Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**EAP-based Authentication Procedure and Primitives**
Date Submitted	**2005-07-12**

Source(s)	Mi Young Yun	myyun@etri.re.kr
	Jung Mo Moon, PhD	jmmoon@etri.re.kr
	Sang Ho Lee, PhD	leesh@etri.re.kr
	ETRI	
	161, Gajeong-dong,Yuseong-gu,	Voice: 82-42-860-4821
	Daejeon, 305-700, Korea	Fax: 82-42-861-1966

Re:	Contribution on comments to IEEE 802.16g-04/03r3
Abstract	In this contribution, we describe the EAP authentication procedure and service primitives that could be exchanged between the BS and the NCMS entities.
Purpose	Adoption
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 text 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 (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing 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:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

EAP-based Authentication Procedure and Primitives

Mi Young Yun, Jung Mo Moon and Sang Ho Lee

ETRI

1. Problem Statement

The purpose is to describe the EAP-based authentication procedure and service primitives that could be exchanged between the BS and the NCMS entities. This proposal makes it possible to perform the authentication as specified in the remainder of this document.

2. Summary of the Proposed Remedy

In this contribution, we define 3 primitives to support service flow management between BS and access network (NCMS) which are described briefly in the following table.

Primitive	Direction	Primitive Contents
EAP_Start.request	BS -> NCMS	MS ID
EAP_Transfer	BS <-> NCMS	MS ID, EAP Payload
EAP_Key_Notification.indication	BS <- NCMS	MS ID, MSK, MSK Lifetime

Figure1 shows the EAP-based authentication procedure using Diameter protocols.

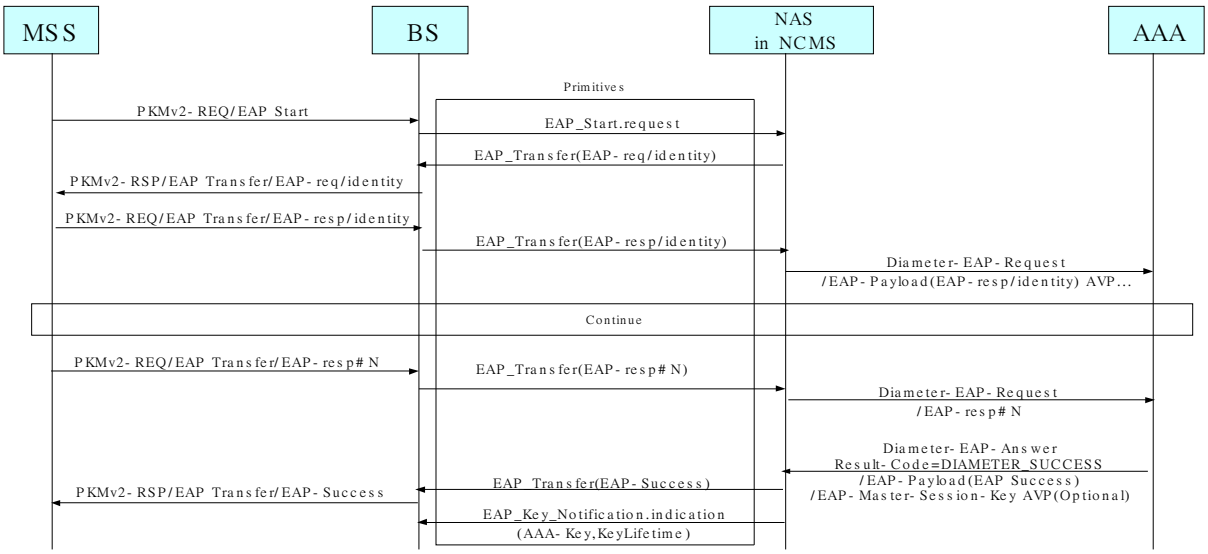

Figure 1. EAP-based authentication procedure using Diameter protocols[1][2]

3. Proposed Text Changes

[*Insert section 14.5.5.5 as follow*]
14.5.5 Security Management

14.5.5.5 EAP-based authentication procedure

When an MS try to initiate an EAP-based authentication or re-authentication procedure with a BS, it sends a PKMv2 EAP Start message. The BS informs of an NAS (Network Access Server) entity in NCMS as an EAP_start.request primitive. If the MS receives EAP-Request/Identity messages, then it sends the EAP-Response/Identity message with MN's identifier to the NAS entity. After the EAP-Response/Identity message, the EAP methods are negotiated between the MS and the AAA server and the EAP messages are exchanged several times. The EAP messages encapsulated are exchanged between the MS and the NAS entity. If the EAP authentication procedure is finished successfully and also yields an MSK (Master Session Key), the BS which does not know EAP protocols receives the MSK and a key lifetime from the EAP client entity as an EAP_Key_Notification.indication primitive. It is already shared between the AAA server and the MS through the EAP exchanges. The MSK is used for derivation for a PMK (Pair wise Master Key) and optional EIK (EAP Integrity Key). Figure 1 shows EAP-based authentication procedure between a BS and an NAS entity in NCMS as follows
.

Figure 1. EAP-based authentication procedure

14.5.5.5.1 Service Primitives

14.5.5.5.1.1EAP_Start.request

14.5.5.5.1.1.2 Function
This primitive inform an AAA Client entity in NCMS that an MS is going to start EAP-based authentication.

14.5.5.5.1.1.2 Semantics of the Service Primitives
The parameters of the primitives are as follows:
EAP_Start.request

{
MS ID
}

MS ID
48-bit unique identifier used for user identification between BS and NCMS

14.5.5.5.1.1.3 When generated
This primitive is issued by a BS when a MS wants to initiate EAP-based authentication procedure.

14.5.5.5.1.1.4 Effect of receipt
EAP payloads are forwarded for the authentication between BS and NCMS entity.

14.5.5.5.1.2 EAP_Transfer

14.5.5.5.1.2.1 Function
After the EAP_start primitive, EAP payloads are exchanged between an MS and an NAS entity. The EAP payloads are encapsulated in the EAP Transfer because it is not interpreted in the MAC.

14.5.5.5.1.2.2 Semantics of the Service Primitives
The parameters of the primitives are as follows:

EAP_Transfer
{
MS ID
EAP Payload
}

MS ID
48-bit unique identifier used for user identification between BS and NCMS
EAP Payload
Contains the EAP authentication data

14.5.5.5.1.3 EAP_Key_Notification.indication

14.5.5.5.1.3.1 Function
A MS derives the key from the EAP payloads and the NCMS entity informs the BS of it when the EAP exchanges are successfully completed and yield the MSK.

14.5.5.5.1.3.2 Semantics of the Service Primitives
The parameters of the primitives are as follows:

EAP_Key_Notification.indication
{
MS ID
MSK
MSK Lifetime
}

MS ID

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

MSK

MSK is the product of EAP exchanges. It is used for the derivation of PMK (Pair wise Master Key) and EIK.

MSK Lifetime

It may be transferred from the EAP method or may be set by a vendor.

14.5.5.5.1.3.3 When generated

This primitive is issued by a NCMS (a NAS entity) when the EAP exchange are successfully completed and yield the MSK.

14.5.5.5.1.3.4 Effect of receipt

The BS could derive a PMK and optional EIK from the MSK.

References

[1] P. Eronen, et. al., "Diameter Extensible Authentication Protocol (EAP) Application," draft-ietf-aaa-eap-10, November 2004.
[2] B. Aboba, et. al., "Extensible Authentication Protocol (EAP)," RFC 3748, June 2004.
[3] IEEE-Std 802.16-2004
[4] IEEE P802.16e/D9