

STIR  
Internet-Draft  
Intended status: Standards Track  
Expires: August 5, 2018

R. Singh  
Vencore Labs  
M. Dolly  
AT&T  
S. Das  
Vencore Labs  
A. Nguyen

Office of Emergency Communication/DHS  
February 01, 2018

PASSporT Extension for Resource-Priority Authorization  
draft-ietf-stir-rph-03

Abstract

This document extends the Secure Telephone Identity Revisited (STIR) Personal Assertion Token (PASSporT) specification defined in [I-D.ietf-stir-passport] to allow the inclusion of cryptographically signed assertions of authorization for the values populated in the Session Initiation Protocol (SIP) 'Resource-Priority' header field, which is used for communications resource prioritization.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 5, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Terminology . . . . .	3
3. PASSporT 'rph' Claim . . . . .	3
4. 'rph' in SIP . . . . .	5
4.1. Authentication Service Behavior . . . . .	5
4.2. Verification Service Behavior . . . . .	5
5. Further Information Associated with 'Resource-Priority' . . . . .	6
6. IANA Considerations . . . . .	6
6.1. PASSporT Extension Claims Registration . . . . .	6
6.2. 'rph' Types . . . . .	7
7. Security Considerations . . . . .	7
7.1. Avoidance of replay and cut and paste attacks . . . . .	7
7.2. Solution Considerations . . . . .	7
7.3. Acknowledgements . . . . .	8
8. References . . . . .	8
8.1. Normative References . . . . .	8
8.2. Informative References . . . . .	9
Authors' Addresses . . . . .	9

## 1. Introduction

PASSporT [I-D.ietf-stir-passport] is a token format based on JSON Web Token (JWT) [RFC7519] for conveying cryptographically signed information about the identities involved in personal communications; it is used with STIR [I-D.ietf-stir-rfc4474bis] to convey a signed assertion of the identity of the participants in real-time communications established via a protocol like SIP [RFC3261]. This specification extends PASSporT to allow cryptographic-signing of the SIP 'Resource-Priority' header field defined in [RFC4412].

[RFC4412] defines the SIP 'Resource-Priority' header field for communications Resource Priority. As specified in [RFC4412], the 'Resource-Priority' header field may be used by SIP user agents [RFC3261], including Public Switched Telephone Network (PSTN) gateways and terminals, and by SIP proxy servers, to influence prioritization afforded to communication sessions, including PSTN calls. However, the SIP 'Resource-Priority' header field could be spoofed and abused by unauthorized entities.

The STIR architecture [RFC7340] assumes that an authority on the originating side of a call provides a cryptographic assurance of the validity of the calling party number in order to prevent impersonation attacks. The STIR architecture allows extensions that can be utilized by authorities supporting real-time communication services using the 'Resource-Priority' header field to cryptographically sign the SIP 'Resource-Priority' header field and convey assertion of the authorization for 'Resource-Priority'. For example, the authority on the originating side verifying the authorization of a particular communication for 'Resource-Priority' can use a PASSporT claim to cryptographically sign the SIP 'Resource-Priority' header field and convey an assertion of the authorization for 'Resource-Priority'. This will allow a receiving entity (including entities located in different network domains/boundaries) to verify the validity of assertions authorizing 'Resource-Priority'. Cryptographically signed SIP 'Resource-Priority' header fields will allow a receiving entity to verify and act on the information with confidence that the information has not been spoofed or compromised.

This specification documents an optional extension to PASSporT and the associated STIR mechanisms to provide a function to sign the SIP 'Resource-Priority' header field. This PASSporT object is used to provide attestation of a calling user authorization for priority communications. This is necessary in addition to the PASSporT object that is used for calling user telephone number attestation. How the optional extension to PASSporT is used for real-time communications supported using SIP 'Resource-Priority' header field is outside the scope of this document.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119] and in RFC 8174 [RFC8174].

## 3. PASSporT 'rph' Claim

This specification defines a new JSON Web Token claim for "rph", which provides an assertion for 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 = "Resource-Priority": r-value, where r-value= "namespace "." priority value") 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 Object with one or more keys. Each key is associated with a JSON Array. These arrays contain Strings 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 a r-value = "namespace "." priority value" of "ets.0" and with another r-value= "namespace "." priority 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 [I-D.ietf-stir-passport] using the full form of PASSPorT. The credentials (e.g., authority responsible for authorizing Resource-Priority) 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 (i.e., CERT) associated with the specific service supported by the SIP namespace in the claim. If r-values are added or dropped by the intermediaries along the path, intermediaries must generate a new "rph" header and sign the claim with its own authority.

The use of the compact form of PASSporT is not specified in this document.

#### 4. 'rph' in SIP

This section specifies SIP-specific usage for the "rph" claim in PASSporT.

##### 4.1. Authentication Service Behavior

The Authentication Service will create the "rph" claim using the values discussed in section 3 based on [RFC4412]. The construction of "rph" claim follows the steps described in Section 4 of [I-D.ietf-stir-rfc4474bis].

The resulting Identity header for "rph" might look as follows(backslashes shown for line folding only):

```
Identity:eyJhbGciOiJFUzI1NiIsInBwdCI6InJwaCI6InR5cCI6InBhc3Nwb3J0\  
IiwieDVlIjoiaHR0cHM6Ly93d3cuZXhhbXBsZS5jb20vY2VydC5jZSIifQo.eyJkZ\  
XN0Ijp7WyJ0biI6IjEyMTU1NTUwMTEzIl19LCJpYXQiOiIxNDQzMjA4MzQ1Iiwib3\  
JpZyI6eyJ0biI6IjEyMTU1NTUwMTEyIn0sInJwaCI6eyJhdXRoIjpbImV0cy4wIiw\  
id3BzLjAiXX19Cg.s37S6VC8HM6Dl6YzJeQDsrZcwJ0lizxhUrA7f_98oWBHvo-cl\  
-n8MIhoCr18vYYFy3blXvs3fslM_oos2P2Dyw;info=<https://www.example.\  
org/cert.cer>;alg=ES256;ppt=rph
```

A SIP authentication service typically will derive the value of "rph" from the 'Resource-Priority' header field based on policy associated with service specific use of the "namespace "." priority value" for r-values based on [RFC4412]. The authentication service derives the value of the PASSporT claim by verifying the authorization for 'Resource-Priority' (i.e., verifying a calling user privilege for 'Resource-Priority' based on its identity) which might be derived from customer profile data or from access to external services.

[RFC4412] allows multiple "namespace "." priority value" pairs, either in a single SIP 'Resource-Priority' header field or across multiple SIP 'Resource-Priority' headers. An authority is responsible for signing all the content of a SIP 'Resource-Priority' header field for which it has the authority.

##### 4.2. Verification Service Behavior

[I-D.ietf-stir-rfc4474bis] 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 'Resource-Priority' 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 'Resource-Priority' as indicated in the claim. In such cases, the priority treatment for the associated communication service is handled as per the local policy.

In addition, [I-D.ietf-stir-rfc4474bis] Section 6.2 Step 4 requires "iat" value in "rph" claim to be verified.

The behavior of a SIP UA upon receiving an INVITE containing a PASSporT object with a "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.

## 5. Further Information Associated with 'Resource-Priority'

There may be additional information about the calling party or the call that could be relevant to authorization for 'Resource-Priority'. This may include information related to the device subscription of the caller, or to any institutions that the caller or device is associated with, or even categories of institutions. All of these data elements would benefit from the secure attestations provided by the STIR and PASSporT frameworks. The specification of the "rph" claim could entail the optional presence of one or more such additional information fields.

A new IANA registry has been defined to hold potential values of the "rph" array; see Section 6.2. The definition of the "rph" claim may have one or more such additional information field(s). Details of such "rph" claim to encompass other data elements are left for future version of this specification.

## 6. IANA Considerations

### 6.1. PASSporT Extension Claims Registration

This document registers a new "ppt" value for the "Personal Assertion Token (PASSporT) Extensions" table.

- o Claim Name: "rph"
- o Claim Description: Resource Priority Header Authorization

- o Change Controller: IESG
- o Specification Document(s): Section 3 of [RFCThis]

## 6.2. 'rph' Types

This specification also requests that the IANA creates a new registry for "rph" types. Each registry entry must contain two fields: the name of the "rph" type and the specification in which the type is described. This registry is to be initially populated with a single value for "auth" which is specified in [RFCThis]. Registration of new "rph" types shall be under the specification required policy.

## 7. Security Considerations

The security considerations discussed in [I-D.ietf-stir-rfc4474bis] in Section 10 are applicable here.

### 7.1. Avoidance of replay and cut and paste attacks

The PASSporT extension with a "ppt" value of "rph" MUST only be sent with SIP INVITE when 'Resource-Priority' header field is used to convey the priority of the communication as defined in [RFC4412]. To avoid the replay, and cut and paste attacks, the procedures described in Section 10.1 of [I-D.ietf-stir-rfc4474bis] MUST be followed.

### 7.2. Solution Considerations

The use of extension to PASSporT tokens with "ppt" value "rph" based on the validation of the digital signature and the associated certificate requires consideration of the authentication and authority or reputation of the signer to attest to the identity being asserted. The following considerations should be recognized when using PASSporT extension with "ppt" value of "rph":

- o An authority (signer) is only allowed to sign the content of a SIP 'Resource-Priority' header field for which it has the right authority. The authority that signs the token MUST have a secure method for authentication of the end user or the device.
- o 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.

### 7.3. Acknowledgements

We would like to thank STIR members, ATIS/SIP Forum Task Force on IPNNI members, and the NS/EP Priority Services community for contributions to this problem statement and specification. We would also like to thank David Hancock and Ning Zhang for their valuable inputs.

## 8. References

### 8.1. Normative References

[I-D.ietf-stir-passport]

Wendt, C. and J. Peterson, "Personal Assertion Token (PASSporT)", February 2017.

[I-D.ietf-stir-rfc4474bis]

Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", February 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <<http://www.rfc-editor.org/info/rfc3261>>.

[RFC4412] Schulzrinne, H. and J. Polk, "Communications Resource Priority for the Session Initiation Protocol (SIP)", RFC 4412, DOI 10.17487/RFC4412, February 2006, <<http://www.rfc-editor.org/info/rfc4412>>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <<http://www.rfc-editor.org/info/rfc7519>>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<http://www.rfc-editor.org/info/rfc8174>>.



## 8.2. Informative References

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <<http://www.rfc-editor.org/info/rfc7340>>.

## Authors' Addresses

Ray P. Singh  
Vencore Labs  
150 Mount Airy Road  
New Jersey, NJ 07920  
USA

Email: [rsingh@vencorelabs.com](mailto:rsingh@vencorelabs.com)

Martin Dolly  
AT&T  
200 Laurel Avenue  
Middletown, NJ 07748  
USA

Email: [md3135@att.com](mailto:md3135@att.com)

Subir Das  
Vencore Labs  
150 Mount Airy Road  
New Jersey, NJ 07920  
USA

Email: [sdas@vencorelabs.com](mailto:sdas@vencorelabs.com)

An Nguyen  
Office of Emergency Communication/DHS  
245 Murray Lane, Building 410  
Washington, DC 20528  
USA

Email: [an.p.nguyen@HQ.DHS.GOV](mailto:an.p.nguyen@HQ.DHS.GOV)