RADIUS attributes for Domain-specific Key Request and Delivery
draft-gaonkar-radext-erp-attrs-00

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 December 31, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document specifies the Key-Request and Key-Response attributes in Remote Authentication and Dial-In User Service (RADIUS). These attributes can be used by a visited network entity to request a key from the home network and the home domain to deliver the key to the visited network entity; the request and response may be piggy-backed on the EAP authentication or EAP Re-authentication bootstrapping exchange between the user and the user’s home RADIUS server or may be
part of a separate exchange.

Table of Contents

1. Introduction ............................................. 3
2. Terminology .............................................. 3
3. RADIUS Key-Request Attribute ............................. 3
4. RADIUS Key-Response Attribute .......................... 4
5. Security Considerations .................................. 6
6. IANA Considerations ..................................... 7
7. Acknowledgments .......................................... 7
8. References ................................................. 8
   8.1. Normative References ................................ 8
   8.2. Informative References .............................. 8
Authors’ Addresses ........................................... 8
Intellectual Property and Copyright Statements .............. 10
1. Introduction

This document specifies two new RADIUS attributes for the purpose of a user’s visited domain entity to request a cryptographic key from the home RADIUS server, and for the home RADIUS server to deliver the key to the visited domain entity that sent the request. The request and response may be piggy-backed on EAP authentication [5] or EAP Re-authentication bootstrapping exchanges [6] between the user and the user’s home RADIUS server or may be part of a separate exchange.

The Extended Master Session Key (EMSK) hierarchy specified in [2] contains Domain-Specific Root Keys (DSRK) specific to an administrative domain. It is plausible for a visited domain entity to request the home domain for a DSRK from the user’s home RADIUS server during EAP authentication or EAP Re-authentication bootstrapping protocol exchange. There is also proposed work on specifying a generic DSRK request protocol. When RADIUS is used as the AAA protocol, the Key-Request attribute specified in this document is used for requesting a key and the Key-Response attribute is used to deliver the key.

The key-request attribute contains the requesting entity’s identity and the type of the key being requested.

The key-response attribute contains the requesting entity’s identity, the type of the key, the key itself, its length, name and lifetime.

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].

3. RADIUS Key-Request Attribute

Description

The RADIUS Key-Request attribute provides a means for a visited domain server to request a key from the home domain of the user. This attribute MAY be used in Access-Request messages by a visited domain server and MUST NOT be used in Access-Challenge, Access-Accept or Access-Reject messages.
Other than the 1-octet Type and Length fields, this attribute has a 1-octet field to indicate the type of the key being requested and a variable length field to carry the Requesting Entity’s Identity.

The Requesting Entity’s Identity is to be copied in the corresponding Key-Response attribute.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length    |    Key Type   | Requesting    |
|              ~     Entity’s Identity (String)    ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Key-Request Attribute

Type

IANA-TBD for Key-Request

Length

>= 4

Key Type

This 1-octet field indicates the type of the key being requested:

0 ....... Reserved

1 ....... Domain-Specific Root Key (DSRK)

Requesting Entity’s Identity The Requesting Entity’s Identity is a string, and typically takes the form of a fully qualified domain name (FQDN).

4. RADIUS Key-Response Attribute

Description
The RADIUS Key-Response attribute MAY be included in the Access-Accept message by the user’s home RADIUS server to send the requested key type, key, its name, length, and lifetime. In addition, the requesting entity’s identity MAY be included. This attribute MUST NOT be used in Access-Request, Access-Challenge or Access-Reject messages.

Other than the 1-octet Type and Length fields, this attribute has a 1-octet field to indicate the type of the key being included, a 1-octet key length field, a 4-octet key lifetime field, an 8-octet key name field, a variable length field to carry the key and optionally a variable length field to carry the Requesting Entity’s Identity.

The Requesting Entity’s Identity is to be copied from the corresponding Key-Request attribute.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length    |    Key Type   |  Key Length   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Key Lifetime (4 Octets)...                                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Key Name (8 Octets)...                                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Key (Variable)                                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Requesting Entity’s Identity (String, Variable) Optional ... |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Key-Response Attribute

Type

IANA-TBD for Key-Response

Length

>= 80

Key Type
This 1-octet field indicates the type of the key being requested. This value is copied from the corresponding Key-Request attribute.

Key Length

This 1-octet field indicates the length of the key in octets. Since the length of the entire message is also included with a 1-octet field, key length cannot be larger than 240 octets. If the optional attribute "Requesting Entity’s Identity" is included in the message, the key length is smaller. Key length MUST be at least 64 octets.

Key Lifetime

The key lifetime in seconds is indicated within a 4-octet field.

Key Name

The key name field in 8 octets in size.

Key

The key of type Key Type is included in this field. This is a variable length field.

A stricter version of RFC 3756 requirements apply for RADIUS messages carrying Key-Response Attribute(s). Implementations of this specification MUST support IPsec along with IKEv2 for key management. IPsec ESP with a non-null transform MUST be supported, and IPsec ESP with a non-null encryption transform and authentication support is necessary to provide per-packet confidentiality, authentication, integrity and replay protection.

Requesting Entity’s Identity

The Requesting Entity’s Identity is a string, and typically takes the form of a fully qualified domain name (FQDN). This field is optional. Given that the Key Length must be at least 64 octets, this field can at most be 192 octets in length.

5. Security Considerations

A stricter version of RFC 3756 requirements apply for RADIUS messages carrying Key-Response Attribute(s). Implementations of this specification MUST support IPsec along with IKEv2 for key management. IPsec ESP with a non-null transform MUST be supported, and IPsec ESP with a non-null encryption transform and authentication support is necessary to provide per-packet confidentiality, authentication,
integrity and replay protection.

EAP Channel bindings may be necessary to ensure that the RADIUS user and the server are in synchronization 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 RADIUS server) via the EAP method for user/peer to server verification of the Requesting Entity’s Identity.

6. IANA Considerations

This document specifies the following IANA registrations in the RADIUS Attribute Types Registry at
http://www.iana.org/assignments/radius-types

   Key-Request
   Key-Response

Within the attributes Key-Request and Key-Response, a Key Type field is being specified with the following assignments and rules:

  0 .......  Reserved
  1 .......  Domain-Specific Root Key (DSRK)
  2-191 .....  IANA-managed (Expert Review)
  192-223 .......  Experimental Use
  224-255 ......  Private Use

7. Acknowledgments

This work originated from Kedar’s work as an intern at QUALCOMM; Kedar wants to thank QUALCOMM for their support. Thanks to Vidya Narayanan, Raymond Hsu, Jun Wang, Fatih Ulupinar for their review and comments.

8. References
8.1. Normative References


8.2. Informative References


Authors’ Addresses

Kedar Gaonkar
Georgia Institute of Technology
Atlanta, GA
USA

Phone: +1 404-201-0432
Email: kgaonkar3@gatech.edu

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

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

Copyright (C) The IETF Trust (2007).

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.

Acknowledgment

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