        Diameter Attribute-Value Pairs for Cryptographic Key Transport

Abstract

   Some Authentication, Authorization, and Accounting (AAA) applications
   require the transport of cryptographic keying material. This
   document specifies a set of Attribute-Value Pairs (AVPs) providing
   native Diameter support of cryptographic key delivery.

Table of Contents

1. Introduction

   The Diameter Extensible Authentication Protocol (EAP) application
   [RFC4072] defines the EAP-Master-Session-Key and EAP-Key-Name AVPs
   for the purpose of transporting cryptographic keying material derived
   during the execution of certain Extensible Authentication Protocol
   (EAP) [RFC3748] methods (for example, EAP-TLS [RFC5216]). At most
   one instance of either of these AVPs is allowed in any Diameter
   message.

   However, recent work (see, for example, [RFC5295]) has specified
   methods to derive other keys from the keying material created during
   EAP method execution that may require transport in addition to the
   Master Session Key (MSK). Also, the EAP Re-authentication Protocol
   (ERP) [RFC6696] specifies new keys that may need to be transported
   between Diameter nodes.

   This document specifies a set of AVPs allowing the transport of
   multiple cryptographic keys in a single Diameter message.

2. Terminology

2.1. Requirements Language

   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].

2.2. Technical Terms and Acronyms

   DSRK
      Domain-Specific Root Key [RFC5295].

   MSK
      Master Session Key [RFC3748].

   rMSK
      re-authentication MSK [RFC6696]. This is a per-authenticator key,
      derived from the rRK (below).

   rRK
      re-authentication Root Key, derived from the Extended Master
      Session Key (EMSK) [RFC3748] or DSRK [RFC6696].

3. Attribute-Value Pair Definitions

   This section defines new AVPs for the transport of cryptographic keys
   in the Diameter EAP application [RFC4072], as well as other Diameter
   applications.

3.1. Key AVP

   The Key AVP (AVP Code 581) is of type Grouped. It contains the type
   and keying material and, optionally, an indication of the usable
   lifetime of the key, the name of the key and a Security Parameter
   Index (SPI) with which the key is associated.

   Key ::= < AVP Header: 581 >
           < Key-Type >
           { Keying-Material }
           [Key-Lifetime]
           [Key-Name]
           [Key-SPI]
         * [AVP]

3.1.1. Key-Type AVP

   The Key-Type AVP (AVP Code 582) is of type Enumerated. This AVP
   identifies the type of the key being sent. The following decimal
   values are defined in this document:

   DSRK (0)
      A Domain-Specific Root Key [RFC5295].

   rRK (1)
      A re-authentication Root Key [RFC6696].

   rMSK (2)
      A re-authentication Master Session Key [RFC6696].

   If additional values are needed, they are to be assigned by IANA
   according to the policy stated in Section 5.2.

3.1.2. Key-Name AVP

   The Key-Name AVP (AVP Code 586) is of type OctetString. It contains
   an opaque key identifier. Exactly how this name is generated and
   used depends on the key type and usage in question and is beyond the
   scope of this document (see [RFC5247] and [RFC5295] for discussions
   of key name generation in the context of EAP).

3.1.3. Keying-Material AVP

   The Keying-Material AVP (AVP Code 583) is of type OctetString. The
   exact usage of this keying material depends upon several factors,
   including the type of the key and the link layer in use and is beyond
   the scope of this document.

3.1.4. Key-Lifetime AVP

   The Key-Lifetime AVP (AVP Code 584) is of type Unsigned32 and
   represents the period of time (in seconds) for which the contents of
   the Keying-Material AVP (Section 3.1.3) is valid.

   NOTE:
      Applications using this value SHOULD consider the beginning of the
      lifetime to be the point in time when the message containing the
      keying material is received. In addition, client implementations
      SHOULD check to ensure that the value is reasonable; for example,
      the lifetime of a key should not generally be longer than the
      session lifetime (see Section 8.13 of [RFC6733]).

3.1.5. Key-SPI

   The Key-SPI AVP (AVP Code 585) is of type Unsigned32 and contains an
   SPI value that can be used with other parameters for identifying
   associated keying material.

4. Security Considerations

   Transporting keys is a security-sensitive action. Some forms of
   keying material are already protected and can be sent safely over the
   open Internet. However, if a Key AVP contains a Keying-Material AVP
   that is not already protected, then the Diameter messages containing
   that Key AVP MUST only be sent protected via mutually authenticated
   TLS or IPsec.

   The security considerations applicable to the Diameter base protocol
   [RFC6733] are also applicable to this document, as are those in
   Section 8.4 of RFC 4072 [RFC4072].

5. IANA Considerations

   IANA has assigned values as described in the following sections.

5.1. AVP Codes

   Codes have been assigned for the following AVPs using the policy
   specified in [RFC6733], Section 11.1.1:

   o Key (581, Section 3.1)

   o Key-Type (582, Section 3.1.1)

   o Keying-Material (583, Section 3.1.3)

   o Key-Lifetime (584, Section 3.1.4)

   o Key-SPI (585, Section 3.1.5)

   o Key-Name (586, Section 3.1.2)

5.2. AVP Values

   IANA has created a new registry for values assigned to the Key-Type
   AVP and populated it with the decimal values defined in this document
   (Section 3.1.1). New values may be assigned for the Key-Type AVP
   using the "Specification Required" policy [RFC5226]; once values have
   been assigned, they MUST NOT be deleted, replaced, or modified.

6. Acknowledgements

   Thanks (in no particular order) to Niclas Comstedt, Semyon
   Mizikovsky, Hannes Tschofenig, Joe Salowey, Tom Taylor, Frank Xia,
   Lionel Morand, Dan Romascanu, Bernard Aboba, Jouni Korhonen, Stephen
   Farrel, Joel Halpern, Phillip Hallam-Baker, Sean Turner, and
   Sebastien Decugis for useful comments, suggestions, and review.

7. References

7.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H.
              Levkowetz, "Extensible Authentication Protocol (EAP)",
              RFC 3748, June 2004.

   [RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible
              Authentication Protocol (EAP) Application", RFC 4072,
              August 2005.

   [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
              IANA Considerations Section in RFCs", BCP 26, RFC 5226,
              May 2008.

   [RFC6733] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn,
              "Diameter Base Protocol", RFC 6733, October 2012.

7.2. Informative References

   [RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS
              Authentication Protocol", RFC 5216, March 2008.

   [RFC5247] Aboba, B., Simon, D., and P. Eronen, "Extensible
              Authentication Protocol (EAP) Key Management Framework",
              RFC 5247, August 2008.

   [RFC5295] Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri,
              "Specification for the Derivation of Root Keys from an
              Extended Master Session Key (EMSK)", RFC 5295,
              August 2008.

   [RFC6696] Cao, Z., He, B., Shi, Y., Wu, Q., Ed., and G. Zorn, Ed.,
              "EAP Extensions for the EAP Re-authentication Protocol
              (ERP)", RFC 6696, July 2012.

Authors' Addresses

   Glen Zorn
   Network Zen
   227/358 Thanon Sanphawut
   Bang Na, Bangkok 10260
   Thailand

   Phone: +66 (0) 909-201060
   EMail: glenzorn@gmail.com

   Qin Wu
   Huawei Technologies Co., Ltd.
   101 Software Avenue, Yuhua District
   Nanjing, Jiangsu 21001
   China

   Phone: +86-25-56623633
   EMail: sunseawq@huawei.com

   Violeta Cakulev
   Alcatel Lucent
   600 Mountain Ave.
   3D-517
   Murray Hill, NJ 07974
   US

   Phone: +1 908 582 3207
   EMail: violeta.cakulev@alcatel-lucent.com