Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Mutual Authorization for PKMv2**
Date Submitted	**2004-6-26**
Source(s)	David Johnston Intel Corporation 2111 NE 25th Ave. Hillsboro 97124 Voice: +1 (503) 264-3855 [mailto:dj.johnston@intel.com]
Re:	IEEE 802.16e Security Adhoc
Abstract	Proposal to introduce an RSA based mutual authorization for PKMv2
Purpose	To create an authorization procedure in PKMv2, similar in style to PKMv2, but secure.
Notice	
Release	
Patent Policy and Procedures	

Mutual Authorization for PKMv2

David Johnston
Jesse Walker

The PKMv1 authorization procedure is insecure. To render a secure variant, mutuality and liveness assurance are required. Also, binding to a names security session is required. For this, the AA (Authorized Association) and its AAID is used.

The mutual certificate exchange in PKMv2 substitutes for the authorization exchange in PKMv2. It is defined as follows:

auth_req: SS → BS: SS-Random | Cert(SS) | Capabilities | Basic CID
auth_reply: BS → SS: SS-Random | BS-Random | RSA-OAEP-Encrypt(PubKey(SS), pre-PAK | Id(SS))| Lifetime | SeqNo | SAIDList | AAID | Cert(BS) | Sig(BS)
auth_ack: SS → BS: BS-Random | SS_MAC_Address | OMAC(Auth-Key, BS_Random | SS_MAC_Address)

Where
Auth-Key = Dot16KDF(pre-PAK, 0x00 | SS-MAC-Addr | BS-MAC-Addr | AAID, 128)
Id(SS) = the SS's identifier from Cert(SS).

The PAK that is yielded by the authorization exchange is computed thusly:
PAK = kdf(pre-PAK, counter | SS-MAC-Addr | BS-MAC-Addr | AAID | 256)

In addition an SS certificate must be defined.

Editor Instructions:
[In the authorization section of PKMv2 in clause 7, insert]

7.x.x.x SS and BS Mutual Authorization and AK Exchange Overview
SS mutual authorization, controlled by the PKMv2 Authorization state machine, is the process of

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

After achieving initial authorization, an SS periodically seeks reauthorization with the BS; reauthorization is also managed by the SS's PKMv2 Authorization state machine. An SS 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 SS 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 SS is authorized to participate in. The Authorization Request includes
a) a manufacturer-issued X.509 certificate
b) a description of the cryptographic algorithms the requesting SS supports; an SS'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 SS supports
c) the SS's Basic CID. The Basic CID is the first static CID the BS assigns to an SS during initial ranging—the primary SAID is equal to the Basic CID

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

An SS 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 SS's AKs have overlapping lifetimes. Both SS 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 SS's AKs (see 7.4), ensures that the SS can refresh TEK keying information without interruption over the course of the SS's reauthorization periods.

[In the clause 6, 6.3.2.3.9.x insert the PKMv2 auth req/reply/ack messages:]

6.3.2.3.9.x PKMv2 Authorization Request (Auth Request) message

Code: x
Attributes are shown in Table xx.

Table xx.

Attribute	Contents
SS_Random	A 64 bit random number generated in the SS
SS_Certificate	Contains the SS's X.509 user certificate
Security_Capabilities	Describes requesting SS's security capabilities
AAID/SAID	Either the AAID or the Basic CID if in initial network entry

The SS-certificate attribute contains an X.509 SS certificate (see 7.6) issued by the SS's manufacturer. The SS's X.509 certificate and Security Capabilities attribute is as defined in 6.3.2.3.9.2.

6.3.2.3.9.x+1 PKMv2 Authorization Request (Auth Reply) message

Code: x

Sent by the BS to a client SS in response to an Authorization Request, the Authorization Reply message contains an AK, the key's lifetime, the key's sequence number, and a list of SA-Descriptors identifying the Primary and Static SAs the requesting SS is authorized to access and their particular properties (e.g., type, cryptographic suite). The AK shall be encrypted with the SS's public key. The SA-Descriptor list shall include a descriptor for the Basic CID reported to the BS in the corresponding Auth Request. The SS_Random number is returned from the auth-req message, along with a BS random number, thus enabling assurance of key liveness.

Attributes are shown in Table xx.

Table xx.

Attribute	Contents
SS_Random	A 64 bit random number received in auth request
BS_Random	A 64 bit random number generated in the BS
SS_Certificate	Contains the SS's X.509 user certificate
EncryptedAK	RSA-OAEP-Encrypt(PubKey(SS), pre-PAK | Id(SS))
AK Lifetime	AK Aging timer
AK Sequence Number	64 bit AK sequence number
AAID/SAID	Either the AAID or the Basic CID if in initial network entry
CertBS	The BS Certificate
SigBS	An RSA signature over all the other attributes in the message