        Assertion Values for a Resource Priority Header Claim in Support of
                        Emergency Services Networks
                  draft-dolly-stir-rph-emergency-services-00

Abstract

   This document adds new assertion values for a Resource Priority
   Header ("rph") claim defined in RFC 8443, in support of Emergency
   Services Networks for emergency call origination and callback.

Status of This Memo

Copyright Notice

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, which is used for communications resource
   prioritization.

   Compromise of the SIP 'Resource-Priority' header field [RFC4412]
   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 can use a PASSporT claim to
   cryptographically sign the SIP 'Resource-Priority' header field and
   convey assertion of the authorization for the SIP 'Resource-Priority'
   header field. A signed SIP 'Resource-Priority' header field will
   allow a receiving entity (including entities located in different
   network domains/boundaries) to verify the validity of assertions
   authorizing the SIP 'Resource-Priority' header field and 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. How
   these new assertion values for real-time communications supported
   using the SIP 'Resource-Priority' header field is outside the scope
   of this document. In addition, the PASSPorT extension defined in
   this document is intended for use in environments where there are

   means to verify that the signer of the SIP 'Resource-Priority' header
   field 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

   This specification defines new assertions values for:

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

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

```
     {
       "orig":{"tn":"CgPN"},
       "dest":{["tn":"911 or URN-SOS"]},
       "iat":1443208345,
       "rph":{"ESorig":["esnet,x"]}
     }
```

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

```
     {
       "orig":{"tn":"EmergNet Num"},
       "dest":{["tn":"CgPN that originated emergency call"]},
       "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.

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

4. IANA Considerations

4.1. 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] |
+--------------+------------+
```

5. Security Considerations

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

6. References

6.1. Normative References

   [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>.

   [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>.

6.2. 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. Tschofenig, "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: mmd3135@att.com

   Chris Wendt
   Comcast
   Comcast Technology Center
   Philadelphia, PA 19103
   USA

   Email: chris-ietf@chriswendt.net