**ATIS IPNNI Task Force**

**November 6-7, 2019**

**Reston, VA**

**Contribution**

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

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

**ISSUE NUMBER:**

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

**Abstract**

This document provides the clean updated baseline text for Draft ATIS standard on SIP RPH Signing using PASSPorT Tokens.

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

**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

[**ATIS-10000XX** i](#_Toc23495336)

[ATIS Standard on i](#_Toc23495337)

[**Session Initiation Protocol Resource Priority Header (SIP RPH) Signing using PASSPorT Tokens** i](#_Toc23495338)

[**Alliance for Telecommunications Industry Solutions** i](#_Toc23495339)

[**Abstract** i](#_Toc23495340)

[Table of Contents iii](#_Toc23495341)

[Table of Figures iii](#_Toc23495342)

[1 Scope & Purpose 1](#_Toc23495343)

[1.1 Scope 1](#_Toc23495344)

[1.2 Purpose 1](#_Toc23495345)

[1.3 General Assumptions 2](#_Toc23495346)

[2 Normative References 2](#_Toc23495347)

[3 Definitions, Acronyms, & Abbreviations 3](#_Toc23495348)

[3.1 Definitions 3](#_Toc23495349)

[3.2 Acronyms & Abbreviations 3](#_Toc23495350)

[4 Overview 4](#_Toc23495351)

[4.1 SIP RPH Signing Overview 4](#_Toc23495352)

[4.1.1 Persona Assertion Token (PASSporT) Token 5](#_Toc23495353)

[4.1.2 RFC 4474bis 5](#_Toc23495354)

[4.1.3 Draft-tbd-stir-rph 5](#_Toc23495355)

[4.2 Governance Model and Certificate Management 5](#_Toc23495356)

[4.3 Reference Architecture for SIP RPH Signing 5](#_Toc23495357)

[4.4 SIP RPH Signing Call Flow 7](#_Toc23495358)

[5 Procedures for SIP RPH Signing 8](#_Toc23495359)

[5.1 PASSporT Token Overview 8](#_Toc23495360)

[5.2 [draft-ietf-rfc4474bis] Authentication procedures 9](#_Toc23495361)

[5.2.1 PASSporT & Identity Header Construction 9](#_Toc23495362)

[5.2.2 PASSporT Extension “rph” 9](#_Toc23495363)

[5.2.3 Origination Identifier (“origid”) 9](#_Toc23495364)

[5.3 4474bis Verification Procedures 9](#_Toc23495365)

[5.3.1 PASSporT Extension & Identity Header Verification 9](#_Toc23495366)

[5.3.2 Verification Error Conditions 10](#_Toc23495367)

[5.3.3 Use of the Full Form of PASSporT 10](#_Toc23495368)

[5.4 SIP Identity Header Example for “rph” Claim 10](#_Toc23495369)

# 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 NS/EP NGN-PS 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 IETF PASSPorT extension specified in [draft-ietf-stir-rph-00] and the associated Secure Telephone Identity (STI) protocols specified in [draft-ietf-stir-rfc4474bis] and [draft-ietf-stir-passport].

This document is intended to provide NS/EP NGN-PS Service Providers with a framework and guidance on how to utilize [draft-ietf-stir-rph-00] and the associated 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 the SIP RPH field using the PASSPorT extension specified in [draft-ietf-stir-rph-00] 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 signing of the SIP RPH field and conveying assertions of the content of the SIP RPH field (i.e., ETS and WPS namespaces).

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. The purpose of this standard is to provide NS/EP NGN-PS Service Providers with a mechanism to cryptographically sign the SIP RPH field to mitigate against spoofing or tampering of the information. The objective is to provide a framework on how the PASSPorT rph extension defined in [draft-ietf-stir-rph-00] can be used as a mitigation tool for protection of NS/EP NGN-PS against security and denial of service threats.

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.

# 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-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-rph], 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

**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 cryptographically sign the the SIP RPH field 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.

## SIP RPH Signing Overview

This ATIS standard uses the PASSPorT “rph” extension specified in [draft-ietf-stir-rph-00] 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) 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.

### Draft-tbd-stir-rph

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

[draft-ietf-stir-rph] 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.

## Governance Model and Certificate Management

[draft-ietf-stir-rph-00] indicates that the credentials (e.g., authority responsible for authorizating 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 Office of Emergency Communications OEC (formerly the NCS) 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 OEC 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.

## Reference Architecture for SIP RPH Signing

Editor’s Note: This section will provide a reference model for RPH Signing

The figure 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 8, 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 – 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 document is on the RPH-AS and RPH-VS functionality and the relevant SIP signaling and interfaces.

## 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”

[draft-ietf-stir-rph] defines a new JSON Web Token claim for "rph" which provides an assertion for information in SIP 'Resource-Priority' header.

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 [RFC4412]. Specifically, the "rph" claim includes assertion of the priority-level of the user to be used for a given communication session. The value of the "rph" claim is an array containing one or more of JSON objects for the content of the SIP 'Resource-Priority' header that is being asserted of which one of the "rph" object, is mandatory.

The following is an example "rph" claim for a SIP "Resource-Priority" header field with a "namespace "." r-priority" value of "ets.0".

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

"dest":{"tn":"12125551213"},

"iat":1443208345,

"rph":{"auth":"ets.0"}}

After the header and claims PASSporT objects have been constructed, their signature is generated normally per the guidance in [I-D.ietf-stir-passport] using the full form of PASSPorT.

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

### Origination Identifier (“origid”)

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

Editor’s Note: provide guidance on how “origid” is used for RPH signing and add “origid” to example

## 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)