**ATIS IPNNI Task Force**

**November 6-7, 2019**

**Reston, VA**

**Contribution**

**TITLE: Propose changes and updates to Draft ATIS Standard on SIP RPH Signing using PASSPorT Tokens**

**SOURCE\*: Editor: Perspecta Labs**

**ISSUE NUMBER:**

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

**Abstract**

This contribution propose changes and additions to Draft ATIS standard on SIP RPH Signing using PASSPorT Tokens. Changes are shown as revision marks against IPNNI-2019-00125R001.

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

The following is a list of the key changes and additions:

1. Title change to make explicit that the standard is NS/EP specific,
2. Section 1 text updates to be more concise and clear on the assumptions,
3. Section 3 update of references to include published IETF RFCs and addition of new definitions for GETS and WPS,
4. Section 4 updates for alignment with published IETF RFC references and agreement on architecture reference model, and
5. Section 5 updates for alignment with IETF RFC 8443.

**ATIS-10000XX**

ATIS Standard on

**National Security / Emergency Prepardness Next Generation Network Priority Service NS/EP NGN-PS) Session Initiation Protocol Resource Priority Header (SIP RPH) Signing using PASSPorT Tokens**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This standard defines how extension to the IETF PASSporT and the associated STIR mechanisms are used to sign the Session Initiation Protocol Resource Priority Header (SIP RPH) header field and convey assertions of authorization for Resource-Priority. This standard provides a procedure for providing cryptographic authentication and verification of the information in the Session Initiation Protocol Resource Priority Header (SIP RPH) field in Internet Protocol (IP)-based service provider communication networks in support of National Security / Emergency Preparedness Next Generation Priority Services (NS/EP NGN-PS).Specifically, this standard provides a mechanism for a originating NS/EP NGN-PS Service Provider to cryptographically-sign the SIP RPH and allow a receiving NS/EP NGN-PS 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 have 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

[The following is a list of the changes and additions: i](#_Toc23794538)

[1. Update references of published IETF documents: draft-ietf-stir-rph-00 reference to RFC 8443, draft-ietf-stir-passport to RFC 8225, and draft-ietf-stir-rfc4474bis to RFC 8224. i](#_Toc23794539)

**[ATIS-10000XX](#_Toc23794540)** [i](#_Toc23794540)

[ATIS Standard on i](#_Toc23794541)

**[National Security / Emergency Prepardness Next Generation Network Priority Service NS/EP NGN-PS) Session Initiation Protocol Resource Priority Header (SIP RPH) Signing using PASSPorT Tokens](#_Toc23794542)** [i](#_Toc23794542)

**[Alliance for Telecommunications Industry Solutions](#_Toc23794543)** [i](#_Toc23794543)

**[Abstract](#_Toc23794544)** [i](#_Toc23794544)

[Table of Contents iii](#_Toc23794545)

[Table of Figures iv](#_Toc23794546)

[1 Scope & Purpose 1](#_Toc23794547)

[1.1 Scope 1](#_Toc23794548)

[1.2 Purpose 1](#_Toc23794549)

[1.3 General Assumptions 2](#_Toc23794550)

[2 Normative References 3](#_Toc23794551)

[3 Definitions, Acronyms, & Abbreviations 4](#_Toc23794552)

[3.1 Definitions 4](#_Toc23794553)

[3.2 Acronyms & Abbreviations 4](#_Toc23794554)

[4 Overview 6](#_Toc23794555)

[4.1 SIP RPH Signing Protocols Overview 6](#_Toc23794556)

[4.1.1 Persona Assertion Token (PASSporT) 6](#_Toc23794557)

[4.1.2 Authenticated Identity Management in the Session Initiation Protocol 6](#_Toc23794558)

[4.1.3 PASSporT Extension for Resource-Priority Authorization 6](#_Toc23794559)

[4.1.4 PASSPorT Extension for Diverted Calls 6](#_Toc23794560)

[4.2 Call Validation Treatment and Display 7](#_Toc23794561)

[4.2.1 Call Validation Treatment 7](#_Toc23794562)

[4.2.2 Display of Signed SIP RPH NS/EP NGN-PS Calls 7](#_Toc23794563)

[4.3 Governance Model and Certificate Management 7](#_Toc23794564)

[4.4 Reference Architecture for SIP RPH Signing 7](#_Toc23794565)

[4.5 SIP RPH Signing Call Flow for NS/EP NGN-PS 9](#_Toc23794566)

[5 Procedures for SIP RPH Signing 10](#_Toc23794567)

[5.1 PASSporT Token Overview 10](#_Toc23794568)

[5.2 [draft-ietf-rfc4474bis] Authentication procedures 11](#_Toc23794569)

[5.2.1 PASSporT & Identity Header Construction 11](#_Toc23794570)

[5.2.2 PASSporT Extension “rph” 11](#_Toc23794571)

[5.2.3 Origination Identifier (“origid”) 12](#_Toc23794572)

[5.3 4474bis Verification Procedures 12](#_Toc23794573)

[5.3.1 PASSporT Extension & Identity Header Verification 12](#_Toc23794574)

[5.3.2 Verification Error Conditions 12](#_Toc23794575)

[5.3.3 Use of the Full Form of PASSporT 12](#_Toc23794576)

[5.4 SIP Identity Header Example for “rph” Claim 12](#_Toc23794577)

# Table of Figures

[Figure 4.1 – SHAKEN Reference Architecture 4](#_Toc467601252)

[Figure 4.2 – SHAKEN Reference Call Flow 5](#_Toc467601253)

# Scope & Purpose

## Scope

[IETF RFC 4412] specifies the SIP 'Resource-Priority' Header (SIP RPH) field for communications Resource-Priority. As specified in [RFC4412], 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 Next Generation Priority Services (NS/EP NGN-PS) in IP-based networks. However, the SIP RPH field could be spoofed and abused by unauthorized entities impacting NS/EP NGN-PS communications. For example, NS/EP NGN-PS 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 NGN-PS Service Provider or whether it was spoofed, or inserted by an unauthorized entity.

This ATIS standard describes a framework leveraging the SHAKEN model specified in [ATIS-1000074] to cryptographically sign and verify the SIP RPH field of NS/EP NGN-PS calls using the PASSPorT extension defined in [IETF RFC 8443] and the associated Secure Telephone Identity (STI) protocols. The SHAKEN framework used for Telephone Number (TN) signing defined in [ATIS-1000074] is leveraged for SIP RPH signing. There are some cross relationships between TN signing and RPH signing. However, TN signing is not a NS/EP NGN-PS 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 use the 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 NGN-PS calls crossing Internet Protocol Network-to-Network Interconnection (IPNNI) boundaries.

The scope of this ATIS standard is limited to the cryptographic signing and verifying SIP RPH field conveying assertions of the content of the SIP RPH field (i.e., ETS and WPS namespaces). This standard does not change or modify NS/EP NGN-PS call processing, signaling and routing procedures; it simply provides a tool that can be used to support a trust mechanism for NS/EP NGN-PS calls crossing IPNNI boundaries.

n be used to support a trust mechanism for NS/EP NGN-PS calls crossing IPNNI boundaries.

Editor’s Note: Display of NS/EP information to the end user is not part of the scope of this document.

## Purpose

Illegitimate spoofing of the SIP RPH and the “ETS” and “WPS” namespace parameters used to support NS/EP NGN-PS is a concern for NS/EP NGN-PS Service Providers. NS/EP Service Providers have difficulty in determining whether a call with an SIP RPH received over an IPNNI 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 the SIP RPH field and verify that the SIP RPH field can be trusted to mitigate against unauthorized spoofing or tampering of the information. The purpose is to provide a framework on how the PASSPorT rph extension defined in [IETF RFC 8443] can be used leveraging the SHAKEN infrastructure used for Telephone Number (TN) signing to provide a trust mechanism for the SIP RPH of NS/EP NGN-PS calls crossing IPNNIs boundaries.

## General Assumptions

The following general assumptions are made in this standard:

The following general assumptions are made in this document:

1. SIP RPH signing is only performed by an authenticating NS/EP Service Provider.
2. NS/EP call information will not be provided to a 3rd party Call Validation Treatment (CVT) for data analytics as per the Errata of [ATIS 1000074].
3. An NS/EP Service Provider can use the same certificates for signing SIP RPH as they use for TN signing, but is not required to do so.
4. Based on local policy, an NS/EP Service Provider may choose to honor NS/EP NGN-PS calls without a signed RPH or process with normal priority.
   1. This may change over time taking into account the maturity of signed RPH deployments and knowledge of the adjacent carrier.
5. SIP RPH signing does not change or modify NS/EP NGN-PS call processing, signaling and routing procedures; it simply provides a security tool for a receiving provider to determine if the SIP RPH is trusted. The procedures for NS/EP NGN-PS (e.g., GETS and WPS authentication and authorization), and SIP signaling involving populating the namespace parameters of the SIP RPH field is part of normal SIP signaling and NS/EP NGN-PS defined procedures that is separate from the cryptographic authentication (i.e., signing) and verification of the PASSporT claims.
6. Only the RPH in the initial SIP INVITE request message is signed. The RPH in response messages within the session/dialog is not signed.
7. Transit NS/EP Service Providers may validate a signed SIP RPH, but MUST transparently pass the received Identity header associated with the SIP RPH.
8. Display of RPH information is not required. However, a capability to send RPH display information to the device could be used based on local processing (e.g., it can be turned on/off) and policy for NS/EP. [NOTE: Currently, this capability has not been standardized].
9. A WPS authenticating carrier is required to sign the SIP RPH of NS/EP NGN-PS calls leaving its network. If the WPS Service Provider is also doing TN signing, the WPS Service Provider **will** perform both TN signing and SIP RPH signing for a WPS GETS call and then route the call to a GETS Service Provider.
   1. A GETS number has a 710 area code or is one of the alternate 8yy toll free GETS access numbers.
10. The GETS Service Provider receiving a signed SIP RPH may validate the signed SIP RPH, but the NS/EP GETS processing is independent (e.g., the incoming Identity header discarded and is not considered as part of the GETS processing).
11. Treatment of signed SIP RPH validation failures in a terminating carrier is based on carrier policy (i.e., strip RPH or keep RPH).
12. As with TN signing, RPH signing will not survive if there is interworking with the PSTN.
13. 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 NGN-PS 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 NGN-PS Service Provider.
14. An NS/EP NGN-PS Service Provider (e.g., authorized provider of GETS and WPS) would include a PASSporT token signing the SIP RPH field before it is sent across an Internet Protocol Network-to-Network Interconnection (IPNNI). For example, after performing a GETS PIN authentication and authorization, assertion about the authorization for Resource-Priority is included in a PASSporT token claim in a SIP identity header.
15. Signing of telephone numbers (i.e., Calling Party Numbers) is separate from SIP RPH signing. A separate SIP identity header is used for SIP RPH signing from that used for telephone number claims (i.e., SHAKEN assertion about Caller Identity).
16. If a SIP identity header with signed TN for the CPN is received and the initially signaled CPN is modified by the NS/EP NGN-PS Service Provider (e.g., for routing translation or anonymity), the received SIP identity header is stripped and replaced with a new identity header as appropriate.
17. The PASSporT extension mechanism for SIP RPH signing is used by the NS/EP NGN-PS Service Provider as a security protection tool. The originating NS/EP NGN-PS Service Provider is responsible for signing all initial NS/EP NGN-PS SIP INVITEs. However, a receiving Service Provider may decide whether all signed tokens are verified or only selected tokens are verified based on their security policy and threat detection mechanisms. In addition, a receiving Service Provider’s local policy will determine what will happen if a TN PASSporT is either not received or fails validation when an RPH PASSporT is received and validated.
18. An NS/EP Terminating Carrier that receives an INVITE with a validated RPH PASSporT from a known NS/EP carrier but no Resource\_Priority field may reinsert the RPH field in the INVITE after verifying the RPH PASSporT, based on local policy.
19. TN signing is not a NS/EP requirement, however, TN signing for NS/EP calls are done -according to [ATIS-1000074], where the ‘orig’ claim ‘tn’ value are derived using the following rules:
    1. The P-Asserted-Identity header field value shall be used as the telephone identity, if present, otherwise the From header field value shall be used.
    2. If there are two P-Asserted-Identity header field values, the authentication service shall have logic to choose the most appropriate one based on local service provider policy.
    3. The action taken when neither the P-Asserted-Identity header field value nor the From header contain tel URI identities is outside the scope of the SHAKEN framework.
20. What happens inside a carrier’s trust domain (i.e., with regard to use of tagging, elements responsible for creating/validating tokens, etc.) is carrier-specific.
21. A GETS Authentication Carrier can process all types of GETS calls (e.g., GETS AN, NT and PDN). For a GETS call, if the GETS Authentication Carrier is the originating network, it will perform a TN signing based on the original calling party number and the destination number entered during the PIN authentication process. If the GETS Authentication Carrier receives a signed TN from the originating network, the received signed TN is replaced with a TN signing based on the original calling party number and the destination number entered during the PIN authentication process.

# 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.

Editor’s Note: the draft RFCs below will be changed to the normative RFC numbers when available from IETF.

[ATIS-1000074], *ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN).*

[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 interchangeable 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.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| 3GPP | 3rd Generation Partnership Project |
| ATIS | Alliance for Telecommunications Industry Solutions |
| B2BUA | Back-to-Back User Agent |
| CRL | Certificate Revocation List |
| CSCF | Call Session Control Function |
| CVT | Call Validation Treatment |
| HTTPS | Hypertext Transfer Protocol Secure |
| IBCF | Interconnection Border Control Function |
| IETF | Internet Engineering Task Force |
| IMS | IP Multimedia Subsystem |
| IP | Internet Protocol |
| JSON | JavaScript Object Notation |
| JWS | JSON Web Signature |
| NNI | Network-to-Network Interface |
| OCSP | Online Certificate Status Protocol |
| PASSporT | Persona Assertion Token |
| PBX | Private Branch Exchange |
| PKI | Public Key Infrastructure |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| SKS | Secure Key Store |
| SPID | Service Provider Identifier |
| 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 |
| TLS | Transport Layer Security |
| TN | Telephone Number |
| TrGW | Transition Gateway |
| UA | User Agent |
| URI | Uniform Resource Identifier |
| UUID | Universally Unique Identifier |
| VoIP | Voice over Internet Protocol |

# Overview

This ATIS standard describes a framework leveraging the SHAKEN model specified in [ATIS-1000074] to cryptographically sign and verify the SIP RPH field of NS/EP NGN-PS calls using the PASSPorT rph extension defined in [IETF RFC 8443].

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

1. **NS/EP NGN-PS Origination/Authentication**: The originating NS/EP NGN-PS Service Provider cryptographically signing the SIP RPH of authorized NS/EP NGN-PS calls before they are sent across an Internet Protocol Network-to-Network Interconnection (IPNNI) boundary. The SIP RPH signing is only performed by an authenticating NS/EP Service Provider (i.e., NS/EP NGN-PS performing authentication of the Service User).
2. **NS/EP NGN-PS Termination/Verification**: The receiving terminating NS/EP NGN-PS Service Provider to be able to verify the received signed PASSPorT token for the SIP RPHs.
3. **NS/EP NGN-PS Transit**: Transit NS/EP Service Providers may validate a signed SIP RPH (to determine treatment within its network), but MUST transparently pass the received Identity header associated with the SIP RPH.

## SIP RPH Signing Protocols Overview

This ATIS standard uses the PASSPorT “rph” extension specified in [IETF RFC 8443] and associated STIR protocols for cryptographic signing of the SIP RPH field in support of NS/EP NGN-PS.

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

### Persona 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 traced back to the known trust anchor who signed the certificate. The Persona Assertion Token (PASSporT) token 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 Identifier (SPID), 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.

Note: PASSporT tokens and signatures themselves are agnostic to network signaling protocols but are used in [draft-ietf-stir-rfc4474bis] to define specific SIP usage as described in the next section.

### Authenticated Identity Management in the Session Initiation Protocol

[IETF RFC 8224] defines a SIP-based framework for an authentication service and verification service for 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 adds the Identity header field and signature to the SIP INVITE generated by the originating provider. The INVITE is delivered to the destination provider which uses the verification service to verify the signature using the identity in the P-Asserted-Identity header field or From header field.

### PASSporT Extension for Resource-Priority Authorization

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

### PASSPorT Extension for Diverted Calls

The IETF is specifying the PASSporT "div" extension in [draft-ietf-stir-divert]. This extension can be utilized within the SHAKEN framework [ATIS-1000074] for TN Signing to provide end-to-end SHAKEN authentication for calls that are retargeted by features such as call-forwarding.

Handling of retargeted NS/EP NGN-PS calls (e.g., forwarded calls) as part of “div” procedures is for further study. This includes retargeted NS/EP NGN-PS calls when there only TN PASSporT according to [ATIS-1000074] and when there is both TN PASSPoT and RPH PASSPorT according to the present document.

## Call Validation Treatment and Display

### Call Validation Treatment

As specified in [ATIS-1000074], post STI-VS information MUST not be passed for Call Validation Treatment (CVT) for calls that contain a SIP Resource Priority Header (RPH) field with the “ETS” and “WPS” namespaces, to ensure the highest probability of call completion for these types of calls.

### Display of Signed SIP RPH NS/EP NGN-PS Calls

According to [ATIS-1000074], the terminating network conveys the verification results to the called user by including a “verstat “parameter in the From and/or P-Asserted-Identity header fields of the INVITE request sent to the called endpoint device. [3GPP TS 24.229], IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)), defines the “verstat” tel URI parameter used in the P-Asserted-Identity and the From header fields in a SIP request. It is used to convey the status of the calling number verification performed by the home network. Specifically, the "verstat" tel URI parameter is inserted by an AS or a proxy in the IM CN subsystem to provide the UE with the calling identity number verification status in an initial INVITE request.

Display of signed of NS/EP NGN-PS calls with signed RPH is outside the scope of this document.

## 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 there is only 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 CISA of the Department of Homeland Security is the authority for NS/EP NGN-PS and claims associated with the “ets” and “wps” namespaces in the SIP RPH. NS/EP Service Providers are delegated by the ECD/CISA/DHS as authority for signing SIP RPH with “ets” and “wps” namespaces.

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

NOTE: An NS/EP Service Provider can use the same certificates for signing SIP RPH as they use for TN signing, but is not required to do so.

## Reference Architecture for SIP RPH Signing

Figure 1 below shows the reference architecture for SIP RPH signing. It is an extension to the SHAKEN architecture defined in [ATIS-100074] for signing the SIP RPH of NS/EP NGN-PS calls across IPNNIs. In Figure 1, the NS/EP NGN-PS call is originated from service provider A’s network that performs the authentication service and the NS/EP NGN-PS call is terminated in service provider B’s network, which performs the verification service. The functional elements within black rectangular boxes are IMS and SHAKEN elements while the dotted red boxes are introduced functional elements necessary to realize the SIP RPH signing for NS/EP NGN-PS.



Figure 1 – Architecture for Signing 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 NGN-PS 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] for TN signing.
* Secure Telephone Identity Verification Service (STI-VS) – Defined in [ATIS-1000074] for TN signing.
* Call Validation Treatment (CVT) – Defined in [ATIS-1000074] for TN signing.
* Secure Key Store (SKS) – Defined in [ATIS-1000074] for TN signing.
* Certificate Provisioning Service – Defined in [ATIS-1000074] for TN signing.
* Secure Telephone Identity Certificate Repository (STI-CR) – Defined in [ATIS-1000074] for TN signing.

**NS/EP NGN-PS Elements**

* Telephone Application Server (TAS) – This element represents NS/EP processing and routing. It is viewed as the element responsible for WPS type functions including WPS call authentication.
* 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 type of functions including PIN authentication.
* RPH Authentication Service (RPH-AS) – This element represents the logical authentication service for SIP RPH signing defined in [IETF RFC 8443].

NOTE: The actual validation of the user device (i.e., for WPS) and user authentication (i.e., PIN) is part of the NS/EP NGN-PS process of the TAS and NS/EP NGN-PS AS respectively. The NS/EP authentication information is conveyed to the RPH-AS not shown in the reference model.

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

The focus of this present document is on the RPH-AS and RPH-VS functionality and the relevant SIP signaling and interfaces.

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



Figure 3 – NS/EP NGN-PS SIP RPH Signing Call Flow

1. The originating SIP UA sends a SIP INVITE for a NS/EP NGN-PS call
2. The CSCF of the originating Service Provider routes the call to the TAS or NS/EP NGN-PS AS for priority processing and handling (e.g., WPS or GETS authorization)
3. The TAS or NS/EP NGN-PS would append a Resource Priority Header to the SIP INVITE after authorizing the NS/EP NGN-PS call request
4. The CSCF of the originating Service Provider initiates an originating trigger to the STI-AS (RPH-AS function) for the SIP INVITE

NOTE: The STI-AS must be invoked after originating call processing.

1. The RPH-AS function of the STI-AS in the originating SP (i.e., Service Provider 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 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 INVITE and adds an Identity header field per [IETF RFC 8224].
3. The STI-AS passes the INVITE with the Identity header field back to the SP A’s CSCF.
4. The originating CSCF, through standard resolution, routes the call to the egress SBC-I (IBCF/TrGW).
5. The INVITE is routed over the NNI through the standard inter-domain routing configuration.
6. The terminating SP’s (Service Provider B) ingress SBC-I (IBCF/TrGW) receives the INVITE over the NNI.
7. The terminating CSCF initiates a terminating trigger to the STI-VS (RPH-AS) for the INVITE.

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

1. The terminating SP STI-VS determine 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).

NOTE: As per [ATIS-100074] SIP RPH calls are not forwarded to the optional CVT function that can be invoked to perform call spam analytics or other mitigation techniques.

1. Depending on the result of the STI verification, the STI-VS determines whether the call is to be completed with or without the RPH (that may be defined outside of this document based on NS/EP NGN-PS policy) and the INVITE is passed back to the terminating CSCF which continues to set up the call to the terminating SIP UA according to NS/EP NGN-PS procedures.

NOTE: Error cases where verification fails are discussed in Section 6.

1. The terminating SIP UA receives the INVITE and normal SIP processing of the call according to NS/EP NGN-PS procedures continues, returning “200 OK” or optionally setting up media end-to-end.

# 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 8224] defines PASSporT and [IETF RFC 8224] defines an authentication service, corresponding to STI-AS in the SHAKEN reference architecture, as well as a verification service or STI-VS. [IETF RFC 8443] defines the PASSPorT extension to sign and verify claims for the SIP RPH field. This section will detail the procedures required for the STI-AS (RPH-AS) to create the required identity header and the STI-VS (RPH-VS) to verify the claims of the identity header for the SIP RPH field.

## PASSporT Token Overview

STI as defined in [IETF RFC 8225] specifies the process of the PASSporT token.

PASSporT tokens have the following form:

* PASSPorT Header: The JWS token header is a JOSE Header [IETF RFC7515] that defines the type and encryption algorithm used in the token.
* PASSPorT Payload: The token claims consist of the information that needs to be verified at the destination party. These claims follow the definition of a JWT claim [IETF RFC7519] and are encoded as defined by the JWS Payload [IETF RFC7515].
* PASSPorT Signature: The signature of the PASSporT is created as specified by JWS [IETF RFC7515].

PASSPorT Header example:

An example of the header would be the following, including the specified passport type, ES256 algorithm, and a URI referencing the network location of the certificate needed to validate the PASSporT signature.

{

"typ":"passport",

"alg":"ES256",

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

}

PASSPorT Payload example:

The following is an example of a single originator with telephone number identity +12155551212, to a single destination with URI identity "sip:alice@example.com":

{

"dest":{"uri":["sip:alice@example.com"]},

"iat":1443208345,

"orig":{"tn":"12155551212"}

}

## Token Constuction and Procedures

### PASSporT & Identity Header Construction

The standard PASSporT base claims shall be used as defined in both [IETF RFC 8224] and [IETF RFC 8225].

[IETF RFC 8225] allows the Identity header to be inserted by a SIP proxy or UA and for multiple instances of the Identity header to occur. The Identity header shall be transited by SIP proxies and Back-to-Back User Agents (B2BUAs), unless otherwise prevented by local service provider policy. A SIP proxy or B2BUA may insert an additional Identity header in the event that the SIP node needs to make a new claim.

### PASSporT Extension “rph”

The standard PASSporT extension for “rph” shall be used as defined in [IETF RFC 8443].

[IETF RFC 8443] defines a JSON Web Token claim for "rph" which provides an assertion for the information in SIP 'Resource-Priority' header field.

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 a "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 look 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 "Resource-Priority" header field (i.e., Resource-Priority: namespace "." r-priority) based on [IETF RFC RFC4412]. The syntax is:

{

Resource-Priority = "Resource-Priority" : r-value,

r-value = namespace "." r-priority

}

Specifically, the "rph" claim includes an assertion of the priority level of the user to be used for a given communication session. The value of the "rph" claim is an object with one or more keys. Each key is associated with a JSON array. These arrays contain string that correspond to the r-values indicated in the SIP 'Resource-Priority' header field.

The following is an example "rph" claim for a SIP 'Resource-Priority' header 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. 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 authority MUST use its credentials associated with the specific service supported by the resource priority namespace in the claim. If r-values are added or dropped by the 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].

### Authentication

The authentication service shall be performed as define in section 4.1 of [IETF RFC 8443].

The Authentication Service will create the "rph" claim using the values discussed in Section 3 of [IETF RFC 8443] that are based on [IETF RFC 4412]. The construction of the "rph" claim follows the steps described in Section 4.1 of [IETF RFC 8224].

A SIP authentication service will derive the value of "rph" from the SIP 'Resource-Priority' header field based on policy associated with service-specific use of r-values, defined as follows in [IETF RFC 4412]:

r-value = namespace "." r-priority

The authentication service derives the value of the PASSPorT claim by verifying the authorization for the SIP 'Resource-Priority' header field (i.e., verifying a calling-user privilege for the SIP 'Resource-Priority' header field based on its identity). The authorization might be derived from customer-profile data or access to external services.

[IETF RFC 4412] allows multiple "namespace "." priority value" pairs, either in a single SIP 'Resource-Priority' header field or across multiple SIP 'Resource-Priority' header fields. An authority is responsible for signing all the content of a SIP 'Resource-Priority' header field for which it has the authority.

NS/EP NGN-PS Service Providers are responsible for signing SIP 'Resource-Priority' header field with the “ETS and “WPS” namespaces.

### Verification

The procedures for validating the PASSporT token, baseline claims, and SHAKEN extension claims are specified in section 5.3.1 of [ATIS-1000074].

[IETF RFC 8224], Section 6.2, Step 5 requires that specifications defining "ppt" values describe any additional verifier behavior. The behavior specified for the "ppt" values of "rph" is as follows:

The verification service MUST extract the value associated with the "auth" key in a full-form PASSPorT with a "ppt" value of "rph". If the signature validates, then the verification service can use the value of the "rph" claim as validation that the calling party is authorized for SIP 'Resource-Priority' header fields as indicated in the claim. This value would, in turn, be used for priority treatment in accordance with local policy for the associated communication service. If the signature validation fails, the verification service should infer that the calling party is not authorized for SIP 'Resource-Priority' header fields as indicated in the claim. In such cases, the priority treatment for the associated communication service is handled as per the local policy of the verifier. In such scenarios, the SIP 'Resource-Priority' header field SHOULD be stripped from the SIP request, and the network entities should treat the call as an ordinary call.

In addition, [IETF RFC 8224], Section 6.2, Step 4 requires the "iat" value in "rph" claim to be verified. The behavior of a SIP UA upon receiving an INVITE containing a PASSporT object with an "rph" claim will largely remain a matter of implementation policy for the specific communication service. In most cases, implementations would act based on confidence in the veracity of this information.

### 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].

## Solution Considerations

As specified in section 7.2 of [IETF RFC 8443] the use of extensions to PASSporT tokens with a "ppt" value of "rph" requires knowledge of the authentication, authorization, and reputation of the signer to attest to the identity being asserted, including validating the digital signature and the associated certificate chain to a trust anchor. The following considerations should be recognized when using PASSporT extensions with a "ppt" value of "rph":

* A signer is only allowed to sign the content of a SIP 'Resource-Priority' header field for which it has the proper authorization. Before signing tokens, the signer MUST have a secure method for authentication of the end user or the device being granted a token.
* The verification of the signature MUST include means of verifying that the signer is authoritative for the signed content of the resource priority namespace in the PASSporT.

The method for authenticating and authorizing the NS/EP NGN-PS Service User is outside the scope of this standard.

NS/EP NGN-PS Service Providers shall use the procedures define in other standards to authenticate and authorize NS/EP NGN-PS Service Users (e.g., WPS and GETS authorization) as the source for signing and attesting to the “rph” claim.

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

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