Diameter Maintenance and
Extensions (DIME)
Internet-Draft
Intended status: Standards Track
Expires: January 15, 2009

L. Dondeti
QUALCOMM, Inc.

July 14, 2008

Diameter Support for EAP Re-authentication Protocol
draft-dondeti-dime-erp-diameter-02.txt

Status of this Memo

This Internet-Draft will expire on January 15, 2009.

Abstract

An EAP extension, called "EAP Re-authentication Protocol (ERP)", has been specified that supports an EAP method-independent protocol for efficient re-authentication between the peer and the server through an authenticator. This document specifies Diameter support for ERP. The Diameter EAP application is re-used for encapsulating the newly defined EAP Initiate and EAP Finish messages specified in the ERP specification. AVPs for request and delivery of Domain Specific Root Keys from the AAA/EAP server to the ER server are also specified. Additionally, this document also specifies Diameter processing rules relevant to ERP.

Table of Contents

1. Introduction

RFC 4072 [1] specifies a Diameter application that carries EAP packets between a Diameter client and the Diameter Server/EAP server. [2] defines the EAP Re-authentication Protocol to allow faster re-authentication of a previously authenticated peer. In ERP, a peer authenticates to the network by proving possession of key material derived during a previous EAP exchange. For this purpose, an Extended Master Session Key (EMSK) based re-authentication key hierarchy has been defined [5]. ERP may be executed between the ER peer and an ER server in the peer's home domain or the local domain visited by the peer. In the latter case, a Domain Specific Root Key (DSRK), derived from the EMSK, is provided to the local domain ER server. The peer and the local server subsequently use the re-authentication key hierarchy from the DSRK to authenticate and derive authenticator specific keys within that domain. To accomplish the reauthentication functionality, ERP defines two new EAP codes - EAP Initiate and EAP Finish. This document specifies the reuse of Diameter EAP application to carry these new EAP messages.

The DSRK can be obtained as part of the regular EAP exchange or as part of an ERP bootstrapping exchange. The local ER server requesting the DSRK needs to be in the path of the EAP or ERP bootstrapping exchange in order to request and obtain the DSRK. This document also specifies how the DSRK is transported to the local ER server using Diameter.

2. Terminology

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 [3].

This document uses terminology defined in [6], [5], [2], and [1].

3. Assumptions

This document defines additional optional AVPs for usage with the Diameter EAP application. Routing of these messages is therefore provided via the Diameter Application Identifier (among other elements), as specified by the Diameter Base protocol [4]. Based on the deployment of ERP, a local Diameter server (the same entity serves as a Diameter proxy during the full EAP authentication) may play the role of the ER server for future re-authentication attempts. As such, the local Diameter server requesting the DSRK needs to be in the path of the current EAP exchange between the peer and the EAP

server and also along in the future. The Diameter client is furthermore assumed to be able to route the re-authentication messages to the ER server.

4. Diameter Support for ERP

4.1. Protocol Overview

Diameter may be used to transport ERP messages between the NAS (authenticator) and an authentication server (ER server).

In ERP, the peer sends an EAP Initiate Reauth message to the ER server via the authenticator. Alternatively, the NAS may send an EAP Initiate Reauth-Start message to the peer to trigger the start of ERP; the peer then responds with an EAP Initiate Reauth message to the NAS.

The general guidelines for encapsulating EAP messages in Diameter from RFC 4072 [1] apply to the new EAP messages defined for ERP as well. The EAP Initiate Reauth message is encapsulated in an EAP-Payload AVP of a Diameter EAP-Request message by the NAS and sent to the Diameter server. The NAS MUST copy the contents of the value field of the 'rIKName as NAI' TLV or the peer-id TLV (when the former is not present) of the EAP Initiate Reauth message into a User-Name AVP of the Diameter EAP-Request.

The ER server processes the EAP Initiate Reauth message in accordance with [2], and if that is successful, it responds with an EAP Finish Reauth message indicating a success ('R' flag set to 0). The Diameter server MUST encapsulate the EAP Finish Reauth message with the R flag set to zero in an EAP-Payload AVP attribute of a Diameter EAP-Answer message. An EAP-Master-Session-Key AVP included in the Diameter EAP-Answer contains the Re-authentication Master Session Key (rMSK). The Diameter Result Code, if any, SHOULD be a success Result Code.

If the processing of the EAP Initiate Reauth message resulted in a failure, the Diameter server MUST encapsulate an EAP Finish Reauth message indicating failure ('R' flag set to 1) in an EAP-Payload AVP of a Diameter EAP-Answer message. The Diameter Result Code, if any, SHOULD be a failure Result Code. Whether an EAP Finish Reauth message is sent at all is specified in [2].

4.2. DSRK Request and Delivery

A local ER server, collocated with a Diameter proxy in the peer's visited domain, may request a DSRK from the EAP server, either in the

initial EAP exchange (implicit bootstrapping) or in an ERP bootstrapping exchange (explicit bootstrapping). It does this by including the EAP-DSRK-Request AVP in the Diameter EAP-Response message. The EAP-DSRK-Request AVP contains the domain or server identity required to derive the DSRK.

An EAP server MAY send the DSRK when it receives a valid Diameter EAP-Request message containing an EAP-DSRK-Request AVP. An ER server MUST send the DSRK (or send a failure result) when it receives a valid Diameter EAP-Request message containing an EAP-DSRK-Request AVP along with a valid EAP Initiate Re-auth packet with the bootstrapping flag turned on. If an EAP-DSRK-Request AVP is included in any other Diameter EAP-Request message, the Diameter server MUST reply with a failure result. An EAP-DSRK AVP MUST be used to send a DSRK; an EAP-DSRK-Name AVP MUST be used to send the DSRK's keyname; and an EAP-DSRK-Lifetime AVP MUST be used to send the DSRK's lifetime.

5. Command Codes

This document re-uses the EAP application commands [1]:

Command-Name	Abbrev.	Code	Reference	Application
Diameter-EAP-Request	DER	268	RFC 4072	EAP
Diameter-EAP-Answer	DEA	268	RFC 4072	EAP

Figure 1: ERP Command Codes

Re-Auth-Request (RAR) may trigger ERP.

Session-Termination-Request (STR), Session-Termination-Answer (STA), Abort-Session-Request (ASR), Abort-Session-Answer (ASA), Accounting-Request (ACR), and Accounting-Answer (ACA) commands are used together with Diameter ERP, they follow the rules in the Diameter EAP application [1] and the Diameter Base specification [4]. The accounting commands use the Application Identifier value of 3 (Diameter Base Accounting); the others use 0 (Diameter Common Messages).

5.1. Diameter-EAP-Request (DER)

The Diameter-EAP-Request (DER) message [1], indicated by the Command-Code field set to 268 and the 'R' bit set in the Command Flags field, is sent by the NAS to the Diameter server to initiate a network access authentication and authorization procedure.

The DEA message format is the same as defined in [1] with an addition of optional EAP Re-authentication Protocol (ERP) AVPs. The addition of the EAP-DSRK-Request AVP to the Diameter-EAP-Request message indicates that an ERP server is present and willing to participate in the ERP protocol for this session. Furthermore, the EAP-DSRK-Request AVP provides identity information about the domain of the ERP server.

```
<Diameter-EAP-Request> ::= < Diameter Header: 268, REQ, PXY >
                           < Session-Id >
                           { Auth-Application-Id }
                           { Origin-Host }
                           { Origin-Realm }
                           { Destination-Realm }
                           { Auth-Request-Type }

                           [ EAP-DSRK-Request ]

                           [ User-Name ]
                           [ Destination-Host ]
                           ...
                         * [ AVP ]
```

5.2. Diameter-EAP-Answer (DEA)

The Diameter-EAP-Answer (DEA) message defined in [1], indicated by the Command-Code field set to 268 and 'R' bit cleared in the Command Flags field, is sent in response to the Diameter-EAP-Request message (DER).

The DEA message format is the same as defined in [1] with an addition of optional EAP Re-authentication Protocol (ERP) AVPs. The addition of the EAP-DSRK, EAP-DSRK-Name and the EAP-DSRK-Lifetime AVP to the Diameter-EAP-Answer message indicates that an Diameter / ER server is able to provide ERP support for this session and delivers keying material, lifetime and a key name.

```
<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY >
                          < Session-Id >
                          { Auth-Application-Id }
                          { Auth-Request-Type }
                          { Result-Code }
                          { Origin-Host }
                          { Origin-Realm }

                          [ EAP-DSRK ]
                          [ EAP-DSRK-Name ]
                          [ EAP-DSRK-Lifetime ]

                          [ User-Name ]
                          ...
                        * [ AVP ]
```

6. Attribute Value Pair Definitions

6.1. EAP-DSRK-Request AVP

The EAP-DSRK AVP (AVP Code TBD) is of type DiameterIdentity. This AVP fulfills two purposes: First, it indicates that a ER server is located in the local domain that is willing to play the role of an ER server for a particular session. Second, it conveys information about the domain and ER server identity to the Diameter/EAP server.

6.2. EAP-DSRK AVP

The EAP-DSRK AVP (AVP Code TBD) is of type OctetString. The Domain Specific Root Key (DSRK) is carried in this payload.

6.3. EAP-DSRK-Name AVP

The EAP-DSRK-Name AVP (AVP Code TBD) is of type OctetString. This AVP contains the name of the DSRK key that is later used during the re-authentication exchange to select the correct DSRK.

6.4. EAP-DSRK-Lifetime AVP

The EAP-DSRK-Lifetime AVP (AVP Code TBD) is of type Unsigned64 and contains the DSRK lifetime in seconds.

7. AVP Occurrence Table

The following table lists the AVPs that may optionally be present in the DER and DEA commands [1].

Attribute Name	Command-Code	
	DER	DEA
EAP-DSRK-Request	0-1	0
EAP-DSRK	0	0-1
EAP-DSRK-Name	0	0-1
EAP-DSRK-Lifetime	0	0-1

Figure 2: DER and DEA Commands AVP Table

When the EAP-DSRK AVP is present in the DEA then the EAP-DSRK-Name and the EAP-DSRK-Lifetime MUST also be present.

8. AVP Flag Rules

The following table describes the Diameter AVPs, their AVP Code values, types, possible flag values, and whether the AVP MAY be encrypted. The Diameter base [4] specifies the AVP Flag rules for AVPs in Section 4.5.

Attribute Name	AVP Code	Section Defined	Data Type	AVP Flag Rules				
				MUST	MAY	SHLD NOT	MUST NOT	Encr
EAP-DSRK-Request	TBD	4.7.1	DiamIdent		P		V,M	Y
EAP-DSRK	TBD	4.7.2	OctetString		P		V,M	Y
EAP-DSRK-Name	TBD	4.7.3	OctetString		P		V,M	Y
EAP-DSRK-Lifetime	TBD	4.7.4	Unsigned64		P		V,M	Y

Due to space constraints, the short form DiamIdent is used to represent DiameterIdentity.

Figure 3: AVP Flag Rules Table

9. Security Considerations

The security considerations specified in RFC 4072 [1], and RFC 3588 [4] are applicable to this document.

EAP channel bindings may be necessary to ensure that the Diameter client and the server are in sync regarding the key Requesting Entity's Identity. Specifically, the Requesting Entity advertises its identity through the EAP lower layer, and the user or the EAP peer communicates that identity to the EAP server (and the EAP server communicates that identity to the Diameter server) via the EAP method for user/peer to server verification of the Requesting Entity's Identity.

10. IANA Considerations

This document requires IANA registration of the following new AVPs to the AVP registry established by RFC 3588 [4]:

- EAP-DSRK-Request
- EAP-DSRK
- EAP-DSRK-Name
- EAP-DSRK-Lifetime

11. Acknowledgments

Vidya Narayanan reviewed a rough draft version and found some errors. Many thanks for her input.

12. References

12.1. Normative References

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

[2] Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)", draft-ietf-hokey-erx-14 (work in progress), March 2008.

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

[4] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

12.2. Informative References

[5] Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", draft-ietf-hokey-emsk-hierarchy-07 (work in progress), June 2008.

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

Author's Address

Lakshminath Dondeti
QUALCOMM, Inc.
5775 Morehouse Dr
San Diego, CA
USA

Phone: +1 858-845-1267
Email: ldondeti@qualcomm.com

Full Copyright Statement

Intellectual Property