Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Extended Set of Event Types for EAP-based Authentication - Comment #1064**
Date Submitted	**2006-05-09**
Source(s)	Christian Guenther, Achim.Brandt@siemens.com Achim Brandt Siemens AG
Re:	Contribution on comments to IEEE 802.16g/D2 – including a remedy for comment #1064 submitted by 2006-04-30
Abstract	To align with 802.16e-2005 and to properly support double EAP mode, we propose to extend the set of event types by the entries “Authenticated EAP Start” and “Authenticated EAP Transfer”
Purpose	Alignment with related specifications
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE’s name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE’s sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Extended Set of Event Types for EAP-based Authentication - Comment #1064

Christian Guenther, Achim Brandt
Siemens

Introduction

This contribution proposes an extended set of event types for EAP-based authentication to properly support double-EAP authentication and authorization procedures and to align with corresponding 802.16e messages. Moreover this change in C-SAP primitives is also in correspondence with the backhaul signaling as currently being worked at in the WiMAX industry fora.

Proposed Changes to 802.16g/D2

In the following the proposed changes are shown by revision marks.

14.2.4.1.1 C-SM-NOTFY

This primitive is used by an 802.16 entity or NCMS to notify security procedures. The Event Type included in this primitive defines the type of security operation in Authentication and Re-authentication procedure to be performed. The possible Event Types for this primitive are listed in Table below:

Table 452—C-SM-NOTFY Operation Types

Event Type	Description
EAP Start	EAP Start
Authenticated EAP Start	Authenticated EAP Start
AK Transfer	AK Transfer notification
EAP Transfer	Transfer EAP Payload
Authenticated EAP Transfer	Authenticated EAP Transfer

14.2.4.1.1.1 Function

14.2.4.1.1.1.1 EAP_Start

This primitive informs an AAA Client entity in NCMS that an MS is going to start EAP-based authentication. PKMv2 EAP-Start is sent by MS to initiate either initial EAP authentication or EAP re-authentication exchange. In case of PKMv2 EAP Start initiating initial EAP authentication, the BS shall drop this message and shall not send an EAP Start to the AAA client in NCMS. In case of EAP re-authentication, the BS shall send

EAP-Start to the AAA Client in NCMS only if the PKMv2 EAP-Start message received from the MS is authenticated and protected by a CMAC or HMAC; otherwise, the BS shall drop the PKMv2 EAP Start message.

14.2.4.1.1.1.2 AK Transfer

…

14.2.4.1.1.1.3 EAP Transfer

…

14.2.4.1.1.1.4 Authenticated_EAP_Start

This primitive informs an AAA client in NCMS that a MS is going to start second round EAP during double EAP authentication and authorization.

14.2.4.1.1.1.5 Authenticated_EAP_Transfer

After the C-SM-NOTFY/Authenticated_EAP_Start primitive, EAP payloads are exchanged between an MS and NCMS. The EAP payloads are encapsulated in C-SM-NOTFY/Authenticated_EAP_Transfer because they are not interpreted in the MAC and because they are exchanged during second round EAP in double EAP authentication and authorization. C-SM-NOTFY/Authenticated_EAP_Transfer is used between NCMS and BS.

Reason for the above changes

IEEE 802.16e-2005 has introduced two different types of PKMv2 messages that initiate EAP authentication:

1) PKMv2 EAP Start (see 802.16e-2005, 6.3.2.3.9.15):
   This message is sent from the MS to the BS either in case of initial EAP authentication or in case of EAP re-authentication. In case of initial EAP authentication, this message is unprotected, i.e., it does not contain the attributes “Key Sequence Number” and “HMAC digest/CMAC digest”. In case of EAP re-authentication, it does contain these two attributes, where “Key Sequence Number” is the AK sequence number and “HMAC digest/CMAC digest” is a message digest value calculated using AK.
2) PKMv2 Authenticated EAP Start (see 802.16e-2005, 6.3.2.3.9.28):
   This message is used only in double EAP mode. It is sent from the MS to the BS in order to initiate second round EAP. Besides the attribute “MS_Random”, this message contains the attribute “HMAC digest/CMAC digest” whose value is calculated using EIK which has been derived during first round EAP.

Furthermore, IEEE 802.16e-2005 has introduced two different types of PKMv2 messages that transfer EAP payloads:

1) PKMv2 EAP Transfer (see 802.16e-2005, 6.3.2.3.9.16):

An MS uses this message to send EAP payload received from an EAP method to the BS, and a BS uses this message to send EAP payload received from an EAP method to the MS. In case of EAP re-authentication, this message also contains the attributes “Key Sequence Number” and “HMAC digest/CMAC digest”, which carry the sequence number of AK and the message digest value calculated using AK.

2) PKMv2 Authenticated EAP Transfer (see 802.16e-2005, 6.3.2.3.9.17):
This message is used for authenticated EAP-based authorization, i.e., after establishing an EIK. It then encapsulates EAP payload that the MS or BS has received from an EAP method. It contains the attribute “HMAC digest/CMAC digest” whose value is calculated using EIK.

To align with 802.16e-2005 and to properly support double EAP mode, we propose to extend the set of event types by the entries “Authenticated EAP Start” and “Authenticated EAP Transfer” as shown in the table above. Then, there are the following equivalences:

802.16e PKMv2 message	802.16g Event Type
PKMv2 EAP Start	EAP Start
PKMv2 Authenticated EAP Start	Authenticated EAP Start
PKMv2 EAP Transfer	EAP Transfer
PKMv2 Authenticated EAP Transfer	Authenticated EAP Transfer

Motivation for changes to section 14.2.4.1.1.1.1: EAP_Start

The forwarding of unprotected EAP-Start messages to the AAA client in the NCMS can be considered a security risk. Moreover, it is not required since the NCMS can be informed of the successful network entry of a MS by other messages. Therefore, it is recommended that the BS drops *all* unprotected PKMv2 EAP Start messages received from a MS. This is, the BS drops each PKMv2 EAP Start message initiating *initial* EAP authentication (of course, these messages are unprotected since there is no AK or EIK available to protect them), and furthermore, the BS also drops each PKMv2 EAP Start message that initiates EAP re-authentication and that is not protected by a “HMAC digest/CMAC digest” attribute.

It is proposed to align 802.16g with 802.16e and to support Event Type “EAP Start” only in case of EAP re-authentication (i.e., the BS drops each unprotected PKMv2 EAP Start message). This is the purpose of the changes shown for sections 14.2.4.1.1.1 above.

Corresponding changes to sections 14.2.4.1.1.2, 14.2.4.1.1.3, 14.2.4.1.1.4:

For the two new Event Types, “Authenticated EAP Start” and “Authenticated EAP Transfer”, additional text will also be required in sections
14.2.4.1.1.2 Semantics of the Service Primitives
14.2.4.1.1.3 When generated
14.2.4.1.1.4 Effect of receipt

This will have to be added once the above changes are agreed in principle.