Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Mutual Authorization for PKMv2**
Date Submitted	**2004-07-07**
Source(s)	David Johnston Intel Corporation 2111 NE 25th Ave. Hillsboro 97124 Voice: +1 (503)264-3855 [mailto:dj.Johnston@intel.com]
Re:	Re: Security Adhoc PKMv2
Abstract	Proposal to introduce mutual authorization for PKMv2
Purpose	Discuss and Adopt as the baseline text
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>.

Mutual Authorization for PKMv2

David Johnston, Intel; Jesse Walker, Intel; JunHyuk Song, Samsung; YoungMan Park, KT; Seong-Choon Lee, KT

Version 1 of PKM defined only a one way SS authorization procedure. This procedure is insecure and renders the SS vulnerable to MITM attacks and rogue networks. To render a secure variant, mutuality and liveness assurance are required. Also, binding to a named security session is required. For this, an AA (Authorization Association) is defined along with an AAID (Authorized Association ID) to identify it.

The mutual certificate exchange in PKMv2 substitutes for the authorization exchanges in PKMv1. It is defined as follows:

auth_req: SS -> BS: SS-Random | Cert(SS) | Capabilites | Basic CID
auth_reply: BS -> SS: SS-Random | BS-Random | RSA-OAEP-Encrypt(PubKey(SS),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)

The PAK (Primary Authorization Key) is generated as a cryptographically strong random number in the BS and transmitted to the SS, encrypted with RSA during the above PKMv2 mutual authorization exchange.

The following are defined in this proposal:

- The auth-req/rsp/ack messages
- A BS certificate

[In the clause 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 certificates
Security Capabilities	Describes requesting SS's security capabilities
SAID	SS's primary SAID equal to the Basic CID

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 6.3.2.3.9.2

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

Code: X+1

Sent by the BS to a client SS in response to an PKMv2 Authorization Request. The Authorization Reply message contains SS_RANDOM, BS_RANDOM, SS Certificate, PAK, PAK Lifetime, PAK Sequence Number, AA-Descriptor, SA-Descriptor, BS Certificate, and SigBS.

The PAK shall be encrypted with the SS's public key. The AA-Descriptor shall contain AAID assigned by BS, while SA-Descriptor list shall include a descriptor for the Basic CID reported to the BS in the corresponding Auth Request. The SA Descriptor list may include descriptors of Static SAIDs that the SS is authorized to access.

SS certificate and BS certificate contains X.509 certificate shall be used for mutual authorization. SigBS shall contain signature over all other attribute of PKMv2 Authorization Reply message according to RSA signature algorithm defined in PKCS #1.

Table xx+1

Attribute	Contents
SS_RANDOM	A 64 bit random number generated in the SS
BS_RANDOM	A 64 bit random number generated in the BS
SS Certificate	Contains the SS's X.509 user certificate
PAK	Primary Authorization Key, encrypted with the target client SS's public Key
Key Lifetime	PAK aging timer
PAK Sequence Number	64bit PAK Sequence number
AA-Descriptor	AA-Descriptor attribute specifies an AAID and its type
(one or more) SA-Descriptor(s)	Each compound SA-Descriptor attribute specifies an SAID and additional properties of the SA.
BS Certificate	Contains the BS's X.509 certificate
SigBS	An RSA signature over all other attributes in the message

6.3.2.3.9.x+2 PKMv2 Authorization Acknowledgement (Auth Ack) message

Code: X+2
Sent by the SS to BS as an acknowledgement of successful BS Authorization.

Table xx+2

Attribute	Contents
BS_RANDOM	A 64 bit random number generated in the BS
SS_MAC_Address	Contains the SS's X.509 user certificates
OMAC Tuple	OMAC Digest

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

7.x.x.x SS and BS Mutual Authorization and PAK 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 a PAK, from which an Authorization key (AK), Key Encryption Key (KEK) and message authentication keys are derived

d) The BS providing the authenticated SS with identities (i.e., the AAID and SAIDs) and properties of Authorization Association (AA), primary and static SAs the SS is authorized to obtain keying information for.
e) The SS acknowledging authenticated BS by providing MSS identity (SS MAC Address)

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

The SS sends an Authorization Request message to its BS immediately after sending the Authentication Information message. This is a request for a PAK, as well as for the Authorization Association information, Security Associations Information such as SAIDs identifying an Static Security SAs the SS is authorized to participate in. Authorization Request includes

a) a 64 bits random number generated by the SS
b) a manufacturer-issued X.509 certificate
c) 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
d) the SS's Basic CID. The Basic CID is the first 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 a PAK for the SS, encrypts it with the SS's public key, and sends it back to the SS with BS authorization information such as SS_RANDOM, BS_RANDOM, and BS certificate in an Authorization Reply message.
The PKMv2 authorization reply includes:

a) a 64 bits random number received in auth request
b) a 64 bits random number generated in the BS
c) an PAK encrypted with the SS's public key
d) a 64-bit PAK sequence number, used to distinguish between successive generations of PAKs
e) a PAK lifetime
f) Authorization Association ID
g) the identities (i.e., the SAIDs) and properties of the single primary and zero or more static SAs the SS is authorized to obtain keying information for
h) BS certificate
i) BS signature over all attributes

The BS, in responding to an SS's Authorization Request, shall determine whether the requesting SS, whose identity can be verified via the X.509 digital certificate, is authorized for basic unicast services, Group Service, and what additional statically provisioned services (i.e., Static SAIDs) the SS's user has subscribed for. Note that the protected services a BS makes available to a client SS can depend upon the particular cryptographic suites SS and BS share support for. The Authorization Reply shall identify Static SAs in addition to the Primary SA whose SAID matches the requesting SS's Basic CID, the Authorization Reply shall not identify any Dynamic SAs.

In response to an PKMv2 Authorization reply message, a SS shall validates the replying BS's identity by X.509 digital certificate, and authenticating the message by running hash function defined in RSA hash function with BS's private key. SS may acknowledge Authorization Reply by sending Authorization Acknowledgement or Authorization Reject
The PKMv2 authorization acknowledge includes:

a) a 64 bits random number received in auth reply
b) SS MAC address
c) OMAC Digest

The BS shall determine successful mutual authorization upon receiving PKMv2 Authorization acknowledgement message. If the PKMv2 Auth Ack, Auth Reject, or further PKM message such as EAP or KEY Request message is not received during certain time skew, BS may remove authorization state according to the operator policy

An SS shall periodically refresh its PAK by reissuing an Authorization Request to the BS. Reauthorization is identical to authorization with the exception that the SS does not send Authentication Information messages during reauthorization cycles. Subclause 7.x.x's description of the authorization state machine clearly indicates when Authentication Information messages are sent.

7.x PKMv2 Authorization state machine

TBD – We need to see the full message sequence before this state machine can be defined

7.x PKMv2 BS Certificate Profile

TBD

[Modify Table 368 as follows:]

Table 368—PKM attribute types

Type	PKM Attribute
0-5	*reserved*
6	Display-String
7	AUTH-Key
8	TEK
9	Key-Lifetime
10	Key-Sequence-Number
11	HMAC-Digest
12	SAID
13	TEK-Parameters
14	reserved
15	CBC-IV
16	Error-Code
17	CA-Certificate
18	SS-Certificate
19	Security-Capabilitie
20	Cryptographic-Suite
21	Cryptographic-Suite-List
22	Version
23	SA-Descriptor
24	SA-Type
25	AA-Descriptor
26	AA-Type
27	PKM Configuration Settings
28	SS_RANDOM
29	BS_RANDOM
30	PAK
31	PAK/AK Sequence Number
32	BS-Certificate
33	SigBS
34	SS-MAC Address
35	OMAC-Digest
36-255	reserved

[Add 11.9.21 as follows:]

11.9.21 SS_RANDOM

Description: This attribute contains a quantity that is pseudo random number generated from SS and used as fresh for mutual authorization message handshake.

Type	Length	Value
28	8	SS generated random number

[Add 11.9.21 as follows:]

11.9.21 BS_RANDOM

Description: This attribute contains a quantity that is pseudo random number generated from BS and used as fresh for mutual authorization message handshake.

Type	Length	Value
29	8	BS generated random number

[Add 11.9.22 as follows:]

11.9.22 PAK

Description: This PAK (Primary Authorization Key) is 16byte quantity, from which a AK, KEK, two MAC message authentication keys, and two EAP message protection keys are derived. This attribute contains a 128byte quantity containing the PAK RSA-encrypted with the SS's 1024 bit RSA public key. Details of the RSA encryption procedure are given 7.x The ciphertext produced by the RSA algorithm shall be the length of the RSA modulus, i.e., 128bytes

Type	Length	Value
30	128	128 byte quantity representing an RSA-encrypted PAK

[Add 11.9.23 as follows:]

11.9.23 PAK/AK Sequence Number

Description This attribute contains sequence number for a PAK. It is a 64bit quantity. A summary of the Key-Sequence-Number attribute format is shown below. Note that this attribute can be used as top level attribute (PAK) as well as a subattribute (AK).

Type	Length	Value
31	8	64bits Sequence for both PAK and AK

[Add 11.9.24 as follows:]

11.9.24 BS-Certificate

Description: This attribute is a string attribute containing an X.509 BS Certificate, as defined 7.x. A summary of the BS-Certificate attribute format is shown below. The fields are transmitted from left to right

Type	Length	Value
32	Variable. Length shall not cause resulting MAC management message to exceed the maximum allowed size	X.509 BS Certificate (DER-encoded ASN.1)

[Add 11.9.25 as follows:]

11.9.25 SigBS

Description: This attribute contains a RSA signature computed over PKMv2 Auth reply message

Type	Length	Value
33	20	An RSA signature over all the message in the PKMv2 Auth reply message

[Add 11.9.26 as follows:]

11.9.26 SS-MAC Address

Description: This attribute is the MAC address of SS

Type	Length	Value
34	6	The MAC address of SS

11.9.27 OMAC Digest

Description: This attribute contains a Message Authentication Code used for message authentication. The OMAC algorithm is defined in draft SP 800-38B.

Type	Length	Value
34	8	A 64 bits (8 byte) keyed OMAC