIS standard can be used in the originating network authorizing NS/EP Priority Service calls to sign a PASSPorT claim for the RPH field of a SIP INVITE before it is sent across an IPNNI boundary and for the receiving network to verify the PASSPorT claim for the RPH field to decide whether the call should be admitted with the RPH field..

## General Assumptions

The following general assumptions are made in this standard:

1. SIP RPH signing is only performed by an authenticating NS/EP Service Provider (e.g., NS/EP Service Provider performing WPS and/or GETS authorization).
2. An NS/EP Service Provider can use the same certificates for signing SIP RPH with “ETS” and “WPS” namespace parameters as they use for signing “shaken” PASSPorTs, but is not required to do so.
3. Based on local policy, an NS/EP Service Provider may choose to honor NS/EP Priority Service calls without a signed RPH or process the calls with normal priority.
	1. This might change over time taking into account the maturity of signed RPH deployments and knowledge of the adjacent carrier.
4. Only the RPH in the initial SIP INVITE request message of an authorized NS/EP Priority Service call is signed or the RPH in a SIP re-INVITE request message of an authorized NS/EP Priority Service call when the “ETS” and/or “WPS” namespaces are included in an exising SIP dialogue for the first time. The RPH in response messages within the session/dialog is not signed.
5. Transit NS/EP Service Providers may verify a signed SIP RPH, but MUST transparently pass the received Identity header associated with the SIP RPH.
6. The NS/EP Service Provider receiving a signed SIP RPH verifies the signed SIP RPH and uses the results to decide whether the call should be admitted with the SIP RPH field based on local carrier policy..
7. The PASSporT extension “rph” defined in [IETF RFC 8443] is used to sign the entire SIP RPH header as opposed to the individual namespaces. The PASSporT object “auth” is defined to convey that the SIP RPH header information is authorized. An NS/EP Service Provider authenticating a Service User would sign the information in the SIP RPH header using the PASSporT “rph” extension and object “auth.” The PASSporT “auth” object conveys authorization for Resource-Priority by the signing NS/EP Service Provider.
8. An NS/EP Service Provider (e.g., authorized provider of GETS and/or WPS) would sign the SIP RPH field of an authorized NS/EP Priority Service call using a “rph” PASSPorT before it is sent across an IPNNI. For example, after performing a GETS PIN authorization or WPS authorization, assertion about the authorization for Resource-Priority is included in a PASSporT “rph” claim in a SIP Identity header.
9. Signing of the caller ID (i.e., Calling Party Telephone Number) using a “shaken” PASSPorT is separate from the signing of the SIP RPH field using a “rph” PASSPorT. A separate SIP Identity header is used for “rph” PASSPorT claims from that used for “shaken” PASSPorT claims (i.e., “shaken” claims about caller ID).
10. What happens inside a carrier’s trust domain to trigger signing and verifying “rph” PASSPorT claims (i.e., with regard to use of tagging, elements responsible for creating/validating PASSPorT tokens, etc.) is carrier-specific and outside the scope of this ATIS standard.

# Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this ATIS 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], *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN).*

[ATIS-1000080], *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance model and certificate management.*

[IETF RFC 8225], *Persona Assertion Token.*[[1]](#footnote-1)

[IETF RFC 8224], *Authenticated Identity Management in the Session Initiation Protocol.*1

[IETF RFC 8226], *Secure Telephone Identity Credentials: Certificates.*1

[IETF RFC 8443], PASSporT Extension for Resource-Priority Authorization. 1

[IETF RFC 3325], *Private Extensions to SIP for Asserted Identity within Trusted Networks.*1

[IETF RFC 3261], *SIP: Session Initiation Protocol.*1

[IETF RFC 5280], *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*1

[IETF RFC 3326], *The Reason Header Field for the Session Initiation Protocol (SIP).*1

[IETF RFC 4412], *Communications Resource Priority for the Session Initiation Protocol (SIP).* 1

# 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

**Government Emergency Telecommunications Service (GETS)** [ATIS-1000057] is one facet of the USA instantiation of Emergency Telecommunication Service (ETS) using public telecommunications networks, offered by government to authorized users for NS/EP purposes. GETS is a circuit-switched form of ETS for voice (and voiceband data) using PIN authorization, in which a user can invoke the service by dialing a GETS-AN or GETS-NT from most phones served by the Public Switched Network (PSN). GETS provides priority treatment across originating, transit and terminating networks.

**NS/EP NGN Priority Services (NS/EP NGN-PS)** [ATIS-1000057] are the evolution of legacy GETS and WPS to achieve service continuity in the packet-switched NGN, and to leverage the NGN to offer new features and priority multimedia services.

Note: NS/EP NGN-PS and NS/EP NGN-GETS are used interchangeably in ATIS standards.

**Wireless Priority Service (WPS)** [ATIS-1000057] is a circuit-switched form of ETS for voice (and voiceband data) using subscription-based authentication, in which a user can invoke the service by dialing a feature code from a WPS-subscribed mobile phone served by a public wireless network. WPS provides priority treatment across originating and terminating public wireless networks, including priority radio resource assignment upon call origination and termination.

Note: Use of “NS/EP Priority Service” in this standard refers to any service supported using the “ETS” and/or ‘WPS namespaces (GETS, WPS and NGN-PS).

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| 3GPP | 3rd Generation Partnership Project |
| ATIS | Alliance for Telecommunications Industry Solutions |
|  |  |
| CPNCRL | Calling Party NumberCertificate Revocation List |
| CSCF | Call Session Control Function |
| CVT | Call Validation Treatment |
| GETSHTTPS | Government Emergency Telecommunications ServiceHypertext Transfer Protocol Secure |
| IBCF | Interconnection Border Control Function |
| IETF | Internet Engineering Task Force |
| IMS | IP Multimedia Subsystem |
| IP | Internet Protocol |
| IPNNI | IP Network-to-Network Interconnection |
| JSON | JavaScript Object Notation |
| JWS | JSON Web Signature |
| NNI | Network-to-Network Interface |
| NS/EPOCSP | National Security / Emergency PreparednessOnline Certificate Status Protocol |
| PASSporT | Personal Assertion Token |
|  |  |
| PKI | Public Key Infrastructure |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| SKS | Secure Key Store |
| SPC | Service Provider Code |
| STI | Secure Telephone Identity |
| STI-AS | Secure Telephone Identity Authentication Service |
| STI-CA | Secure Telephone Identity Certification Authority |
| STI-CR | Secure Telephone Identity Certificate Repository |
| STI-VS | Secure Telephone Identity Verification Service |
| STIR | Secure Telephone Identity Revisited |
|  |  |
| TN | Telephone Number |
| TrGW | Transition Gateway |
| UA | User Agent |
| URI | Uniform Resource Identifier |
|  |  |
| VoIP | Voice over Internet Protocol |
| WPS | Wireless Priority Service |

# Overview

The SHAKEN architecture described in [ATIS-1000074], describes a Call Session Control Function (CSCF) interacting with a Secure Telephone Identity Authentication Service (STI-AS) (in the originating network) and a Secure Telephone Identity Verification Service (STI-VS) (in the terminating network) for attestion, signing and verifying the caller ID of a call.

The present document is an ATIS standard that describes a framework leveraging the SHAKEN model specified in [ATIS-1000074] to cryptographically sign and verify the SIP RPH field of NS/EP Priority Service calls with the “ETS” and/or “WPS” namespace parameters using the “rph” PASSPorT extension defined in [IETF RFC 8443].

The framework specified in this standard can be used to support a trust mechanism for the SIP RPH field of NS/EP Priority Service calls crossing IPNNI boundaries. The basic concept of the framework involves the following;

1. **Origination** **- Secure Telephone Identity Authentication Service (STI-AS) for RPH**: The originating NS/EP Service Provider cryptographically signs the RPH in the initial SIP INVITE request message of an authorized NS/EP Priority Service call (e.g., WPS, GETS or NGN-PS call) using the “rph” PASSPorT extension defined in [IETF RFC 8443] and includes a SIP Identity header before it is sent across an IPNNI boundary. The originating NS/EP Service Provider may also cryptographically signs the RPH in a SIP re-INVITE when the “ETS” and/or “WPS” namespace parameters are included in an exising SIP dialogue for the first time for an authorized NS/EP Priority Service call. The SIP RPH signing is only performed for authorized NS/EP Priority Service calls by an authenticating NS/EP Service Provider (i.e., NS/EP Service Provider performing GETS or WPS authorization of the NS/EP Service User).
2. **Termination** **- Secure Telephone Identity Verification Service (STI-VS)**  **for RPH**: The receiving terminating NS/EP Service Provider verifies the received “rph” PASSPorT for the SIP RPH field in the SIP INVITE message. The result of the verification of the “rph” PASSPorT is used by the terminating NS/EP Service Provider to decide whether the RPH field should be kept or stripped based on carrier policy.

**NOTE:** A Transit NS/EP Service Provider may verify a received SIP identity header with a “rph” PASSPorT for the SIP RPH field (i.e., to determine priority treatment within its network), but MUST transparently pass the received Identity header associated with the SIP RPH field.

## SIP RPH Signing Protocols Overview

This ATIS standard uses the “rph” PASSPorT extension specified in [IETF RFC 8443] and associated STIR protocols for cryptographic signing and verifying the SIP RPH field of NS/EP Priority Service calls (i.e., calls with the “ETS” and/or “WPS” namespace parameters).

The following provides an overview of the associated IETF STIR protocols.

### Personal Assertion Token (PASSporT)

[IETF RFC 8225] defines a token-based signature that combines the use of JavaScript Object Notation (JSON) Web Tokens, JSON Web Signatures, and X.509 certificate key pairs, or Public Key Infrastructure (PKI), to create a trusted signature. The authorized owner of the certificate used to generate the signature can be validated and used to trace back to the known trust anchor who signed the certificate. The PASSporT includes a number of claims the signer of the token is asserting. The associated public certificate is used to verify the digital signature and the claims included in the PASSporT token. The public certificate is also used to validate the entity that signed the token through a Service Provider Code (SPC), as defined in [IETF RFC 8226]. The validated claims and the validated identity of the entity signing the claims can both be used to determine the level of trust in the originating entity and their asserted SIP RPH information.

### Authenticated Identity Management in the Session Initiation Protocol

[IETF RFC 8224] defines a SIP-based framework for an authentication service and verification service using the PASSporT signature in a SIP INVITE. It defines a new Identity header field that delivers the PASSporT signature and other associated parameters. The authentication service as defined according to [IETF RFC 8224] adds the Identity header field to the SIP INVITE generated by the originating service provider. The SIP INVITE is delivered to the destination service provider which uses the verification service to verify the signature using the information in the SIP RPH field.

NOTE: The authentication service and verification service defined in [IETF RFC 8224] are viewed as the STI-AS and STI-VS functions defined in the SHAKEN framework [ATIS-1000074].

### PASSporT Extension for Resource-Priority Authorization

[IETF RFC 8443] defines an optional extension “rph” to PASSporT and the associated STIR mechanisms to provide a function to sign the SIP RPH field. It extends PASSporT to allow cryptographic-signing and verifying of the SIP RPH field which is used for communications resource prioritization. It also describes how the “rph” PASSPorT extension is used in SIP signaling to convey assertions of authorization of the information in the SIP RPH field.

## Governance Model and Certificate Management

[IETF RFC 8443] indicates that the credentials (e.g., authority responsible for authorizing resource-priority) used to create the signature must have authority over the "rph" claim and indicates that there can only be one authority per claim. The authority MUST use its credentials (i.e., CERT) associated with the specific service supported by the SIP namespace in the claim.

The Emergency Communication Division (formerly OEC and formerly NCS) under the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) is the authority for NS/EP Priority Services and the claims associated with the “ETS” and “WPS” namespace parameters. . ECD/CISA/DHS delegates “ETS” and “WPS” namespace signing authority to NS/EP Service Providers.

The governance model and the management of the credentials (i.e., certificates) used by NS/EP Service Providers for cryptographic signing of the SIP RPH is not within the scope of this standard.

NOTE: NS/EP NGN-PS Service Providers can use the same certificates for signing SIP RPH as they use for SHAKEN (i.e., Caller ID signing) including the associated SHAKEN governance and certificate management defined in [ATIS-1000080], but are not required to do so.

## Reference Architecture for SIP RPH Signing

The SHAKEN architecture described in [ATIS-1000074], describes a Call Session Control Function (CSCF) interacting with a Secure Telephone Identity Authentication Service (STI-AS) (in the originating network) and a Secure Telephone Identity Verification Service (STI-VS) (in the terminating network) where the STI-AS and STI-VS are SIP application servers.

Figure 1 below shows a reference architecture for signing and verifying the SIP RPH calls with “ETS” and “WPS” namespace parameters. It is an extension to the SHAKEN architecture defined in [ATIS-100074] for signing and verifying the SIP RPH of NS/EP Priority Service calls across IPNNIs. In Figure 1, the NS/EP Priority Service call is originated from service provider A’s network that performs the STI-AS function, and the NS/EP Priority Service call is terminated in service provider B’s network, which performs the STI-VS function in accordance to the procedures defined in [IETF RFC 8443] for a “rph” PASSPorT. In Figure 1, the functional elements within black rectangular boxes are IMS and SHAKEN elements as described in [ATIS-1000074] while the dotted red boxes are introduced functional elements necessary to realize signing and verifying the SIP RPH of NS/EP Priority Service calls.



Figure 1 – Architecture for Signing and Verifying SIP RPH of NS/EP Calls

The reference architecture includes the following elements:

**IMS Elements:**

* SIP User Agent (SIP UA) – This component represents the originating and terminating end points for an NS/EP Priority Service session.
* IMS/Call Session Control Function (CSCF) – This component represents the SIP registrar and routing function. It also has a SIP application server interface.
* Session Border Controller – Interconnection (SBC-I) (Interconnection Border Control Function (IBCF)/Transition Gateway (TrGW) – This function is at the edge of the service provider network and represents the Network-to-Network Interface (NNI) or peering interconnection point between telephone service providers. It is the ingress and egress point for SIP calls between providers.

**SHAKEN Elements**

* Secure Telephone Identity Authentication Service (STI-AS) – Defined in [ATIS-1000074].
* Secure Telephone Identity Verification Service (STI-VS) – Defined in [ATIS-1000074].
* Call Validation Treatment (CVT) – Defined in [ATIS-1000074].
* Secure Key Store (SKS) – Defined in [ATIS-1000074].
* Certificate Provisioning Service – Defined in [ATIS-1000074].
* Secure Telephone Identity Certificate Repository (STI-CR) – Defined in [ATIS-1000074].

**NS/EP NGN-PS Elements**

* Telephone Application Server (TAS) – This element represents telephone application processing and routing. It may include some aspects of NS/EP Priority Services call handling. .
* NS/EP NGN-PS Application Server (NS/EP NGN-PS AS) – This element represents NS/EP NGN-PS processing and routing. It is viewed as the element responsible for GETS and WPS authorization.
* RPH Authentication Service (RPH-AS) – This element represents the logical authentication service for SIP RPH signing defined in [IETF RFC 8443].

NOTE: The logical RPH-AS function is not required to perform the WPS or GETS authorization. It is responsible for verifying that an NS/EP NGN-PS entity (e.g., NS/EP NGN-PS AS or TAS) has authorized the Service User for the NS/EP Priority Service call. .

* RPH Verification Service (RPH-VS) - This element represents the logical verification service for SIP RPH signing defined in [IETF RFC 8443].

In keeping with the SHAKEN architecture described in [ATIS-1000074], Figure 1 shows a CSCF interacting with a STI-AS (in the originating network) and a STI-VS (in the terminating network). The RPH–AS in Figure 1 represents logical STI-AS functions for RPH signing and the RPH–VS represents logical STI-VS functions for verifying signed RPH in accordance with the procedures defined in [IETF RFC 8443]. The logical RPH-AS function is not required to perform the NS/EP Priority Service call authorization (i.e., WPS or GETS authorization). The RPH-AS function is responsible for verifying that an NS/EP NGN-PS entity (e.g., NS/EP NGN-PS AS or TAS) has authorized the Service User for the NS/EP Priority Service call. For example, an NS/EP Priority Service call is sent to a RPH-AS function to be signed after the WPS or GETS authorization had been performed by an NS/EP NGN-PS entity (e.g., by the NS/EP NGN-PS AS or TAS). The trigger mechanism to send a NS/EP Priority Service call to sign the SIP RPH field is based on carrier specific implementation and out of scope of this ATIS standard.

The reference architecture in Figure 1 is a logical model and does not impose any restrictions on implementations. Figure 1 shows interactions between a CSCF and SIP based Application Servers where the Application Servers provide the logical STI-AS (RPH-AS) and STI-VS (RPH-VS) functions and may interact via an Ms interface (as defined in 3GPP 24.229) using HTTP with Application Servers to sign and verify the SIP RPH field. Other approaches not shown in Figure 1 are also possible such as an SBC-I (IBCF/TrGW) providing the logical STI-AS (RPH-AS) and STI-VS (RPH-VS) functions and may interact via an Ms interface (as defined in 3GPP TS 24.229) using HTTP with Application Servers to sign and verify the SIP RPH field.

## SIP RPH Signing Call Flow for NS/EP NGN-PS

Figure 2 below illustrates a possible SIP RPH signing and verifying call flow, based on the example architecture illustrated in Figure 1.



Figure 2 – NS/EP SIP RPH Signing and Verifying Call Flow Example

1. The originating SIP UA sends a SIP INVITE for a NS/EP Priority Service call.
2. Based on the dialed digits (e.g., WPS FC or GETS AN), the originating Service ProviderA routes the call to the NS/EP NGN-PS AS for priority processing and handling (e.g., WPS or GETS authorization).
3. The NS/EP NGN-PS AS appends a Resource Priority Header with “ETS” and/or “WPS” namespace parameters to the SIP INVITE after authorizing the NS/EP Priority Service call request.
4. The originating Service Provider A routes the SIP INVITE to the STI-AS (RPH-AS function).

NOTE: The STI-AS must be invoked after originating call processing and after the WPS or GETS authorization. The mechanism to send a NS/EP NGN-PS call to the STI-AS to sign the SIP RPH field is based on carrier specific policy and implementation (e.g., solution specific mechanism identifying calls egressing the carrier trusted SIP domain).

1. The RPH-AS function of the STI-AS in the originating Service Provider network A determines through service provider-specific means the legitimacy of the content of the RPH field (i.e., ETS and WPS namespaces) being used in the SIP INVITE. The STI-AS then securely requests its private key from the SKS.
2. The SKS provides the private key in the response, and the STI-AS signs the RPH field in the INVITE per [IETF RFC 8443] and adds an Identity header field per [IETF RFC 8224].
3. The STI-AS after signing the RPH field, passes back the SIP INVITE with the Identity header field for routing.
4. The originating Service Provider A, through standard resolution, routes the call to the egress SBC-I (IBCF/TrGW).
5. The SIP INVITE with the identity header field is routed over the IPNNI through the standard inter-domain routing configuration.
6. The terminating Service Provider B ingress SBC-I (IBCF/TrGW) receives the SIP INVITE over the IPNNI.
7. Based on the presence of the “rph” PASSPorT, the terminating Service Provider B, routes the SIP INVITE to the STI-VS (RPH-AS).

NOTE: The STI-VS must be invoked before terminating call processing.

1. The terminating Service Provider B STI-VS determines the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR as per [ATIS-1000074].
2. The STI-VS (RPH-VS) validates the certificate and then extracts the public key as per [ATIS-1000074]. It constructs the RFC 8224 format and uses the public key to verify the signature in the Identity header field, which validates the RPH field used when signing the INVITE on the originating service provider STI-AS (RPH-AS).
3. The result of the STI verification is used by terminating Service Provider B to determine whether the call is to be admitted and completed with or without the RPH field (This decision is based on local operator and other policies that may be defined outside of this ATIS standard based on NS/EP Priority Service requirements) and the SIP INVITE is passed back to set up the call to the terminating SIP UA according to NS/EP Priority Service procedures.

NOTE: Error cases where verification fails are discussed in clause 5.3.2 of the SHAKEN framework [ATIS-1000074].

1. The terminating SIP UA receives the SIP INVITE and SIP processing of the call according to NS/EP Priority Service procedures continues to set up the media end-to-end.

The above call flow is intended to be illustrative and does not impose any restrictions on implementations. Other approaches not shown in Figure 2 are also possible such as an SBC-I (IBCF/TrGW) providing the logical STI-AS (RPH-AS) and STI-VS (RPH-VS) functions and may interact via an Ms interface (as defined in 3GPP TS 24.229) using HTTP with Application Servers to sign and verify the SIP RPH field.

# Procedures for SIP RPH Signing

[IETF RFC 8224] and [IETF RFC 8225] define a base set of procedures for how STI fits into the SIP call flow. [IETF RFC 8225] defines the procedures for constructing the PASSPorT token. [IETF RFC 8224] defines an authentication service and a verification service corresponding to the STI-AS and STI-VS described in the SHAKEN reference architecture.

[IETF RFC 8443] defines the “rph” PASSPorT extension to sign and verify claims for the SIP RPH field. This section details the procedures required for the STI-AS (RPH-AS) function to create the required identity header and the STI-VS (RPH-VS) function to verify the claims of the identity header for the SIP RPH field, where the STI-AS (RPH-AS) and STI-AS (RPH-VS) are logical functions described in clause 4.4.

## PASSporT Token Overview

STI as defined in [IETF RFC 8225] specifies the process of the PASSporT token. Refer to [RFC 8225] for the process and specific examples of a PASSporT token.

##  Token Construction and Procedures

### PASSporT & Identity Header Construction

The PASSPorT for the “rph” claim shall be constructed as defined using the base PASSPorT defined in [IETF RFC 8225] and the “rph” PASSPorT extension defined in [IETF RFC 8443].

The procedures defined in [IETF RFC 8224] shall be used to construct and include a SIP identity header for the “rph” PASSPorT in the SIP INVITE generated by the originating service provider.

### PASSporT Extension “rph”

The standard PASSporT extension for “rph” shall be used as defined in [IETF RFC 8443] to sign and verify the SIP RPH field with “ETS” and/or “WPS” namespace parameters.

The creator of a PASSporT object adds a "ppt" value of "rph" to the header of a PASSporT object, in which case the PASSporT claims MUST contain an "rph" claim, and any entities verifying the PASSporT object will be required to understand the "ppt" extension in order to process the PASSporT in question. A PASSPorT header with the "ppt" included will appear as follows:

 {

 "typ":"passport",

 "ppt":"rph",

 "alg":"ES256",

 "x5u":"https://www.example.org/cert.cer"

 }

The "rph" claim will provide an assertion of authorization, "auth" for information in the SIP RPH with “ETS” and/or “WPS” namespace parameter fields.

The following is an example "rph" claim for a SIP RPH field with one r-value of "ets.0" and with another r-value of "wps.0":

 {

 "orig":{"tn":"12155550112"},

 "dest":{["tn":"12125550113"]},

 "iat":1443208345,

 "rph":{"auth":["ets.0", "wps.0"]}

 }

After the header and claims PASSporT objects have been constructed, their signature is generated normally per the guidance in [IETF RFC 8225] using the full form of PASSPorT.

According to [IETF RFC 8443], the credentials (i.e., certificate) used to create the signature must have authority over the namespace of the "rph" claim, and there is only one authority per claim. The DHS/CISA/ECD delegates signing authority for “rph” claims with the “ETS” and/or “WPS” namespace parameters. As indicated in clause 4.2, the NS/EP Service Provider can use the same credentials as that used to sign “shaken” PASSPorTs, but is not required to do so.

If r-values are modified, added or dropped by intermediaries along the path, the intermediaries must generate a new "rph" header and sign the claim with their own authority.

The use of the compact form of PASSporT is not specified in [IETF RFC 8443].

###  STI-AS (RPH-AS) Procedures

The STI-AS (RPH-AS) is a logical function that provides the authentication service defined in clause 4.1 of [IETF RFC 8443] with the exceptions and additions specified in this clause.

After NS/EP Priority Service call processing and authorization (i.e., WPS or GETS authorization), the SIP INVITE is sent to the logical STI-AS (RPH-AS) function using a trigger mechanism based on carrier policy and implementation (e.g., when the call is tagged as leaving the carrier’s trusted SIP domain) to sign the SIP RPH field.

The STI-AS (RPH-AS) function derives the value of the “rph” claim after verifying that an NS/EP Priority Service entity (e.g., NS/EP NGN-PS AS or TAS) has authorized the Service User for the NS/EP Priority Service call (i.e., using GETS or WPS authorization), and then securely requests its private key from the SKS.

Upon receiving the private key from the SKS, the STI-AS (RPH-AS) function signs the RPH field and returns an identity header field value for the SIP RPH field.

NOTE: The procedures being defined in 3GPP TS 24.229 for “Priority verification using assertion of priority information” are used for signing and verifying the SIP RPH.

###  STI-VS (RPH-VS) Procedures

The STI-VS (RPH-VS) is a logical function providing the verification service defined in clause 4.2 of [IETF RFC 8443] with the exceptions and additions specified in this clause.

When a terminating NS/EP Priority Service Provider receives an NS/EP Priority Service call with an identity header containing a "ppt" value of "rph", the SIP INVITE is sent to the logical STI-AS (RPH-AS) function using a trigger mechanism based on carrier policy and implementation (e.g., a NS/EP Priority Service call tagged as received from outside of the carrier trusted SIP domain) to verify the signed SIP RPH. The verifier retrieves the certificate referenced in the “rph” PASSporT protected header and follows the basic certificate path processing as described in clause 5.3.1 of [ATIS-1000074], following the chain until the root certificate is reached and ensures that the root certificate is on the list of trusted STI-CAs.

The verifier validates that the “rph” claim including the “iat” claim as specified in clause 4.2 and clause 6.2 of [IETF RFC 8443] respectively. The verifier shall also follow the [RFC 8224]-defined verification procedures to check the corresponding originating identity (i.e., the originating telephone number in the “orig” claim) and destination identity (i.e., the terminating telephone number in the “dest” claim).

If the “rph” claim is successfully validated, the RPH field is considered to be authorized and the SIP INVITE should be admitted with the RPH field and provided priority treatment according to the local carrier policy.

If the “rph” claim validation fails, the RPH field is handled as per local carrier policy. In such cases, the RPH field should be stripped and the call treated as an ordinary call.

NOTE: The procedures being defined in 3GPP TS 24.229 for “Priority verification using assertion of priority information” are used for signing and verifying the SIP RPH.

### Verification Error Conditions

The procedures described in section 5.3.2 of [ATIS-1000074] shall be followed.

### Use of the Full Form of PASSporT

[IETF RFC 8225] supports the use of both full and compact forms of the PASSporT token in the Identity header. The full form of the PASSPorT token shall be used in accordance with [IETF RFC 8443].

## Other Considerations

### Call Validation Treatment (CVT)

Post STI-VS and CVT handling of NS/EP Priority Service calls with signed SIP RPH is specified in [ATIS-1000074] clause 5.3.4 of [ATIS-1000074].

### Display

Conveying the verification status of the “rph” claim to end user devices is not required for NS/EP Priority Service calls with “ETS” and/or “WPS” namespace parameters.

Note: Further study is needed to determine if there is need to define “verstat” parameter values in [3GPP TS 24.229] for “rph” claim status of NS/EP Priority Service calls with “ETS” and/or “WPS” namespace parameters.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-1)