

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

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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 August 28, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	RADIUS Support for ERP . . . . .	<a href="#">3</a>
<a href="#">3.1.</a>	Protocol Overview . . . . .	<a href="#">4</a>
<a href="#">3.2.</a>	DSRK Request and Delivery . . . . .	<a href="#">5</a>
<a href="#">3.3.</a>	Conflicting Messages . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Security Considerations . . . . .	<a href="#">5</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">6</a>
<a href="#">6.</a>	Acknowledgments . . . . .	<a href="#">6</a>
<a href="#">7.</a>	References . . . . .	<a href="#">6</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">6</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">6</a>
	Authors' Addresses . . . . .	<a href="#">7</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">8</a>



## **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

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

## Acknowledgment

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

