Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Corrections for the Protocol Stack of Security Layer**
Data Submitted	**2005-05-04**
Source(s)	Seokheon Cho Taeyong Lee Jaesun Cha Chulsik Yoon ETRI Yong Chang SAMSUNG Yongjoo Tcha KT Li Rui, Tian Feng ZTE corporation Yigal Eliaspur Intel Corp.	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr 161, Gajeong-dong,Yuseong-Gu, Daejeon, 305-350, Korea
Re:	IEEE P802.16e/D7
Abstract	The document contains suggestions on the changes into IEEE 802.16e/D7 that would correct the protocol stack of security layer.
Purpose	Adoption of proposed changes into P802.16e/D7
Notice	
Release	
Patent Policy and Procedures	

Corrections for the Protocol Stack of Security Layer

Seokheon Cho, Taeyong Lee, Jaesun Cha, and Chulsik Yoon
ETRI

Jicheol Lee and Yong Chang
SAMSUNG

Yongjoo Tcha
KT

Li Rui and Tian Feng
ZTE corporation

Yigal Eliaspur
Intel Corp.

Introduction

The protocol stack for the security components of the system is defined in the P802.16/D7.

However, the protocol stack doesn't fully support all security sub-functions; it skips some important security components and is wrong-arranged.

The new following security components need to be considered, compared to the existing security protocol stack (Figure 130j and Figure 130k).
- Traffic Data Encryption/Authentication Processing: Stack for processing the traffic data encryption/decryption and authentication as data plane
- Message Authentication Processing: Stack for executing message authentication function as control plane, e.g., HMAC or OMAC
- PKM Control Management: Stack for entirely managing the PKM version 1 and the PKM version 2, and controlling all security components
- Authorization Control: Stack for controlling the authorization key state machine
- SA Control: Stack for controlling multiple traffic encryption key state machines

The following security components, which are defined in the P802.16/D7, are needed to be clearly arranged in the security protocol stack.
- Control Message Processing: Stack for processing the PKM-related MAC messages. Since the general MAC messages (e.g., DSA-REQ, DSA-RSP, and so on) are made in the MAC CPS layer, it is reasonable that the function for processing PKM-related MAC message should be executed in the PKM CPS layer.

Proposed changes to IEEE 802.16e/D7

7.1 Architecture
[Exchange Figure 130j for the following new Figure and Add contents below Figure 130j as follows:]
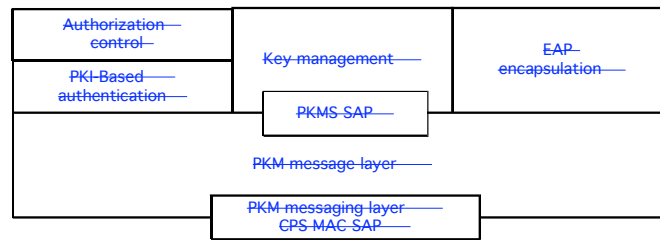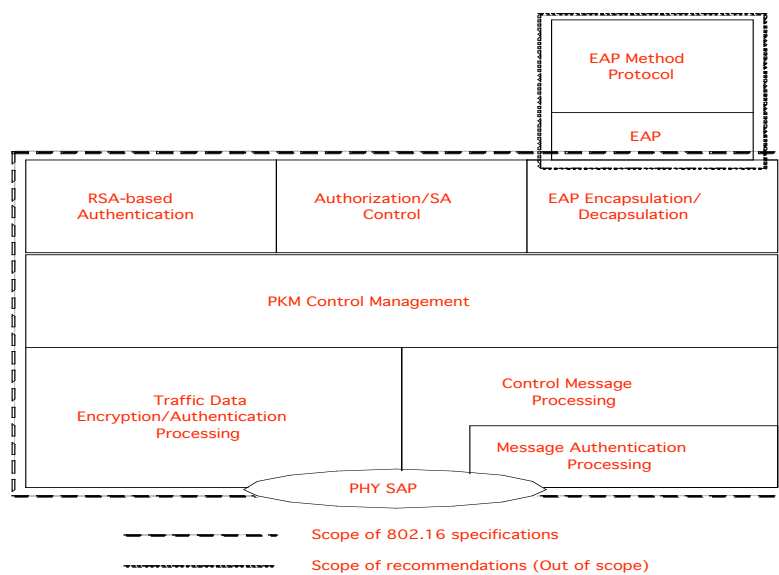

Figure 130j-Security sublayer

Figure 130j-Security sublayer

7.1.3.2 PKM EAP authentication
[Modify the sub-clause 7.1.3.2 as follows:] and *[Delete Figure 130k]*

PKM EAP Authentication uses Extensible Authentication Protocol [IETF RFC 3748] in conjunction with a vendor-selected standardized EAP Method (eg. EAP-TLS [IETF RFC 2716]). The EAP method will use a particular kind of credential – such as an x.509 certificate in the case of EAP-TLS, or a Subscriber Identity Module in the case of EAP-SIM.

The particular credentials and EAP methods that are to be used are outside of the scope of this specification, but they should be selected with awareness of the security issues described in [IETF RFC 3748] section 7.

Figure 130k shows the relationship between the lower levels of the 802.16 MAC and the generic EAP components (and the interface between them).
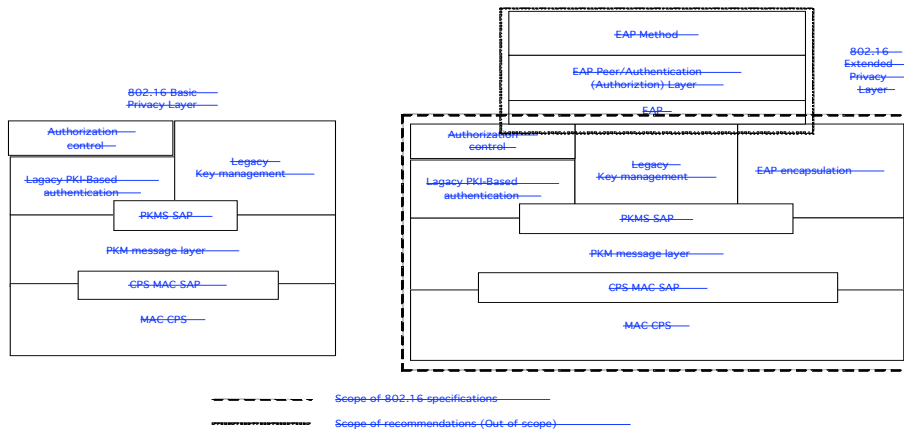
Figure 130k Comparison of the Basic and Extended

Privacy Layers (Control plane)