

Network Working Group	Q. Wu, Ed.	
Internet-Draft	Huawei	
Intended status: Standards Track	G. Zorn, Ed.	
Expires: June 10, 2010	Network Zen	
	December 07, 2009	

[TOC](#)

Diameter Attribute-Value Pairs for Cryptographic Key Transport draft-wu-dime-local-keytran-03

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. This document may not be modified, and derivative works of it may not be created, except to format it for publication as an RFC or to translate it into languages other than English.

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 <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on June 10, 2010.

Copyright Notice

Copyright (c) 2009 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 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
- [4.](#) AVP Occurrence Table
- [5.](#) Security Considerations
- [6.](#) IANA Considerations
 - [6.1.](#) AVP Codes
 - [6.2.](#) AVP Values
- [7.](#) Acknowledgements
- [8.](#) References
 - [8.1.](#) Normative References
 - [8.2.](#) Informative References
- [§](#) Authors' Addresses

1. Introduction

[TOC](#)

The Diameter EAP application (Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," August 2005.) [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] (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)," June 2004.) methods (for example, EAP-TLS [RFC5216] (Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol," March 2008.)). At most one instance of either of these AVPs is allowed in any Diameter message.

However, recent work [RFC5295] (Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys

[from an Extended Master Session Key \(EMSK\)," August 2008.](#)) 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 [\[RFC5296\] \(Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol \(ERP\)," August 2008.\)](#) 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

[TOC](#)

2.1. Standards Language

[TOC](#)

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 \(Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.\)](#) [RFC2119].

2.2. Technical Terms and Acronyms

[TOC](#)

DER Diameter EAP request [\[RFC4072\] \(Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol \(EAP\) Application," August 2005.\)](#).

DEA Diameter EAP Answer [\[RFC4072\] \(Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol \(EAP\) Application," August 2005.\)](#).

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

DSUSRK Domain-Specific Usage-Specific Root Key. This is a Usage-Specific Root Key derived from a DSRK [\[RFC5295\] \(Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key \(EMSK\)," August 2008.\)](#).

EAP

Extensible Authentication Protocol [\[RFC3748\]](#) (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)," June 2004.).

EMSK Extended Master Session Key [\[RFC3748\]](#) (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)," June 2004.).

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

MSK Master Session Key [\[RFC3748\]](#) (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)," June 2004.).

rMSK reauthentication MSK [\[RFC5296\]](#) (Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)," August 2008.). This is a per-authenticator key, derived from the rRK (see below).

rRK reauthentication Root Key, derived from the EMSK or DSRK [\[RFC5296\]](#) (Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)," August 2008.).

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

3. Attribute-Value Pair Definitions

[TOC](#)

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

[TOC](#)

The Key AVP (AVP Code <AC1>) is of type Grouped [\[RFC3588\]](#) (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.) 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 ]
      * [ AVP ]

```

3.1.1. Key-Type AVP

[TOC](#)

The Key-Type AVP (AVP Code <AC2>) is of type Enumerated and signifies the type of the key being sent. The Key-Type AVP MAY be included in a DER command as a signal that a certain type of key is required in the response (e.g., to support ERP). The following values are defined in this document:

- MSK (0)** The EAP Master Session Key [\[RFC3748\]](#) (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)," June 2004.)
- DSRK (1)** A Domain-Specific Root Key [\[RFC5295\]](#) (Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)," August 2008.).
- USRK (2)** A Usage Specific Root Key [\[RFC5295\]](#) (Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)," August 2008.).
- rRK (3)** A reauthentication Root Key [\[RFC5296\]](#) (Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)," August 2008.).
- rMSK (4)** A reauthentication Master Session Key [\[RFC5296\]](#) (Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)," August 2008.).
- DSUSRK (5)** A Domain-Specific Usage-Specific Root Key [\[RFC5295\]](#) (Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)," August 2008.).

If additional values are needed, they are to be assigned by IANA according to the policy stated in [Section 6.2 \(AVP Values\)](#)

3.1.2. Key-Name AVP

[TOC](#)

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 [\[RFC5247\]](#) (Aboba, B., Simon, D., and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework," August 2008.) and [\[RFC5295\]](#) (Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)," August 2008.) for discussions of key name generation in the context of EAP).

3.1.3. Keying-Material AVP

[TOC](#)

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

[TOC](#)

The Key-Lifetime AVP (AVP Code <AC4>) is of type Integer64 [\[RFC3588\]](#) (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.) and represents the period of time (in seconds) for which the contents of the Keying-Material AVP [Section 3.1.3 \(Keying-Material AVP\)](#) 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.

4. AVP Occurrence Table

[TOC](#)

The following table lists the AVPs that MAY be present in the DER and DEA commands [\[RFC4072\]](#) (Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," August 2005.).

	+-----+	
	Command-Code	
	+-----+	
AVP Name	DER	DEA
	+-----+	
Key	0	0+
Key-Type	0+	0
Key-Name	0-1	0-1
	+-----+	

DER and DEA Commands AVP Table

5. Security Considerations

[TOC](#)

The security considerations applicable to the Diameter Base Protocol [\[RFC3588\]](#) (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.) are also applicable to this document.

6. IANA Considerations

[TOC](#)

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

6.1. AVP Codes

[TOC](#)

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

- *Key (<AC1>, [Section 3.1 \(Key AVP\)](#))
- *Key-Type (<AC2>, [Section 3.1.1 \(Key-Type AVP\)](#))
- *Keying-Material (<AC3>, [Section 3.1.3 \(Keying-Material AVP\)](#))
- *Key-Lifetime (<AC4>, [Section 3.1.4 \(Key-Lifetime AVP\)](#))

6.2. AVP Values

[TOC](#)

New values may be assigned for the Key-Type AVP ([Section 3.1.1 \(Key-Type AVP\)](#)) using the "First Come First Served" policy [\[RFC5226\]](#) (Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," May 2008.).

7. Acknowledgements

[TOC](#)

Thanks to Semyon Mizikovsky and Sebastien Decugis for useful comments.

[Section 3.1.2 \(Key-Name AVP\)](#) is largely derived from Section 4.1.4 of RFC 4072 [\[RFC4072\]](#) (Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," August 2005.).

8. References

[TOC](#)

8.1. Normative References

[TOC](#)

[RFC2119]	Bradner, S. , "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT , HTML , XML).
[RFC3588]	Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, " Diameter Base Protocol ," RFC 3588, September 2003 (TXT).
[RFC3748]	Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, " Extensible Authentication Protocol (EAP) ," RFC 3748, June 2004 (TXT).
[RFC4072]	Eronen, P., Hiller, T., and G. Zorn, " Diameter Extensible Authentication Protocol (EAP) Application ," RFC 4072, August 2005 (TXT).
[RFC5226]	Narten, T. and H. Alvestrand, " Guidelines for Writing an IANA Considerations Section in RFCs ," BCP 26, RFC 5226, May 2008 (TXT).

8.2. Informative References

[TOC](#)

[RFC5216]	Simon, D., Aboba, B., and R. Hurst, " The EAP-TLS Authentication Protocol ," RFC 5216, March 2008 (TXT).
[RFC5247]	Aboba, B., Simon, D., and P. Eronen, " Extensible Authentication Protocol (EAP) Key Management Framework ," RFC 5247, August 2008 (TXT).
[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 (TXT).
[RFC5296]	Narayanan, V. and L. Dondeti, " EAP Extensions for EAP Re-authentication Protocol (ERP) ," RFC 5296, August 2008 (TXT).

Authors' Addresses

[TOC](#)

	Qin Wu (editor)
	Huawei Technologies Co., Ltd.
	Site B, Floor 12F, Huihong Mansion, No.91 Baixia Rd.
	Nanjing, JiangSu 210001
	China
Phone:	+86-25-84565892
Email:	Sunseawq@huawei.com
	Glen Zorn (editor)
	Network Zen
	1310 East Thomas Street
	Seattle, Washington 98102
	+1 (206) 377-9035
Email:	gwz@net-zen.net