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-06

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 August 14, 2021.

Table of Contents

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]. [I-D.rosen-stir-emergency-calls]
   introduces the need and justification for the protection of both the
   SIP "Resource-Priority" and "Priority" header fields, used for
   categorizing the priority use of the call in the telephone network,
   specifically for emergency calls.

   Compromise of the SIP "Resource-Priority" or "Priority" header fields
   could lead to misuse of network resources (i.e., during congestion
   scenarios), impacting the application services supported using the
   SIP "Resource-Priority" header field and the handling of Public
   Saftey Answering Point (PSAP) callbacks.

   [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 field and convey assertion of those values by the
   signing party authorization. A signed SIP "Resource-Priority" or
   "Priority" header field 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 "auth" array key 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 additionally defines a new PASSPorT claim,
"sph", including protection of the SIP Priority header field for the
indication of an emergency service call-back assigned the value
"psap-callback" as defined in [RFC7090]. The use of the newly
defined claim and key values corresponding to 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 the ability to sign the SIP Resource-
Priority Header field namespace for local emergency communications
defined in [RFC7135] and represented by the string "esnet.x" where x
is the priority-level allowed in the esnet namespace. As of the
writing of this specification the priority-level is between 0 and 4,
inclusive, but may be extended by future specifications.

Similar to the values allowed by [RFC8443] for the "auth" JSON object
key inside the "rph" claim, the string "esnet.x" with the appropriate
value should be used when resource priority is required for local
emergency communications corresponding and exactly matching the SIP
Resource-Priority header field representing the namespace invoked in
the call.

When using "esnet.x" as the "auth" assertion value in emergency
service destined calls, 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 [RFC5031], representing the emergency
   services destination of the call.

   The following is an example of an "rph" claim for SIP 'Resource-
   Priority' header field with an "esnet.1" assertion:

```
  {
    "orig":{"tn":"12155551212"},
    "dest":{"uri":["urn:service:sos"]},
    "iat":1443208345,
    "rph":{"auth":["esnet.1"]}
  }
```

   For emergency services callbacks, the "orig" claim of the "rph"
   PASSporT MUST represent the Public Saftey Answering Point (PSAP)
   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 "esnet.0" assertion:

```
  {
    "orig":{"tn":"12155551213"},
    "dest":{"tn":["12155551212"]},
    "iat":1443208345,
    "rph":{"auth":["esnet.0"]}
  }
```

   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" identity header
   and sign the claim with their own authority.

4. The SIP Priority header "sph" claim

   As defined in [RFC7090] the SIP Priority header field 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". This is an optional claim that MUST only be used only with an "auth" claim with an "esnet.x" value indicating an authorized emergency callback call and corresponding to a SIP Priority header field with the value "psap-callback".

The value of the "sph" claim key should only be "psap-callback" which MUST match the SIP Priority header field value for authorized emergency services callbacks. If the value is anything other than "psap-callback", the PASSporT validation MUST be considered a failure case.

Note: Because the intended use of this specification is only for emergency services, there is also an explicit assumption that the signer of the "rph" PASSporT can authoritatively represent both the content of the Resource Priority Header field and Priority Header field information associated specifically with a emergency services callback case where both could exist. This document is not intended to be a general mechanism for protecting SIP Priority Header fields, this could be accomplished as part of future work with a new PASSporT extension or new claim added to either an existing PASSporT or PASSporT extension usage.

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":{"auth":["esnet.0"]},
  "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. Acknowledgements

The authors would like to thank Brian Rosen, Terry Reese, and Jon
Peterson for helpful suggestions, comments, and corrections.

8. IANA Considerations

8.1. JSON Web Token claims

This specification requests that the IANA add one new claim 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]

9. Security Considerations

The security considerations discussed in [RFC8224], Section 12, are
applicable here.

10. References

10.1. Normative References

[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>.

[RFC5031] Schulzrinne, H., "A Uniform Resource Name (URN) for
           Emergency and Other Well-Known Services", RFC 5031,
           DOI 10.17487/RFC5031, January 2008,
           <https://www.rfc-editor.org/info/rfc5031>.

   [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>.

   [RFC7135] Polk, J., "Registering a SIP Resource Priority Header
              Field Namespace for Local Emergency Communications",
              RFC 7135, DOI 10.17487/RFC7135, May 2014,
              <https://www.rfc-editor.org/info/rfc7135>.

   [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>.

   [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>.

10.2. Informative References

   [I-D.rosen-stir-emergency-calls]
              Rosen, B., "Non-Interactive Emergency Calls", draft-rosen-
              stir-emergency-calls-00 (work in progress), March 2020.

   [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>.

   [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