

Network Working Group	G. Zorn
Internet-Draft	Network Zen
Intended status: Standards Track	Q. Wu
Expires: February 20, 2012	Huawei
	V. Cakulev
	Alcatel Lucent
	August 19, 2011

Diameter Attribute-Value Pairs for Cryptographic Key Transport
draft-ietf-dime-local-keytran-14

[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 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 <http://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 February 20, 2012.

[Copyright Notice](#)

Copyright (c) 2011 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 (<http://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. [Terminology](#)
- *2.1. [Standards Language](#)
- *2.2. [Technical Terms and Acronyms](#)
- *3. [Attribute-Value Pair Definitions](#)
- *3.1. [Key AVP](#)
- *3.1.1. [Key-Type AVP](#)
- *3.1.2. [Key-Name AVP](#)
- *3.1.3. [Keying-Material AVP](#)
- *3.1.4. [Key-Lifetime AVP](#)
- *3.1.5. [Key-SPI](#)
- *4. [Security Considerations](#)
- *5. [IANA Considerations](#)
- *5.1. [AVP Codes](#)
- *5.2. [AVP Values](#)
- *6. [Acknowledgements](#)
- *7. [References](#)
- *7.1. [Normative References](#)
- *7.2. [Informative References](#)
- *[Authors' Addresses](#)

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 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 MSK. In addition, the EAP Re-authentication Protocol (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

DSRK

Domain-Specific Root Key [\[RFC5295\]](#).

MSK

Master Session Key [\[RFC3748\]](#).

rMSK

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

rRK

reauthentication Root Key, derived from the EMSK Extended Master Session Key [\[RFC3748\]](#) or DSRK [\[RFC5296\]](#).

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. 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: 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. This AVP identifies the type of the key being sent. The following decimal values are defined in this document: [Section 5.2](#),

DSRK (0)

A Domain-Specific Root Key [\[RFC5295\]](#).

rRK (1)

A reauthentication Root Key [\[RFC5296\]](#).

rMSK (2)

A reauthentication Master Session Key [\[RFC5296\]](#).

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

3.1.2. Key-Name AVP

The Key-Name AVP (AVP Code <AC6>) 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 <AC3>) 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 <AC4>) 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 [\[I-D.ietf-dime-rfc3588bis\]](#)).

[3.1.5. Key-SPI](#)

The Key-SPI AVP (AVP Code <AC5>) is of type Unsigned32 and contains a 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 Keying-Material 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 [\[I-D.ietf-dime-rfc3588bis\]](#) 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 [\[I-D.ietf-dime-rfc3588bis\]](#), 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](#))
- *Key-Name (<AC6>, [Section 3.1.2](#))

[5.2. AVP Values](#)

IANA is requested to create a new registry for values assigned to the Key-Type AVP and populated 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. Levkowitz, " Extensible Authentication Protocol (EAP) ", RFC 3748, June 2004.
[I-D.ietf-dime-rfc3588bis]	Fajardo, V, Arkko, J, Loughney, J and G Zorn, " Diameter Base Protocol ", Internet-Draft draft-ietf-dime-rfc3588bis-29, August 2011.
[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.

[7.2. Informative References](#)

[RFC5216]	Simon, D., Aboba, B. and R. Hurst, " The EAP-TLS Authentication Protocol ", RFC 5216, March 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.
[RFC5247]	Aboba, B., Simon, D. and P. Eronen, " Extensible Authentication Protocol (EAP) Key Management Framework ", RFC 5247, August 2008.

Authors' Addresses

Glen Zorn Zorn Network Zen 227/358 Thanon Sanphawut
Bang Na, Bangkok 10260 Thailand Phone: +66 (0) 87-040-4617 EMail:
glenzorn@gmail.com

Qin Wu Wu Huawei Technologies Co., Ltd. 101 Software Avenue, Yuhua
District Nanjing, Jiangsu 21001 China Phone: +86-25-56623633 EMail:
sunseawq@huawei.com

Violeta Cakulev Cakulev Alcatel Lucent 600 Mountain Ave. 3D-517
Murray Hill, NJ 07974 US Phone: +1 908 582 3207 EMail:
violeta.cakulev@alcatel-lucent.com