Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	Enhancement of MSS and BS mutual authorization for PKMV2
Date Submitted	**2004-12-28**
Source(s)	[Rui Li] [Feng Tian] [JianYong Chen] [zte] [ZTE Plaza , Keji Road South , Hi-tech Industrial Park , Nanshan District , Shenzhen , P.R.China , 518057] Voice: [86-0755-26772016] Fax: [86-0755-26772004] [mailto:li.rui2@zte.com.cn]
Re:	802.16e/D5
Abstract	This supplementary contents for MSS and BS mutual authorization in PKMv2
Purpose	The document is submitted for review by 802.16 Working Group members
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>.

Enhancement of MSS and BS mutual authorization for PKMv2

Rui Li
Feng tian
JianYong Chen

1. Introduction

PKMv2 Authorization mechanism supports MSS and BS mutual authorization in 802.16/D5. The PKMv2 authorization request message and reply message are defined in the sixth section. But the description about mutual authorization for PKMv2 in the seventh section is not detailed.

In this contribution, we suggest some contents needed to be supplemented so that the description about MSS and BS mutual authorization for PKMv2 can be fully understood.

2. Proposed changes

7.8.2.2 MSS and BS mutual authorization and AK exchange overview

MSS mutual authorization, controlled by the PKMv2 Authorization state machine, is the process of

a) The BS authenticating a client MSS's identity
b) The MSS authenticating the BS's identity
c) The BS providing the authenticated MSS with an AK, from which a key encryption key (KEK) and message authentication keys are derived
d) The BS providing the authenticated MSS with the identities (i.e., the SAIDs) and properties of primary and static SAs the MSS is authorized to obtain keying information for.

After achieving initial authorization, an MSS periodically seeks reauthorization with the BS; reauthorization is also managed by the MSS's PKMv2 Authorization state machine. An MSS must maintain its authorization status with the BS in order to be able to refresh aging TEKs and GTEKs. TEK state machines manage the refreshing of TEKs.

The MSS sends an Authorization Request message to its BS immediately after sending the Authentication Information message. This is a request for an AK, as well as for the SAIDs identifying any Static Security SAs the MSS is authorized to participate in. The Authorization Request includes (see 6.3.2.3.9.19)

a) a manufacturer-issued X.509 certificate
b) a description of the cryptographic algorithms the requesting MSS supports; an MSS's cryptographic capabilities are presented to the BS as a list of cryptographic suite identifiers, each indicating a particular pairing of packet data encryption and packet data authentication algorithms the MSS supports
c) the MSS's Basic CID. The Basic CID is the first static CID the BS assigns to an MSS during initial ranging—the primary SAID is equal to the Basic CID
d) A 64-bit random number generated in the MSS

In response to an Authorization Request message, a BS validates the requesting MSS's identity, determines the encryption algorithm and protocol support it shares with the MSS, activates an AK for the MSS, encrypts it with the MSS's public key, and sends it back to the MSS in an Authorization Reply message. Random numbers are included in the exchange to ensure liveness. The Authorization Reply includes (see 6.3.2.3.9.20)

a) the BS's X.509 certificate, used to verify the BS's identity
b) the MSS's X.509 certificate, used to verify the MSS's identity

c) an AK encrypted with the MSS's public key
d) a 8-bit key sequence number, used to distinguish between successive generations of AKs
e) a key lifetime
f) the identities (i.e., the SAIDs) and properties of the single primary and zero or more static SAs the MSS is authorized to obtain keying information for
g) the 64-bit random number generated in the MSS
h) a 64-bit random number generated in the BS, used to ensure key of liveness along with the random number of MSS
i) the RSA signature over all the other attributes in the auth-reply message by BS, used to assure the reality of two PKMv2 authorization messages.

An MSS shall periodically refresh its AK by reissuing an Authorization Request to the BS. Reauthorization is identical to authorization. To avoid service interruptions during reauthorization, successive generations of the MSS's AKs have overlapping lifetimes. Both MSS and BS shall be able to support up to two simultaneously active AKs during these transition periods. The operation of the Authorization state machine's Authorization Request scheduling algorithm, combined with the BS's regimen for updating and using a client MSS's AKs (see 7.4), ensures that the MSS can refresh TEK keying information without interruption over the course of the MSS's reauthorization periods.