Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 28, 2008

K. Gaonkar
Georgia Tech University
L. Dondeti
V. Narayanan
QUALCOMM, Inc.
G. Zorn

February 25, 2008

# RADIUS Support for EAP Re-authentication Protocol
# draft-gaonkar-radext-erp-attrs-03

## Status of this Memo



## Copyright Notice



## Abstract

RFCxxxx (draft-ietf-hokey-erx after publication) [6] specifies the EAP Re-authentication Protocol (ERP). This document specifies RADIUS support for ERP. The procedures in RFC3579 [1] are used for encapsulating the EAP Initiate and Finish messages specified in RFCxxxx (draft-ietf-hokey-erx after publication) [6]. This document

specifies attributes for the request and delivery of Domain Specific Root Keys from the AAA/EAP server to the ER Server. Additionally, this document also specifies RADIUS message processing rules relevant to ERP.

Table of Contents

## 1. Introduction

RFC3579 [1] specifies EAP message encapsulation in RADIUS messages. [6] 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, ERP defines two new EAP codes - EAP Initiate and EAP Finish. This document specifies the encapsulation of these messages in RADIUS. In addition, a Domain Specific Root Key (DSRK) may be transported from the RADIUS or EAP Server to an EAP Re-authentication (ER) server in the local domain for the purpose of re-authenticating the peer within that domain (see Figure 2 of [6]. This document defines how the DSRK is transported to the ER server using RADIUS.

## 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 [2].

This document uses terminology defined in [7], [8], [6], and [1].

## 3. RADIUS Support for ERP

The EAP Re-authentication Protocol, defined in [6], provides a mechanism for efficient re-authentication of EAP peers that have unexpired keying material from a previous EAP exchange. For this purpose, an Extended Master Session Key (EMSK) based re-authentication key hierarchy has been defined [8]. 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.

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.

### 3.1. Protocol Overview

RADIUS 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 RADIUS from RFC3579 [1] apply to the new EAP messages defined for ERP as well. The EAP Initiate Reauth message is encapsulated in an EAP-Message attribute of a RADIUS Access-Request message by the NAS and sent to the RADIUS server. In order to permit non-EAP aware RADIUS proxies to forward the Access-Request packet, 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 the User-Name attribute of the Access-Request.

The ER server processes the EAP Initiate Reauth message in accordance with [6], and if that is successful, it responds with an EAP Finish Reauth message indicating a success ('R' flag set to 0). The RADIUS server MUST encapsulate the EAP Finish Reauth message with the R flag set to zero in an EAP-Message attribute of a RADIUS Access-Accept message. The Re-authentication Master Session Key (rMSK) is transported along with this message to the NAS. The rMSK transport follows the same procedures of MSK transport along with EAP Success messages in a regular EAP exchange. The MS-MPPE-Recv-Key and MS-MPPE-Send-Key attributes defined in RFC2548 [3] are used to transport the rMSK from the server to the NAS as follows:

MS-MPPE-Recv-Key = rMSK (0, n/2-1)

MS-MPPE-Send-Key = rMSK (n/2, n-1)

where, 'n' is the total length of the rMSK in octets and the (x, y) notation indicates the starting and ending octets of the key material.

If the processing of the EAP Initiate Reauth message resulted in a failure, the RADIUS server MUST encapsulate an EAP Finish Reauth message indicating failure ('R' flag set to 1) in an EAP-Message attribute of a RADIUS Access-Reject message. Whether the RADIUS server sends an EAP Finish Reauth message is specified in [6].

### 3.2. DSRK Request and Delivery

A local ER server, collocated with a RADIUS server in the peer's visited domain, may request a DSRK from the EAP server, either in the initial EAP exchange or in an ERP bootstrapping exchange. The key request and delivery mechanism specified in [9] is used. A RADIUS server acting as an ER server may include the Keying-Material attribute defined in [9] in the RADIUS Access-Request message containing an EAP Response packet or an EAP Initiate Reauth packet in the EAP-Message attribute. The App ID field of the Keying-Material attribute MUST be set to "EAP DSRK" and the Optional Data field SHOULD be set to the domain or server identity required to derive the DSRK. The RADIUS server requesting the DSRK needs to be in the path of the corresponding EAP or ERP exchange between the peer and the EAP or ER server.

The RADIUS server, acting as the EAP server, if it wishes to include a DSRK in response to a request for it, SHOULD include the Keying-Material attribute defined in [9] in the RADIUS Access-Accept message (containing either an EAP Success or EAP Finish Reauth with the 'R' flag set to 0). The App ID of the Keying-Material attribute MUST be set to "EAP DSRK" and the Optional Data field SHOULD be set to the domain or server identity used by the EAP server to derive the DSRK. The encrypted DSRK itself must be included in the Data field of the Keying-Material attribute in accordance with [9].

### 3.3. Conflicting Messages

In addition to the rules specified in Section 2.6.3. of RFC3579 [1], the following combinations SHOULD NOT be sent by a RADIUS Server:

Access-Accept/EAP-Message/EAP Finish Reauth with 'R' flag set to 1

Access-Reject/EAP-Message/EAP Finish Reauth with 'R' flag set to 0

Access-Reject/Keying-Material

Access-Challenge/EAP-Message/EAP Initiate Reauth

Access-Challenge/EAP-Message/EAP Finish Reauth

## 4. Security Considerations

The security considerations specified in RFC 3579 [1], RFC 2548 [3], and [9] are applicable to this document.

## 5. IANA Considerations

This document requires IANA registration of the following value of the App ID field for the RADIUS Keying-Material attribute:

2 ... EAP DSRK

## 6. Acknowledgments

## 7. References

### 7.1. Normative References

[1] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

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

[3] Zorn, G., "Microsoft Vendor-specific RADIUS Attributes", RFC 2548, March 1999.

[4] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[5] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", draft-narten-iana-considerations-rfc2434bis-08 (work in progress), October 2007.

### 7.2. Informative References

[6] Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)", draft-ietf-hokey-erx-12 (work in progress), February 2008.

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

[8] 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-04 (work in progress), February 2008.

[9] Zorn, G., "RADIUS Attributes for the Delivery of Keying Material", draft-zorn-radius-keywrap-13 (work in progress), April 2007.

## Authors' Addresses

Kedar Gaonkar
Georgia Tech University

Email: kgaonkar3@gatech.edu

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

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

Vidya Narayanan
QUALCOMM, Inc.
5775 Morehouse Dr
San Diego, CA
USA

Phone: +1 858-845-2483
Email: vidyan@qualcomm.com

Glen Zorn

Email: glenzorn@comcast.net

## Full Copyright Statement



## Intellectual Property



## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).