Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Extended Set of Event Types for EAP-based Authentication – "Semantics", "When generated" and "Effects"**
Date Submitted	2006-07-07
Source(s)	Christian Guenther, Achim Brandt Siemens AG Achim.Brandt@siemens.com
Re:	Contribution on comments to IEEE 802.16g/D3
Abstract	For the recently adopted, new event types "Authenticated EAP Start" and "Authenticated EAP Transfer", the missing contents of the sections "Semantics", "When generated", and "Effect of receipt" is provided.
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 - “Semantics”, “When generated” and “Effects”

Christian Guenther, Achim Brandt
Siemens

Introduction

Contribution C802.16g-06/033, accepted at LB#20a, introduced the “Authenticated EAP Start” and “Authenticated EAP Transfer” event types to properly support double EAP authentication and authorization procedures and to align with corresponding 802.16e messages. This contribution provides the missing paragraphs of the corresponding sections “Semantics of the service primitives”, “When generated” and “Effect of receipt”.

Proposed Changes to 802.16g/D3

Change #1: Insert paragraphs 14.2.4.1.1.2.4 and 14.2.4.1.1.2.5 into 14.2.4.1.1.2:

14.2.4.1.1.2 Semantics of the service primitives

14.2.4.1.1.2.1. EAP_Start

…

14.2.4.1.1.2.2. AK Transfer

…

14.2.4.1.1.2.3. EAP_Transfer

…

14.2.4.1.1.2.4 Authenticated EAP Start

The parameters of this primitive are as follows:

```
C-SM-NOTFY
        (
        Message_id,
        Event Type: Authenticated_EAP_Start,
        Object ID: NCMS,
        Attribute List:
                MS ID,
```

BS ID

)

MS ID

48-bit unique identifier used for mobile station identification between BS and NCMS

BS ID

48-bit unique identifier for BS

14.2.4.1.1.2.5 Authenticated EAP Transfer

The parameters of this primitive are as follows:

C-SM-NOTFY

(

Message_id,

Event Type: Authenticated_EAP_Transfer,

Object ID: BS_ID or NCMS,

Attribute List:

MS ID,

EAP Payload

)

MS ID

48-bit unique identifier used for mobile station identification between BS and NCMS

EAP Payload

Contains the EAP authentication data.

Change #2: Insert new paragraphs 14.2.4.1.1.3.4 and 14.2.4.1.1.3.5 into 14.2.4.1.1.3:

14.2.4.1.1.3 When generated

14.2.4.1.1.3.1 EAP_Start

…

14.2.4.1.1.3.2 AK Transfer

…

14.2.4.1.1.3.3 EAP Transfer

…

14.2.4.1.1.3.4 Authenticated_EAP_Start

The BS shall send a notification message with this event type to the NCMS whenever it received from the MS a PKMv2 Authenticated EAP Start message, equipped with a valid “HMAC digest/CMAC digest” attribute value.

14.2.4.1.1.3.5 Authenticated_EAP_Transfer

The BS shall send a notification message with this event type to the NCMS whenever it received from the MS a PKMv2 Authenticated EAP Transfer message, equipped with a valid “HMAC digest/CMAC digest” attribute value. This way, the BS shall relay the EAP payload contained in the PKMv2 Authenticated EAP Transfer message to the NCMS.

The NCMS shall send a notification message with this event type to the BS in order to response to an Authenticated_EAP_Transfer primitive received from the BS.

Change #3: Insert new paragraphs 14.2.4.1.1.4.4 and 14.2.4.1.1.4.5 into 14.2.4.1.1.4:

14.2.4.1.1.4 Effect of Receipt

14.2.4.1.1.4.1 EAP_Start

…

14.2.4.1.1.4.2 AK Transfer

…

14.2.4.1.1.4.3 EAP Transfer

…

14.2.4.1.1.4.4 Authenticated_EAP_Start

Reception of an Authenticated_EAP_Start primitive from the BS informs the NCMS of the MS having initiated second round EAP by means of a PKMv2 Authenticated EAP Start message with a valid “HMAC digest/CMAC digest” attribute value. This triggers the NCMS to send Authenticated EAP Transfer primitives to the BS carrying EAP payloads for second round EAP.

14.2.4.1.1.4.5 Authenticated_EAP_Transfer

When received by BS: When the BS receives a Authenticated_EAP_Transfer primitive from NCMS, it generates a PKMv2 Authenticated EAP Transfer message carrying the EAP contained in the primitive to the MS.

When received by NCMS: When the NCMS receives an Authenticated_EAP_Transfer primitive, it generates either a response primitive of the same type and sends it to the BS, or – after successful completion of the second EAP round – derives PMK2 from MSK2, then AK from PKM and PMK2, and an AK context.

[End of changes]

Reason for the above changes

Regarding the “Authenticated EAP Start” and “Authenticated EAP Transfer”, the corresponding paragraphs of the sections “Semantics of the service primitives”, “When generated” and “Effect of receipt” have been missing.

Remark

In order to enable the BS to validate “HMAC digest/CMAC digest” attribute values attached to second round PKMv2 EAP messages received from the MS, the NCMS must provide the BS with the EIK value. Currently, this is still missing in 802.16g/D3.