**ATIS IPNNI Task Force**

**August 2, 2017**

**Denver, CO**

**Contribution**

**TITLE: Baseline Text for Draft ATIS Standard on Signature-based Handling of SIP RPH Assertion using Tokens**

**SOURCE\*: Editor: Vencore Labs**

**ISSUE NUMBER:**

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

**Abstract**

This document provides the updated baseline text incorporating IPNNI-2017-00058R1 from the May 22, 2017 virtual meeting.

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

**ATIS-10000XX**

ATIS Standard on

**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

[1 Scope & Purpose 1](#_Toc474933780)

[1.1 Scope 1](#_Toc474933781)

[1.2 Purpose 1](#_Toc474933782)

[2 Normative References 2](#_Toc474933783)

[3 Definitions, Acronyms, & Abbreviations 2](#_Toc474933784)

[3.1 Definitions 2](#_Toc474933785)

[3.2 Acronyms & Abbreviations 2](#_Toc474933786)

[4 Overview 3](#_Toc474933787)

[4.1 SHAKEN Overview 4](#_Toc474933788)

[4.1.1 Persona Assertion Token (PASSporT) Token 4](#_Toc474933789)

[4.1.2 RFC 4474bis 4](#_Toc474933790)

[4.1.3 Governance Model and Certificate Management 4](#_Toc474933791)

[4.1.4 Draft-tbd-stir-rph 4](#_Toc474933792)

[4.2 SHAKEN Architecture 4](#_Toc474933793)

[4.3 SIP RPH Signing Call Flow 5](#_Toc474933794)

[5 Procedures for SIP RPH Signing 7](#_Toc474933795)

[5.1 PASSporT Token Overview 7](#_Toc474933796)

[5.2 [draft-ietf-rfc4474bis] Authentication procedures 7](#_Toc474933797)

[5.2.1 PASSporT & Identity Header Construction 7](#_Toc474933798)

[5.2.2 PASSporT Extension “rph” 7](#_Toc474933799)

[5.2.3 Attestation Indicator (“attest”) 8](#_Toc474933800)

[5.2.4 Origination Identifier (“origid”) 9](#_Toc474933801)

[5.3 4474bis Verification Procedures 9](#_Toc474933802)

[5.3.1 PASSporT Extension & Identity Header Verification 9](#_Toc474933803)

[5.3.2 Verification Error Conditions 9](#_Toc474933804)

[5.3.3 Use of the Full Form of PASSporT 9](#_Toc474933805)

[5.4 SIP Identity Header Example for “rph” Claim 9](#_Toc474933806)

# 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 in a multiple service provider IP-based network environment. NS/EP NGN-PS Service Providers receiving SIP RPHs across IP Network-to-Network Interconnections (IPNNIs) have no means of verifying that the RPH was populated by an authorized NS/EP NGN-PS Service Provider and that it was not spoofed.

This standard defines a mechanism for providing cryptographic authentication and verification of the SIP RPH field by using extension to the IETF PASSporT and the associated STIR mechanisms to sign the SIP RPH header field and convey assertions of authorization for Resource-Priority. It provides a procedure for providing cryptographic authentication and verification of the information in the SIP RPH field in an Internet Protocol (IP)-based service provider communication networks in support of National Security / Emergency Preparedness Next Generation Priority Services (NS/EP NGN-PS).

It defines the framework for telephone service providers to create signatures asserting the “ETS” and “WPS” namespace parameters in the SIP RPH field and validate initiators of the signatures by leveraging the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework specified in [ATIS-1000074] and the associated Secure Telephone Identity (STI) protocols specified by the IETF in [draft-ietf-stir-rfc4474bis] and [draft-ietf-stir-passport].

This document is intended to provide telephone service providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies for validation of legitimate information in the SIP RPH field and the mitigation of illegitimate spoofing of information in SIP RPH fields. It provides a mechanism for an originating service provider to sign the information the “ETS” and “WPS” namespace parameters in the SIP RPH field as specified in [IETF RFC 4412] before it is sent across an Internet Protocol Network-to-Network Interconnection (IPNNI) and the receiving service provider to be able to validate and act on the received information with confidence in support of NS/EP NGN-PS.

This standard does not specify any procedures using the “ETS” and “WPS” namespace parameters of the SIP RPH field. For example, the population and use of the “ETS” and “WPS” namespace parameters of the SIP RPH field to support NS/EP NGN-PS are not within the scope of this document. Such procedures are defined in other document specifying NS/EP NGN-PS. The scope of this ATIS standard is limited to the cryptographic authentication and verification of the “ETS” and “WPS” namespace parameters in the SIP RPH field.

The primary focus of this document is on the format of IETF STIR claims for the “ETS” and “WPS” namespace parameters of the SIP RPH field and the mapping of these claims to SIP [IETF RFC 3261], and the authentication and verification functions.

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 “ETS” and “WPS” namespace parameters in the SIP RPH used to support NS/EP NGN-PS is a concern for North American telephone service providers. The purpose of this standard is to provide telephone service providers with a mechanism to sign and validate claims for the “ETS” and “WPS” namespace parameters of the SIP RPH field to mitigate against spoofing or tampering of the information.

The objective of this specification is to make use and leverage the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework [ATIS-1000074] and the associated protocols defined in draft-ietf-stir-rfc4474bis and draft-ietf-stir-passport. The objective is also to make use of the associated certificate management infrastructure used to support STI.

The objective is to make use of service provider’s SHAKEN infrastructure (i.e., ATIS-1000074 and associated IETF STIR Working Group protocols) and defines extensions only where necessary.

Editor’s Note: This work involves identifying where extensions to IETF RFCs are needed in support of SIP RPH Signing.

Editor’s Note: Need to address security and denial of service implications.

Editor’s Note: Need to address practical considerations for deployment (e.g., taking into account trust model)

## General Assumptions

The following general assumptions are made in this standard:

1. The PASSPortT extension “rph’ defined in [draft-singh-stir-rph-00] 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. A NS/EP NGN-PS Service Provider authenticating a Service User would sign the information in the SIP RPH header using the PASSPorT “rph” extention and object “auth.” The PASSPorT “auth” object conveys authorization for Resource-Priority by the signing NGN-PS Service Provider.
2. 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.
3. 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.
4. Signing of telephone numbers (i.e., Calling Party Numbers) is independent of 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).
5. If a SIP identity header with signed assertion of 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.
6. Only SIP RPH in SIP Invites are signed. Although the SIP RPH are also populated and used in the backward direction (e.g., SIP response messages) for NS/EP NGN-PS signaling in the backward direction (e.g., response messages) is not within scope.
7. The PASSporT extension mechanism for SIP RPH signing is used by the NS/EP NGN-PS Service Provider as a security protection tool. Originating NS/EP NGN-PS Service Provider are responsible for signing all NS/EP NGN-PS SIP Invites. However, a receiving Service Provider may decide whether all signed tokens are valued or only selected token are validated based on their security policy and threat detection mechanisms.
8. SIP RPH Signing in support of NS/EP NGN-PS would Governance Model and Certificate Management

# 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).*

[Draft ATIS-0x0000x], *ATIS Standard on Signature-based Handling of Asserted Information Using Tokens (SHAKEN): Governance Model and Certificate Management*.

[draft-ietf-stir-passport], *Persona Assertion Token.*[[1]](#footnote-1)

[draft-ietf-stir-rfc4474bis], *Authenticated Identity Management in the Session Initiation Protocol.*1

[draft-ietf-stir-certificates], *Secure Telephone Identity Credentials: Certificates.*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

**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.

## 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 provides a mechanism for an originating service provider to sign the information the “ETS” and “WPS” namespace parameters in the SIP RPH field as specified in [IETF RFC 4412] before it is sent across an Internet Protocol Network-to-Network Interconnection (IPNNI) and the receiving service provider to be able to validate and act on the received information with confidence in support of NS/EP NGN-PS.

Note: This standard does not specify any procedures using the “ETS” and “WPS” namespace parameters of the SIP RPH field. The population and use of the “ETS” and “WPS” namespace parameters of the SIP RPH field to support NS/EP NGN-PS are not within the scope of this document. Such procedures are defined in other documents specifying NS/EP NGN-PS.

The primary focus of this standard is on the format of IETF STIR claims for the “ETS” and “WPS” namespace parameters of the SIP RPH field and the mapping of these claims to SIP [IETF RFC 3261], and the authentication and verification functions to mitigate against spoofing or tampering of the information.

## SHAKEN Overview

This ATIS standard uses the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework defined in [ATIS-1000074]. SHAKEN provides a framework for managing the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and using the IETF STIR Working Group protocols defined in draft-ietf-stir-rfc4474bis and draft-ietf-stir-passport for telephone service providers to create signatures in Session Initiation Protocol (SIP) and validate initiators of signatures.

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

### Persona Assertion Token (PASSporT) Token

[Draft-ietf-stir-passport] 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 [draft-ietf-stir-certificates]. 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.

### RFC 4474bis

[draft-ietf-stir-rfc4474bis] 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.

### Governance Model and Certificate Management

[Draft ATIS-Governance] provides a governance model and the X.509 certificate management procedures for SHAKEN based on [draft-ietf-stir-certificates]. The Governance model identifies functional entities that have the responsibility to establish policies and procedures to ensure that only authorized entities are allowed to administer certificates.

### Draft-tbd-stir-rph

Editor Note: This section will describe [draft-ietf-stir-rph] as appropriate.

## SHAKEN Architecture

Figure 4.1 shows the SHAKEN reference architecture described in Section 4.2 of [ATIS-1000074]. [ATIS-1000074] provides a logical view of the architecture and does not mandate any particular deployment and/or implementation. For reference, this architecture is specifically based on the 3GPP IMS architecture with an IMS application server, and is only provided as an example to set the context for the functionality described in this document. Figure 4.1 shows the two IMS instances that comprise the IMS half-call model; an originating IMS network hosted by Service Provider A, and a terminating IMS network hosted by Service Provider B.



Figure 4.1 – SHAKEN Reference Architecture

The SHAKEN reference architecture includes the following elements:

* SIP UA – The SIP User Agent that is authenticated by the service provider network. When the SIP UA is under direct management control of the telephone service provider, the service provider network can assert the calling party identity in originating SIP INVITE requests initiated by the SIP UA.
* IMS/Call Session Control Function (CSCF) – This component represents the SIP registrar and routing function. It also has a SIP application server interface.
* 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.
* Authentication Service (STI-AS) – The SIP application server that performs the function of the authentication service defined in draft-ietf-stir-rfc4474bis. It should either itself be highly secured and contain the Secure Key Store (SKS) of secret private key(s) or have an authenticated, Transport Layer Security (TLS)-encrypted interface to the SKS that stores the secret private key(s) used to create PASSporT signatures.
* Verification Service (STI-VS) – The SIP application server that performs the function of the verification service defined in draft-ietf-stir-rfc4474bis. It has an Hypertext Transfer Protocol Secure (HTTPS) interface to the Secure Telephone Identity Certificate Repository that is referenced in the Identity header field to retrieve the provider public key certificate.
* Call Validation Treatment (CVT) – This is a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified. The CVT can also provide information in its response that indicates how the results of the verification should be displayed to the called user.
* SKS – The Secure Key Store is a logical highly secure element that stores secret private key(s) for the authentication service (STI-AS) to access.
* Certificate Provisioning Service – A logical service used to provision certificate(s) used for STI.
* Secure Telephone Identity Certificate Repository (STI-CR) – This represents the publically accessible store for public key certificates. This should be an HTTPS web service that can be validated back to the owner of the public key certificate.

[ATIS-1000074] focuses on the STI-AS and STI-VS functionality and the relevant SIP signaling and interfaces.

Note: If there is any discrepancy between the information in this section and [ATIS-1000074], then ATIS-1000074 takes precedence.

## SIP RPH Signing Call Flow



Figure 4.2 – Reference Call Flow

Editor’s Note: update figure to make functional entities specific to RPH signing

Section 4.3 of [ATIS-1000074] describes a reference call flow of SHAKEN using Figure 4.2.

This standard extends the SHAKEN call flow example to illustrate how the SHAKEN infrastructure can be used to support signing of the “ETS” and “WPS” namespace parameters of the SIP RPH field as follows:

1. The originating SIP UA, which first REGISTERs and is authenticated to the CSCF, creates a SIP INVITE.
2. The CSCF of the originating provider adds an “ETS” or “WPS” namespace parameter to the “resource-priority” header (SIP RPH) field. The CSCF then initiates an originating trigger to the STI-AS for the INVITE.

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

1. The STI-AS in the originating SP (i.e., Service Provider A) first determines through service provider-specific means the legitimacy of the “ETS” or “WPS” namespace parameters 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 draft-ietf-stir-rfc4474bis using the STIR claim “rph” for the SIP RPH field.
3. The STI-AS passes the INVITE back to the SP A’s CSCF.
4. The originating CSCF, through standard resolution, routes the call to the egress IBCF.
5. The INVITE is routed over the NNI through the standard inter-domain routing configuration.
6. The terminating SP’s (Service Provider B) ingress IBCF receives the INVITE over the NNI.
7. The terminating SP’s (Service Provider B) CSCF initiates a terminating trigger to the STI-VS for the INVITE.

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

1. The terminating SP STI-VS uses the “info” parameter information in the Identity header field per [draft-ietf-stir-rfc4474bis] to determine the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR.
2. The STI-VS validates the certificate (see Section 5.3.1 for details) and then extracts the public key. It constructs the [draft-ietf-stir-rfc4474bis] format and uses the public key to verify the signature in the Identity header field, which validates the “ETS or “WPS” namespace parameter used when signing the INVITE on the originating service provider STI-AS.
3. The CVT is an optional function that can be invoked to perform analytics or other mitigation techniques.
4. Depending on the result of the STI validation, the STI-VS determines trust associated with the “ETS or “WPS” namespace and the INVITE is passed back to the terminating CSCF which continues to set up the call to the terminating SIP UA. The call is treated as a priority or normal call based on the STI validation in accordance with NS/EP NGN-PS specific requirements and service provider policy.

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 continues, returning “200 OK” or optionally setting up media end-to-end.

Editor’s Note: Need to determine whether the RPH claim will be a separate identity header. How local policy will determine cases when there are separate identity headers.

Editor’s Note: Need to address the physical location of the STI-VS and STI-AS.

# Procedures for SIP RPH Signing

[Draft-ietf-stir-4474bis] and [draft-ietf-stir-passport] define a base set of procedures for how STI fits into the SIP call flow. [Draft-ietf-stir-rfc4474bis] defines an authentication service, corresponding to STI-AS in the SHAKEN reference architecture, as well as a verification service or STI-VS. This section will detail the procedures required for the STI-AS to create the required identity header.

## PASSporT Token Overview

STI as defined in draft-ietf-stir-passport specifies the process of the PASSporT token.

PASSporT tokens have the following form:

* A protected header with the value BASE64URL(UTF(JWS Protected Header)).
* A payload with the value BASE64URL(JWS Payload).
* A signature with the value BASE64URL(JWS Signature).

An example of each is as follows:

*Protected Header*

{

"typ":"passport",

"alg":"ES256",

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

}

*Payload*

{

"iat":"1443208345",

"orig":{“tn”:"12155551212"},

"dest":{“tn”:"12155551213"}

}

[draft-ietf-stir-passport] has specific examples of a PASSporT token.

## [draft-ietf-rfc4474bis] Authentication procedures

### PASSporT & Identity Header Construction

The standard PASSporT base claims shall be used as defined in both [draft-ietf-stir-passport] and [draft-ietf-stir-rfc4474bis].

[draft-ietf-stir-rfc4474bis] 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 base PASSporT set of claims cover the assertion of the telephone number along with date and destination telephone numbers to avoid replay attacks using valid Identity header fields.

This section specifies a specific extension “rph” to PASSporT to sign the SIP RPH. The “rph” extension to PASSporT shall be implemented with all extension claims as part of the signed PASSporT token.

1. The ability to provide an assertion of the authorization for "Resource-Priority.
2. The ability to provide a unique originating identifier, as described in Section 5.2.4 of [ATIS-1000074].

The “rph” extension to PASSporT shall include both an attestation indicator (“attest”), as described in section 5.2.3 and an origination identifier (”origid”) as described in section 5.2.4. The “rph” PASSporT token would have the form given in the example below:

*Protected Header*

{

"typ":"passport",

"ppt":"rph",

"alg":"ES256",

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

}

*Payload*

{

"rph":{"auth":["Resource-Priority"]},

"iat":1443208345,

"origid":"123e4567-e89b-12d3-a456-426655440000"

}

Editor’s Note: need to define origid in the context of NS/EP

### Attestation Indicator (“attest”)

This indicator allows for both identifying the service provider that is vouching for the NS/EP NGN-PS call as well as clearly indicating what information the service provider is attesting to.

The following attestation is defined:

1. **“auth”: authorized Resource-Priority**

### Origination Identifier (“origid”)

The “origid” as defined in [ATIS-1000074] shall be used.

## 4474bis Verification Procedures

[draft-ietf-stir-rfc4474bis] defines the procedures for verification services including the methods used to verify the signature contained in the Identity header field.

### PASSporT Extension & Identity Header Verification

The certificate referenced in the “info” parameter of the Identity header field shall be validated by performing the following as specified in section 5.3.1 of [ATIS-1000074]:

* Check the certificate’s validity using the Basic Path Validation algorithm defined in the X.509 certificate standard (RFC 5280).
* Check that the certificate is not revoked using CRLs and/or OCSP.

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

The following applies to the “rph” PASSporT extension claim:

The “rph” claim shall be of type “auth”.

The “rph” claim “auth” value validation shall be performed as follows:

* The “resource-priority” header field shall be checked as the NS/EP NGN-PS identity to be validated if present.
* If there are more than one namespace values, the verification service shall check each of them until it finds one that is valid.

Editor’s Note: Will need to be updated based on whether there is more than one identity header.

### Verification Error Conditions

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

### Use of the Full Form of PASSporT

[draft-ietf-stir-rfc4474bis] 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 to avoid any potential SIP network element interaction with headers, in particular the Date header field, which could lead to large numbers of 438 (‘Invalid Identity Header’) errors being generated.

## SIP Identity Header Example for “rph” Claim

Editor Note: To be provided.

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

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