Diameter Attribute-Value Pairs for Cryptographic Key Transport
draft-ietf-dime-local-keytran-02

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.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering
Task Force (IETF), its areas, and its working groups. Note that
other groups may also distribute working documents as Internet-
Drafts.

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."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at

This Internet-Draft will expire on September 5, 2010.

Copyright Notice

Copyright (c) 2010 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
Table of Contents

1. Introduction .............................................. 3
2. Terminology .............................................. 3
  2.1. Standards Language ................................ 3
  2.2. Technical Terms and Acronyms ..................... 3
3. Attribute-Value Pair Definitions ....................... 4
  3.1. Key AVP ................................................ 4
    3.1.1. Key-Type AVP .................................. 4
    3.1.2. Key-Name AVP .................................. 5
    3.1.3. Keying-Material AVP ......................... 5
    3.1.4. Key-Lifetime AVP .............................. 5
    3.1.5. Key-SPI ........................................ 5
4. Security Considerations .................................. 6
5. IANA Considerations ..................................... 6
  5.1. AVP Codes ............................................ 6
  5.2. AVP Values .......................................... 6
6. Acknowledgements ......................................... 6
7. References ................................................ 6
  7.1. Normative References ............................... 6
  7.2. Informative References ......................... 7
Authors’ Addresses ........................................... 7
1. Introduction

The Diameter 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
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
MSK. In addition, ERP [RFC5296] specifies new keys that may need to
be transported between Diameter nodes.

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

2. Terminology

2.1. Standards 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

DER
  Diameter EAP request [RFC4072].

DEA
  Diameter EAP Answer [RFC4072].

DSRK
  Domain-Specific Root Key [RFC5295].

DSUSRK
  Domain-Specific Usage-Specific Root Key. This is a Usage-Specific
  Root Key derived from a DSRK [RFC5295].

EAP
  Extensible Authentication Protocol [RFC3748].

EMSK
  Extended Master Session Key [RFC3748].
EAP Re-authentication Protocol [RFC5296].

Master Session Key [RFC3748].

reauthentication MSK [RFC5296]. This is a per-authenticator key, derived from the rRK (see below).

reauthentication Root Key, derived from the EMSK or DSRK [RFC5296].

Usage-Specific Root Key [RFC5295]

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 <AC1>) is of type Grouped [RFC3588] It contains the name, type and optionally, the usable lifetime of the key, as well as the keying material itself.

Key ::= < AVP Header: AC1 >
< Key-Type >
{ Keying-Material }
[ Key-Lifetime ]
[ Key-Name ]
[ Key-SPI ]
* [ AVP ]

3.1.1. Key-Type AVP

The Key-Type AVP (AVP Code <AC2>) is of type Enumerated and signifies the type of the key being sent. The following values are defined in this document:

MSK (0)
  The EAP Master Session Key [RFC3748]
DSRK (1)  
A Domain-Specific Root Key [RFC5295].

USRK (2)  
A Usage Specific Root Key [RFC5295].

rRK (3)  
A reauthentication Root Key [RFC5296].

rMSK (4)  
A reauthentication Master Session Key [RFC5296].

DSUSRK (5)  
A Domain-Specific Usage-Specific Root Key [RFC5295].

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 is of type OctetString. It contains an opaque key identifier. Exactly how this name is generated and used depends on the key type and link layer 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 <AC3>) is of type OctetString. The exact usage of this keying material depends upon several factors, including the link layer in use and the type of the key; it is beyond the scope of this document.

3.1.4. Key-Lifetime AVP

The Key-Lifetime AVP (AVP Code <AC4>) is of type Integer64 [RFC3588] 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 keying material is first used.

3.1.5. Key-SPI

The Key-SPI AVP (AVP Code <AC5>) is of type Unsigned32 and contains a Security Parameter Index (SPI) value that can be used with other parameters for identifying associated keying material.
4. Security Considerations

The security considerations applicable to the Diameter Base Protocol [RFC3588] are also applicable to this document, as are those in Section 8.4 of RFC 4072 [RFC4072].

5. IANA Considerations

Upon publication of this memo as an RFC, IANA is requested to assign values as described in the following sections.

5.1. AVP Codes

Codes must be assigned for the following AVPs using the policy specified in RFC 3588, Section 11.1.1:

- Key (<AC1>, Section 3.1)
- Key-Type (<AC2>, Section 3.1.1)
- Keying-Material (<AC3>, Section 3.1.3)
- Key-Lifetime (<AC4>, Section 3.1.4)
- Key-SPI (<AC5>, Section 3.1.5)

5.2. AVP Values

IANA is requested to create a new registry for values assigned to the Key-Type AVP and populated with the values defined in this document (Section 3.1.1). New values may be assigned for the Key-Type AVP using the "Expert Review" policy [RFC5226]; once values have been assigned, they MUST NOT be deleted, replaced, modified or deprecated.

6. Acknowledgements

Thanks to Semyon Mizikovsky, Hannes Tschofenig and Sebastien Decugis for useful comments.

7. References

7.1. Normative References


Levkowetz, "Extensible Authentication Protocol (EAP)",

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.

7.2. Informative References

[RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS

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.

[RFC5296] Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-
authentication Protocol (ERP)", RFC 5296, August 2008.

Authors’ Addresses

Glen Zorn (editor)
Network Zen
1463 East Republican Street
Seattle, Washington 98112
US

Email: gwz@net-zen.net