

STIR
Internet-Draft
Intended status: Standards Track
Expires: January 14, 2021

M. Dolly
AT&T
C. Wendt
Comcast
July 13, 2020

Assertion Values for a Resource Priority Header Claim and a SIP Priority
Header Claim in Support of Emergency Services Networks
[draft-ietf-stir-rph-emergency-services-02](#)

Abstract

This document adds new assertion values for a Resource Priority Header ("rph") claim and a new SIP Priority Header claim ("sph") for protection of the "psap-callback" value as part of the "rph" PASSport extension, in support of the security of Emergency Services Networks for emergency call origination and callback.

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 January 14, 2021.

Copyright Notice

Copyright (c) 2020 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.	New Assertion Values for "rph" claim	3
3.1.	ESorig	3
3.2.	EScallback	4
4.	The SIP Priority header "sph" claim	4
5.	Order of Claim Keys	5
6.	Compact Form of PASSporT	5
7.	IANA Considerations	5
7.1.	PASSporT Resource Priority Header (rph) Types	5
7.2.	JSON Web Token claims	6
8.	Security Considerations	6
9.	References	6
9.1.	Normative References	6
9.2.	Informative References	7
	Authors' Addresses	8

[1.](#) Introduction

Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization [[RFC8443](#)] extended the Personal Assertion Token (PASSporT) specification defined in [[RFC8225](#)] to allow the inclusion of cryptographically signed assertions of authorization for the values populated in the Session Initiation Protocol (SIP) "Resource-Priority" header field [[RFC4412](#)], which is used for communications resource prioritization and the SIP "Priority" header field, used for categorizing the priority use of the call.

Compromise of the SIP "Resource-Priority" header field could lead to misuse of network resources (i.e., during congestion scenarios), impacting the application services supported using the SIP "Resource-Priority" header field.

[[RFC8225](#)] allows extensions by which an authority on the originating side verifying the authorization of a particular communication for the SIP "Resource-Priority" header field or the SIP "Priority" header field can use PASSporT claims to cryptographically sign the information associated with either the SIP "Resource-Priority" or

"Priority" header fields and convey assertion of those values by the signing party authorization. A signed SIP "Resource-Priority" or "Priority" header fields will allow a receiving entity (including entities located in different network domains/boundaries) to verify

the validity of assertions to act on the information with confidence that the information has not been spoofed or compromised.

This document adds new assertion values for a Resource Priority Header ("rph") claim defined in [\[RFC8443\]](#), in support of Emergency Services Networks for emergency call origination and callback. This document also defines a new claim, "sph", including protection of the SIP Priority header for the indication of an emergency service callback assigned the value "psap-callback" as defined in [\[RFC7090\]](#). The use of these new assertion values for real-time communications supported using the SIP 'Resource-Priority' and 'Priority' header fields for emergency services is introduced in [\[I-D.rosen-stir-emergency-calls\]](#) but otherwise out-of-scope of this document. In addition, the PASSPorT claims and values defined in this document are intended for use in environments where there are means to verify that the signer of the SIP 'Resource-Priority' and 'Priority' header fields is authoritative.

[2.](#) Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [\[RFC2119\]](#) [\[RFC8174\]](#) when, and only when, they appear in all capitals, as shown here.

[3.](#) New Assertion Values for "rph" claim

This specification defines new assertions values for:

- * "ESorig": Emergency Services call origination
- * "EScallback": Emergency Services callback.

[3.1.](#) ESorig

When using "ESorig" as the "rph" assertion value, the "orig" claim of

the PASSporT MUST represent the calling party number that initiates the call to emergency services. The "dest" claim MUST either be a country or region specific dial string (e.g., "911" for North America or "112" GSM defined string used in Europe and other countries) or "urn:service:sos" as defined in TBD, representing the emergency services destination of the call.

The following is an example of an "rph" claim for SIP 'Resource-Priority' header field with a "ESorig" assertion:

```
{
  "orig":{"tn":"12155551212"},
  "dest":{"uri":"urn:service:sos"}},
  "iat":1443208345,
  "rph":{"ESorig":["esnet,x"]}
}
```

[3.2.](#) EScallback

When using "EScallback" as the "rph" assertion value, the "orig" claim of the PASSporT MUST represent the emergency network telephone number. The "dest" claim MUST be the telephone number representing the original calling party of the emergency service call that is being called back.

The following is an example of an "rph" claim for SIP 'Resource-Priority' header field with a "EScallback" assertion:

```
{
  "orig":{"tn":"12155551213"},
  "dest":{"tn":"12155551212"}},
  "iat":1443208345,
  "rph":{"EScallback":["esnet,x"]}
}
```

After the header and claims PASSporT objects have been constructed, their signature is generated normally per the guidance in [RFC8225](#) 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.

4. The SIP Priority header "sph" claim

As discussed in [[I-D.rosen-stir-emergency-calls](#)], and as defined in [[RFC7090](#)] the SIP Priority header may be set to the value "psap-callback" for emergency services callback calls. Because some SIP networks may act on this value and provide priority or other special routing based on this value, it is important to protect and validate the authoritative use associated with it.

Therefore, we define a new claim key as part of the "rph" PASSport, "sph", which MUST be used only for authorized emergency callbacks and correspond to a SIP Priority header with the value "psap-callback".

The value of the "sph" claim key should only be "psap-callback" to match the SIP Priority header field value for authorized emergency services callbacks.

The following is an example of an "sph" claim for SIP 'Priority' header field with the value "psap-callback":

```
{
  "orig":{"tn":"12155551213"},
  "dest":{"tn":"12155551212"}},
  "iat":1443208345,
  "rph":{"EScallback":["esnet,x"]},
  "sph":"psap-callback"
}
```

5. Order of Claim Keys

The order of the claim keys MUST follow the rules of [[RFC8225](#) [Section 9](#)]; the claim keys MUST appear in lexicographic order.

Therefore, the claim keys discussed in this document appear in the PASSport Payload in the following order,

- o dest
- o iat
- o orig
- o rph
- o sph

6. Compact Form of PASSporT

The use of the compact form of PASSporT is not specified in this document or recommended for 'rph' PASSporTs.

7. IANA Considerations

7.1. PASSporT Resource Priority Header (rph) Types

This specification requests that the IANA add two new assertion values to the "PASSporT Resource Priority Header (rph) Types" Registry as defined in [[RFC8443](#)].

The following assertion values will be added to the registry:

- * "ESorig": Emergency Services call origination
- * "EScallback": Emergency Services callback

+-----+-----+
rph Type Reference
+-----+-----+
ESorig [this RFC]
+-----+-----+
EScallback [this RFC]
+-----+-----+

7.2. JSON Web Token claims

This specification requests that the IANA add two new claims to the JSON Web Token Claims registry as defined in [[RFC7519](#)].

Claim Name: "sph"

Claim Description: SIP Priority header field

Change Controller: IESG

Specification Document(s): [RFCThis]

8. Security Considerations

The security considerations discussed in [\[RFC8224\], Section 12](#), are applicable here.

9. References

9.1. Normative References

- [I-D.rosen-stir-emergency-calls]
Rosen, B., "Non-Interactive Emergency Calls", [draft-rosen-stir-emergency-calls-00](#) (work in progress), March 2020.
- [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, <<https://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, <<https://www.rfc-editor.org/info/rfc4412>>.

- [RFC7090] Schulzrinne, H., Tschofenig, H., Holmberg, C., and M. Patel, "Public Safety Answering Point (PSAP) Callback", [RFC 7090](#), DOI 10.17487/RFC7090, April 2014, <<https://www.rfc-editor.org/info/rfc7090>>.
- [RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", [RFC 7519](#), DOI 10.17487/RFC7519, May 2015, <<https://www.rfc-editor.org/info/rfc7519>>.

- [RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", [RFC 8224](#), DOI 10.17487/RFC8224, February 2018, <<https://www.rfc-editor.org/info/rfc8224>>.
- [RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", [RFC 8225](#), DOI 10.17487/RFC8225, February 2018, <<https://www.rfc-editor.org/info/rfc8225>>.
- [RFC8226] Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", [RFC 8226](#), DOI 10.17487/RFC8226, February 2018, <<https://www.rfc-editor.org/info/rfc8226>>.
- [RFC8443] Singh, R., Dolly, M., Das, S., and A. Nguyen, "Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization", [RFC 8443](#), DOI 10.17487/RFC8443, August 2018, <<https://www.rfc-editor.org/info/rfc8443>>.

9.2. Informative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC7340] Peterson, J., Schulzrinne, H., and H. Tschafenig, "Secure Telephone Identity Problem Statement and Requirements", [RFC 7340](#), DOI 10.17487/RFC7340, September 2014, <<https://www.rfc-editor.org/info/rfc7340>>.
- [RFC7375] Peterson, J., "Secure Telephone Identity Threat Model", [RFC 7375](#), DOI 10.17487/RFC7375, October 2014, <<https://www.rfc-editor.org/info/rfc7375>>.

- [RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for

Writing an IANA Considerations Section in RFCs", [BCP 26](#),
[RFC 8126](#), DOI 10.17487/RFC8126, June 2017,
<<https://www.rfc-editor.org/info/rfc8126>>.

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

Authors' Addresses

Martin Dolly
AT&T

Email: md3135@att.com

Chris Wendt
Comcast
Comcast Technology Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net