Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Notification of Completion for EAP-based Authorization Procedure**
Data Submitted	**2005-06-08**

Source(s)	Seokheon Cho Sungcheol Chang Chulsik Yoon ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr

Re:	IEEE P802.16e/D8

Abstract	The existing EAP-based authorization flow has two kinds of messages; PKMv2 EAP Start message and PKMv2 EAP Transfer message, in order to notify start of EAP-based authorization procedure and transfer EAP payload to each other node. This contribution provides a resolution for notifying completeness of EAP-based authorization procedure.

Purpose	Adoption of proposed changes into P802.16e/D8

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:chiar@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>.

Notification of Completion for the EAP-based Authorization Procedure

Seokheon Cho, Sungcheol Chang, and Chulsik Yoon

ETRI

Introduction

The PKMv2 supports the EAP-based authorization procedure.

0.1 IEEE P802.16e/D8 Status

The EAP-based authorization procedure constitutes two messages; PKMv2 EAP Start message and PKMv2 EAP Transfer message. An MS sends a PKMv2 EAP Start message to initiate device authorization and user authorization achieved from the upper EAP authentication layer such as EAP-TLS or EAP-TTLS. When an MS's MAC or a BS's MAC receives EAP-payload from an EAP method, an MS or a BS sends a PKMv2 EAP Transfer message for transmitting EAP-payload to one another.

0.2 Problems

There are several problems in the existing EAP-based authorization procedure.

The BS doesn't know the completion time of the EAP-based authorization procedure in case that EAP protocol doesn't yield AAA-key.

In addition, the BS doesn't know whether an MS receives the last PKMv2 EAP Transfer message (including AAA-key, such as "EAP Success" used in EAP-TLS) or not. Both the BS and an MS cannot share the AK derived from PMK simultaneously, when an MS doesn't receive the last PKMv2 EAP Transfer message. Even though an MS receives the last PKMv2 EAP Transfer message, there may be possibility of an MS's MAC receiving the PKMv2 SA-TEK-Challenge message from the BS before getting the AAA-key from MS's EAP method layer, because the BS can almost simultaneously send the last PKMv2 EAP Transfer message and PKMv2 SA-TEK-Challenge message. The existing EAP-based authorization procedure is shown in Fig 0.1.

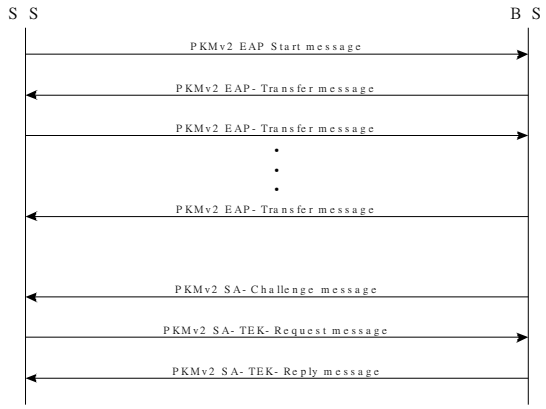

Figure 1 Existing EAP-based authorization procedure

Therefore, it is necessary that an MS notifies the completion of the EAP-based authorization procedure to the BS.

0.3 Solutions

We provide a new PKMv2 EAP Transfer Complete message to notify that an MS receives the last PKMv2 EAP Transfer message. An MS will send a PKMv2 EAP Transfer Complete message to the BS. As soon as the BS receives this message, the BS will send a PKMv2 SA-TEK-Challenge message to an MS.

Proposed Changes into IEEE P802.16e/D8

[Change the Table 26 in sub-clause 6.3.2.3.9:]

6.3.2.3.9 Privacy key management (PKM) message (PKM-REQ/PKM-RSP)

Code	PKM message type	MAC Management message name
		… **All contexts to here will be maintained in this table.**
29	~~EAP Start~~ PKMv2 EAP Transfer Complete-	PKM-REQ
30-255	reserved	

[Insert the following sub-clause in 6.3.2.3.9:]

6.3.2.3.9.27 PKMv2 EAP Transfer-Complete message

An MS sends the PKMv2 EAP-Transfer-Complete message to the BS to report the completion of the EAP-based authorization procedure, as soon as the MS receives the last PKMv2 EAP-Transfer message or the last PKMv2 Authenticated EAP-Transfer message.

Code: 29

This message has no attribute.