Network Working Group	G. Zorn, Ed.
Internet-Draft	Network Zen
Intended status: Standards Track	Q. Wu, Ed.
Expires: January 2, 2011	Huawei
	V. Cakulev
	Alcatel Lucent
	July 1, 2010

TOC

Diameter Attribute-Value Pairs for Cryptographic Key Transport
draft-ietf-dime-local-keytran-07

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 January 2, 2011.

Copyright Notice

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

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 The Extensible Authentication Protocol (EAP) [RFC3748] (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "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 (see, for example, [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, the EAP Re-authentication Protocol (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

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.).

MSK Master Session Key [RFC3748] (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "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 (below).

rRK reauthentication Root Key, derived from the EMSK Extended Master Session Key [RFC3748] (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)," June 2004.) or DSRK [RFC5296] (Narayanan, V. and

L. Dondeti, “EAP Extensions for EAP Re-authentication Protocol (ERP),” 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] (Eronen, P., Hiller, T., and G. Zorn, “Diameter Extensible Authentication Protocol (EAP) Application,” August 2005.), 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 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

TOC

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

MSK (0) The EAP Master Session Key [RFC3748] (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, “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.).

rRK (2) A reauthentication Root Key [RFC5296] (Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)," August 2008.).

rMSK (3) A reauthentication Master Session Key [RFC5296] (Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)," August 2008.).

IKEv2-PSK (4) A pre-shared key for use in IKE-V2 key exchange [I-D.ietf-dime-ikev2-psk-diameter] (Cakulev, V. and A. Lior, "Diameter IKEv2 PSK: Pre-Shared Secret-based Support for IKEv2 Server to Diameter Server Interaction," March 2010.).

RSA-KEM (5) A symmetric keying material encrypted using the RSA public key of the recipient [I-D.ietf-smime-cms-rsa-kem] (Brainard, J., Turner, S., Randall, J., and B. Kaliski, "Use of the RSA-KEM Key Transport Algorithm in CMS," May 2010.).

If additional values are needed, they are to be assigned by IANA according to the policy stated in Section 5.2 (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 usage 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 message containing the keying material is received.

3.1.5. Key-SPI

TOC

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

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, as are those in Section 8.4 of RFC 4072 [RFC4072] (Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," August 2005.).

---

5. IANA Considerations

TOC

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

TOC

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 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))
- *Key-SPI (<AC5>, Section 3.1.5 (Key-SPI))

5.2. AVP Values

TOC

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 (Key-Type AVP)). New values may be assigned for the Key-Type AVP using the "Expert Review" policy [RFC5226] (Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” May 2008.); once values have been assigned, they MUST NOT be deleted, replaced, modified or deprecated.

---

6. Acknowledgements

TOC

Thanks to Semyon Mizikovsky, Hannes Tschofenig, Joe Salowey, Tom Taylor, Frank Xia and Sebastien Decugis for useful comments.

---

7. References

TOC

7.1. 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. Levkowetz, “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).

7.2. Informative References

TOC

[I-D.ietf-dime-ikev2-psk-diameter]	Cakulev, V. and A. Lior, “Diameter IKEv2 PSK: Pre-Shared Secret-based Support for IKEv2 Server to Diameter Server Interaction,” draft-ietf-dime-ikev2-psk-diameter-02 (work in progress), March 2010 (TXT).
[I-D.ietf-smime-cms-rsa-kem]	Brainard, J., Turner, S., Randall, J., and B. Kaliski, “Use of the RSA-KEM Key Transport Algorithm in CMS,” draft-ietf-smime-cms-rsa-kem-13 (work in progress), May 2010 (TXT).
[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

	Glen Zorn (editor)
	Network Zen
	1463 East Republican Street
	#358
	Seattle, Washington 98112

	US
Email:	gwz@net-zen.net
	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
	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