Internet Engineering Task Force (IETF)
Request for Comments: 5904
Category: Informational
ISSN: 2070-1721
G. Zorn
Network Zen
June 2010

RADIUS Attributes for IEEE 802.16 Privacy Key Management Version 1 (PKMv1) Protocol Support

Abstract

This document defines a set of Remote Authentication Dial-In User Service (RADIUS) Attributes that are designed to provide RADIUS support for IEEE 802.16 Privacy Key Management Version 1.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5904.

Copyright Notice

Table of Contents

1. Introduction

Privacy Key Management Version 1 (PKMv1) [IEEE.802.16-2004] is a public-key-based authentication and key establishment protocol typically used in fixed wireless broadband network deployments. The protocol utilizes X.509 v3 certificates [RFC2459], RSA encryption [RFC2437], and a variety of secret key cryptographic methods to allow an 802.16 Base Station (BS) to authenticate a Subscriber Station (SS) and perform key establishment and maintenance between an SS and BS.

This document defines a set of RADIUS Attributes that are designed to provide support for PKMv1. The target audience for this document consists of those developers implementing RADIUS support for PKMv1; therefore, familiarity with both RADIUS [RFC2865] and the IEEE 802.16-2004 standard is assumed.

Please note that this document relies on IEEE.802.16-2004, which references RFC 2437 and RFC 2459, rather than any more recent RFCs on RSA and X.509 certificates (e.g., RFC 3447 and RFC 5280).

2. Acronyms

CA
    Certification Authority; a trusted party issuing and signing X.509 certificates.

For further information on the following terms, please see Section 7 of [IEEE.802.16-2004].

SA
    Security Association

SAID
    Security Association Identifier

TEK
    Traffic Encryption Key

3. Attributes

The following subsections describe the Attributes defined by this document. This specification concerns the following values:

137 PKM-SS-Cert

138 PKM-CA-Cert

139 PKM-Config-Settings

140 PKM-Cryptosuite-List

141 PKM-SAID

142 PKM-SA-Descriptor

143 PKM-Auth-Key

3.1. PKM-SS-Cert

Description

The PKM-SS-Cert Attribute is variable length and MAY be transmitted in the Access-Request message. The Value field is of type string and contains the X.509 certificate [RFC2459] binding a public key to the identifier of the Subscriber Station.

The minimum size of an SS certificate exceeds the maximum size of a RADIUS attribute. Therefore, the client MUST encapsulate the certificate in the Value fields of two or more instances of the PKM-SS-Cert Attribute, each (except possibly the last) having a length of 255 octets. These multiple PKM-SS-Cert Attributes MUST appear consecutively and in order within the packet. Upon receipt, the RADIUS server MUST recover the original certificate by concatenating the Value fields of the received PKM-SS-Cert Attributes in order.

A summary of the PKM-SS-Cert Attribute format is shown below. The fields are transmitted from left to right.

```
                    1                   2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |      Len      |    Value...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

137 for PKM-SS-Cert

Len

> 2

Value

The Value field is variable length and contains a (possibly complete) portion of an X.509 certificate.

3.2. PKM-CA-Cert

Description

The PKM-CA-Cert Attribute is variable length and MAY be transmitted in the Access-Request message. The Value field is of type string and contains the X.509 certificate [RFC2459] used by the CA to sign the SS certificate carried in the PKM-SS-Cert attribute (Section 3.1) in the same message.

The minimum size of a CA certificate exceeds the maximum size of a RADIUS attribute. Therefore, the client MUST encapsulate the certificate in the Value fields of two or more instances of the PKM-CA-Cert Attribute, each (except possibly the last) having a length of 255 octets. These multiple PKM-CA-Cert Attributes MUST appear consecutively and in order within the packet. Upon receipt, the RADIUS server MUST recover the original certificate by concatenating the Value fields of the received PKM-CA-Cert Attributes in order.

A summary of the PKM-CA-Cert Attribute format is shown below. The fields are transmitted from left to right.

```
                     1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |      Len      |    Value...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

138 for PKM-CA-Cert

Len

> 2

Value

The Value field is variable length and contains a (possibly complete) portion of an X.509 certificate.

3.3. PKM-Config-Settings

Description

The PKM-Config-Settings Attribute is of type string [RFC2865]. It is 30 octets in length and consists of seven independent fields, each of which is conceptually an unsigned integer. Each of the fields contains a timeout value and corresponds to a Type-Length-Value (TLV) tuple encapsulated in the IEEE 802.16 "PKM configuration settings" attribute; for details on the contents of each field, see Section 11.9.19 of [IEEE.802.16-2004]. One instance of the PKM-Config-Settings Attribute MAY be included in the Access-Accept message.

A summary of the PKM-Config-Settings Attribute format is shown below. The fields are transmitted from left to right.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |      Len      |       Auth Wait Timeout
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    Auth Wait Timeout (cont.)   |      Reauth Wait Timeout
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   Reauth Wait Timeout (cont.)  |        Auth Grace Time
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Auth Grace Time (cont.)    |        Op Wait Timeout
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Op Wait Timeout (cont.)    |       Rekey Wait Timeout
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   Rekey Wait Timeout (cont.)   |         TEK Grace Time
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     TEK Grace Time (cont.)     |     Auth Rej Wait Timeout
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  Auth Rej Wait Timeout (cont.) |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

139 for PKM-Config-Settings

Len

30

Auth Wait Timeout

The Auth Wait Timeout field is 4 octets in length and corresponds to the "Authorize wait timeout" field of the 802.16 "PKM configuration settings" attribute.

Reauth Wait Timeout

The Reauth Wait Timeout field is 4 octets in length and corresponds to the "Reauthorize wait timeout" field of the 802.16 "PKM configuration settings" attribute.

Auth Grace Time

The Auth Grace Time field is 4 octets in length and corresponds to the "Authorize grace time" field of the 802.16 "PKM configuration settings" attribute.

Op Wait Timeout

The Op Wait Timeout field is 4 octets in length and corresponds to the "Operational wait timeout" field of the 802.16 "PKM configuration settings" attribute.

Rekey Wait Timeout

The Rekey Wait Timeout field is 4 octets in length and corresponds to the "Rekey wait timeout" field of the 802.16 "PKM configuration settings" attribute.

TEK Grace Time

The TEK Grace Time field is 4 octets in length and corresponds to the "TEK grace time" field of the 802.16 "PKM configuration settings" attribute.

Auth Rej Wait Timeout

The Auth Rej Wait Timeout field is 4 octets in length and corresponds to the "Authorize reject wait timeout" field of the 802.16 "PKM configuration settings" attribute.

3.4. PKM-Cryptosuite-List

Description

The PKM-Cryptosuite-List Attribute is of type string [RFC2865] and is variable length; it corresponds roughly to the "Cryptographic-Suite-List" 802.16 attribute (see Section 11.19.15 of [IEEE.802.16-2004]), the difference being that the RADIUS Attribute contains only the list of 3-octet cryptographic suite identifiers, omitting the IEEE Type and Length fields.

The PKM-Cryptosuite-List Attribute MAY be present in an Access-Request message. Any message in which the PKM-Cryptosuite-List Attribute is present MUST also contain an instance of the Message-Authenticator Attribute [RFC3579].

Implementation Note

The PKM-Cryptosuite-List Attribute is used as a building block to create the 802.16 "Security-Capabilities" attribute ([IEEE.802.16-2004], Section 11.9.13); since this document only pertains to PKM version 1, the "Version" sub-attribute in that structure MUST be set to 0x01 when the RADIUS client constructs it.

A summary of the PKM-Cryptosuite-List Attribute format is shown below. The fields are transmitted from left to right.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |      Len      |          Value...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

140 for PKM-Cryptosuite-List

Len

2 + 3n < 39, where 'n' is the number of cryptosuite identifiers in the list.

Value

The Value field is variable length and contains a sequence of one or more cryptosuite identifiers, each of which is 3 octets in length and corresponds to the Value field of an IEEE 802.16 Cryptographic-Suite attribute.

3.5. PKM-SAID

Description

The PKM-SAID Attribute is of type string [RFC2865]. It is 4 octets in length and contains a PKM Security Association Identifier ([IEEE.802.16-2004], Section 11.9.7). It MAY be included in an Access-Request message.

A summary of the PKM-SAID Attribute format is shown below. The fields are transmitted from left to right.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |      Len      |             SAID              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

141 for PKM-SAID

Len

4

SAID

The SAID field is two octets in length and corresponds to the Value field of the 802.16 PKM SAID attribute

3.6. PKM-SA-Descriptor

Description

The PKM-SA-Descriptor Attribute is of type string and is 8 octets in length. It contains three fields, described below, which together specify the characteristics of a PKM security association. One or more instances of the PKM-SA-Descriptor Attribute MAY occur in an Access-Accept message.

A summary of the PKM-SA-Descriptor Attribute format is shown below. The fields are transmitted from left to right.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |      Len      |             SAID              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    SA Type    |                  Cryptosuite                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

142 for PKM-SA-Descriptor

Len

8

SAID

The SAID field is two octets in length and contains a PKM SAID (Section 3.5).

SA Type

The SA Type field is one octet in length. The contents correspond to those of the Value field of an IEEE 802.16 SA-Type attribute.

Cryptosuite

The Cryptosuite field is 3 octets in length. The contents correspond to those of the Value field of an IEEE 802.16 Cryptographic-Suite attribute.

3.7. PKM-AUTH-Key

Description

The PKM-AUTH-Key Attribute is of type string, 135 octets in length. It consists of 3 fields, described below, which together specify the characteristics of a PKM authorization key. The PKM-AUTH-Key Attribute MAY occur in an Access-Accept message. Any packet that contains an instance of the PKM-AUTH-Key Attribute MUST also contain an instance of the Message-Authenticator Attribute [RFC3579].

A summary of the PKM-AUTH-Key Attribute format is shown below. The fields are transmitted from left to right.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |      Len      |            Lifetime
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
          Lifetime (cont.)      |    Sequence    |     Key...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

143 for PKM-AUTH-Key

Len

135

Lifetime

The Lifetime field is 4 octets in length and represents the lifetime, in seconds, of the authorization key. For more information, see Section 11.9.4 of [IEEE.802.16-2004].

Sequence

The Sequence field is one octet in length. The contents correspond to those of the Value field of an IEEE 802.16 Key-Sequence-Number attribute (see [IEEE.802.16-2004], Section 11.9.5).

Key

The Key field is 128 octets in length. The contents correspond to those of the Value field of an IEEE 802.16 AUTH-Key attribute. The Key field MUST be encrypted under the public key from the Subscriber Station certificate (Section 3.1) using RSA encryption [RFC2437]; see Section 7.5 of [IEEE.802.16-2004] for further details.

Implementation Note

It is necessary that a plaintext copy of this field be returned in the Access-Accept message; appropriate precautions MUST be taken to ensure the confidentiality of the key.

3.7.1. AUTH-Key Protection

The PKM-AUTH-Key Attribute (Section 3.7) contains the AUTH-Key encrypted with the SS's public key. The BS also needs the AK, so a second copy of the AK needs to be returned in the Access-Accept message.

It is RECOMMENDED that the AK is encapsulated in an instance of the MS-MPPE-Send-Key Attribute [RFC2548]. However, see Section 4.3.4 of RFC 3579 [RFC3579] for details regarding weaknesses in the encryption scheme used.

If better means for protecting the Auth-Key are available (such as RADIUS key attributes with better security properties, or means of protecting the whole Access-Accept message), they SHOULD be used instead of (or in addition to) the MS-MPPE-Send-Key Attribute.

4. Table of Attributes

The following table provides a guide to which attributes may be found in which kinds of packets, and in what quantity.

Request	Accept	Reject	Challenge	Acct-Req	#	Attribute
0+	0	0	0	0	137	PKM-SS-Cert [Note 1]
0+	0	0	0	0	138	PKM-CA-Cert [Note 2]
0	0-1	0	0	0	139	PKM-Config-Settings
0-1	0	0	0	0	140	PKM-Cryptosuite-List
0-1	0	0	0	0	141	PKM-SAID
0	0+	0	0	0	142	PKM-SA-Descriptor
0	0-1	0	0	0	143	PKM-Auth-Key
0	0-1	0	0	0		MS-MPPE-Send-Key [Note 3]

[Note 1]
No more than one Subscriber Station Certificate may be transferred in an Access-Request packet.

[Note 2]
No more than one CA Certificate may be transferred in an Access-Request packet.

[Note 3]
MS-MPPE-Send-Key is one possible attribute that can be used to convey the AK to the BS; other attributes can be used instead (see Section 3.7.1).

The following table defines the meaning of the above table entries.

```
0   This attribute MUST NOT be present in packet
0+  Zero or more instances of this attribute MAY be present in packet
0-1 Zero or one instance of this attribute MAY be present in packet
1   Exactly one instance of this attribute MUST be present in packet
```

5. Diameter Considerations

Since the Attributes defined in this document are allocated from the standard RADIUS type space (see Section 7), no special handling is required by Diameter nodes.

6. Security Considerations

Section 4 of RFC 3579 [RFC3579] discusses vulnerabilities of the RADIUS protocol.

Section 3 of the paper "Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005" [SecEn] discusses the operation and vulnerabilities of the PKMv1 protocol.

If the Access-Request message is not subject to strong integrity protection, an attacker may be able to modify the contents of the PKM-Cryptosuite-List Attribute, weakening 802.16 security or disabling data encryption altogether.

If the Access-Accept message is not subject to strong integrity protection, an attacker may be able to modify the contents of the PKM-Auth-Key Attribute. For example, the Key field could be replaced with a key known to the attacker.

See Section 3.7.1 for security considerations of sending the authorization key to the BS.

7. IANA Considerations

IANA has assigned numbers for the following Attributes:

137 PKM-SS-Cert

138 PKM-CA-Cert

139 PKM-Config-Settings

140 PKM-Cryptosuite-List

141 PKM-SAID

142 PKM-SA-Descriptor

143 PKM-Auth-Key

The Attribute numbers are to be allocated from the standard RADIUS Attribute type space according to the "IETF Review" policy [RFC5226].

8. Contributors

Pasi Eronen provided most of the text in Section 3.7.1.

9. Acknowledgements

Thanks (in no particular order) to Bernard Aboba, Donald Eastlake, Dan Romascanu, Avshalom Houri, Juergen Quittek, Pasi Eronen, and Alan DeKok for their mostly useful reviews of this document.

10. References

10.1. Normative References

[IEEE.802.16-2004]
Institute of Electrical and Electronics Engineers, "IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems", IEEE Standard 802.16, October 2004.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

10.2. Informative References

[RFC2437] Kaliski, B. and J. Staddon, "PKCS #1: RSA Cryptography Specifications Version 2.0", RFC 2437, October 1998.

[RFC2459] Housley, R., Ford, W., Polk, T., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.

[RFC2548] Zorn, G., "Microsoft Vendor-specific RADIUS Attributes", RFC 2548, March 1999.

[SecEn] Altaf, A., Jawad, M., and A. Ahmed, "Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008.

Author's Address

Glen Zorn
Network Zen
1463 East Republican Street
#358
Seattle, WA 98112
US

EMail: gwz@net-zen.net