Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Final Draft for SDD text on Security from Security RG**
Date Submitted	**2008-11-12**
Source(s)	Wei-Peng Chen Fujitsu DJ Johnston Intel Ranga Reddy US Army **Security Rapporteur Group Chairs** E-mail:wei-peng.chen@us.fujitsu.com E-mail:dj.johnston@intel.com E-mail:ranga.reddy@us.army.mil *<http://standards.ieee.org/faqs/affiliationFAQ.html>
Re:	Security Rapporteur Group Discussions
Abstract	This contribution represents the final version of the Security RG consensus document. It includes all the comments reviewed and resolved during Session #58
Purpose	Review, discussion, and approval by the Security RG
Notice	*This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups*. It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who reserve(s) the right to add, amend or withdraw material contained herein.
Release	
Patent Policy	

Final Draft for SDD text on Security from Security RG

Wei-Peng Chen, DJ Johnston, Ranga Reddy

Fujitsu, Intel, US Army

Security Rapporteur Group Chairs

1. Introduction

This contribution represents the Final Draft for Section 10.5 text of the IEEE 802.16m SDD (80216m-08/003r5). In this revision of text, RG chairs have incorporated the contributions from C802.16m-Security-08/022 through 08/037, and the editing changes represented by the comment resolution stored in the Session #58 Security RG comment resolution database (802.16m-Security-08/002r2).

2. List of Contributions

This section contains a list of contributions made by participants in the Security RG, towards development of text for the Final Draft of Security SDD text.

Contribution #	Author & Affiliation
C802.16m-Security-08/022 & 08/023	Allan Xu, Lei Jin Libra Xiao (Huawei Technologies)
C802.16m-Security-08/028 & 08/029	DJ Shyy (MITRE)
C802.16m-Security-08/035	Masato Okuda (Fujitsu)
C802.16m-Security-08/030 & 08/031	Yair Bourlas (NextWave Wireless Inc)
C802.16m-Security-08/024 & 08/025	GeneBeck Hahn, KiSeon Ryu and Ronny YongHo Kim (LG Electronic, Inc.)
C802.16m-Security-08/032, 08/033, & 08/037	Youngkyo Baek, Anil Agiwal (Samsung Electronics)
C802.16m-Security-08/034	Per Ernström, Per-Erik Östling (Ericsson)
C802.16m-Security-08/026, 08/027, & 08/036	Jan Suumaki (Nokia)

3. Text Proposal

[---Start of Text Proposal---]

10.5 Security

10.5.1 Security Architecture

The security functions provide subscribers with privacy, authentication, and confidentiality across the 802.16m network. It does this by applying cryptographic transforms to MAC PDUs carried across connections between MS and BS.

The security architecture of 802.16m system consists of the following functional entities; the MS, the BS, and the Authenticator.

Figure 10.5.1-1 describes the protocol architecture of security services.

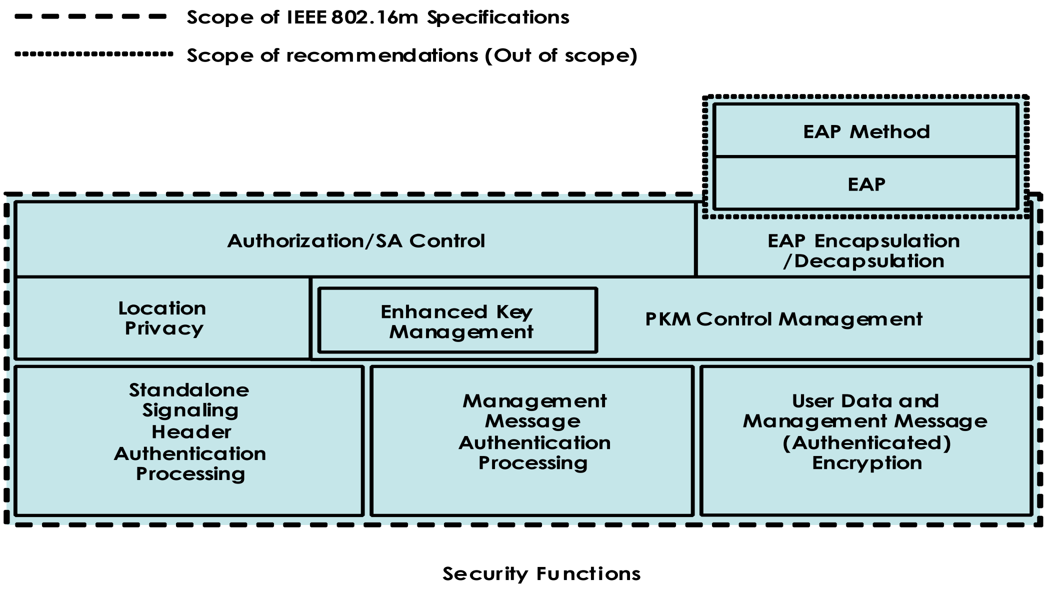
Scope of IEEE 802.16m Specifications
Scope of recommendations (Out of scope)
EAP Method
EAP
Authorization/SA Control
EAP Encapsulation /Decapsulation
Location Privacy
Enhanced Key Management
PKM Control Management
Standalone Signaling Header Authentication Processing
Management Message Authentication Processing
User Data and Management Message (Authenticated) Encryption
Security Functions

Figure 10.5.1-1: Functional Blocks of IEEE 802.16m Security Architecture

Within MS and BS the security architecture is divided into two logical entities:

- Security management entity
- Encryption and integrity entity

Security management entity functions includes :

- Overall security management and control
- EAP encapsulation/decapsulation for authentication & authorization
- Privacy Key Management (PKM) Control (e.g. Key Generation/Derivation/Distribution, Key State Management)
- Security Association (SA) management
- Identity/Location Privacy

Encryption and integrity protection entity functions include:

- Traffic Data Encryption/Authentication Processing
- Message authentication processing
- Message Confidentiality Protection

10.5.2 Authentication and Authorization Protocol

Authorization is the process of one station authenticating the identity of another. In the reference system this process is mutual, i.e. the BS authenticates the identity of SS and the SS authenticates the identity of the BS. In the reference system, RSA-based authentication is defined. [However, in IEEE 802.16m, ECC (Elliptic Curve Cryptography)-based authorization should be supported as well.] Credentials used for RSA [and ECC] authorization will be based on X.509 certificates (IETF RFC 3279, 3280). RSA [or ECC]-based authorization can be coupled with EAP authentication. EAP authentication (IETF RFC 3748) provides and additional level of authentication with an operator-selected EAP method (e.g EAP-TLS, EAP-SIM).

Execution of EAP methods and selection of credentials that are used during EAP authentication are outside the scope of this specification.

Authentication is executed during initial network entry after security capabilities and policies are negotiated. General SS capability negotiation shall be performed after authentication and authorization.

Re-authentication should be made before lifetime of authentication materials/credentials expires. Data transmission may continue during re-authentication process ,by providing SS with two sets of authentication/ keying material with overlapping lifetimes. Authentication procedure is controlled by authorization state machine, which defines allowed operations in specific states.

10.5.2.1 MS Privacy

In reference system there is no explicit means by which identity of user is protected. During initial ranging and certificate exchange during authorization MS MAC Address (MS ID) is transmitted in the clear. Hence, the identity or location information can be easily inferred from fixed MS MAC address, result of which violates the security aspects of IEEE 802.16m SRD. Detailed method for providing MS ID privacy is FFS.

[Editor's Note: During RG discussion support for Authorization was removed. However, this text remains, as there was no specific comment submitted to address it. It would be appropriate to remove Section 10.5.2.2 to make it consistent with the removal of the other authorization text.]

10.5.2.2 Elliptic Curve Cryptography-based Authorization

In addition to the current RSA-based authorization within the PKM protocol, Elliptic Curve Cryptography (ECC)-based authorization may be employed.

During initial and re-authorization, the SS can format the request in either one of two ways. The first way is to make use of a manufacturer-installed ECC certificate and public key that is associated with the SS in the initial authorization request. The other method is that the SS uses the elliptic curve domain parameters defined in its certificate to generate an ephemeral key pair.

Regardless of the method used, the BS then verifies the domain parameters, the public key, and the signature over the request. If any of these checks fail, the then authorization request is rejected. When the BS responds, it can choose between either of two methods (similar to SS initiation methods) when formatting the response.

10.5.3 Key Management Protocol

IEEE 802.16m inherits the key hierarchies of the reference system. The 802.16m uses the PKM protocol to achieve:

- Transparent exchange of authentication and authorization (EAP) messages (Chapter 10.5.2)
- Key Agreement (Chapter 10.5.3.2)
- Security material exchange (Chapter 10.5.3.2)

PKM protocol provides mutual and unilateral authentication and establishes shared secret between the MS and the BS. The shared secret is then used to exchange or derive other keying material. This two-tiered mechanism allows frequent traffic key refreshing without incurring the overhead of computation intensive operations.

10.5.3.1 Key Derivation

All 802.16m security keys are either derived directly / indirectly from the MSK or generated randomly by the BS.

The Pairwise Master Key (PMK) is derived from the MSK and then this PMK is used to derive the Authorization Key (AK).

Some IEEE 802.16m keys are respectively derived and updated by both the BS and the SS.

[Editor's Note: During RG discussion support for Authorization was removed. However, this text remains, as there was no specific comment submitted to address it. It would be appropriate to remove the following text in Section 10.5.3.1 to make it consistent with the removal of the other authorization text.]

Elliptic-Curve Diffie Hellman primitives (as defined in Section 5.4 of ANSI X9.62-2005) will be used to generate the PMK if ECC authorization is used. Key hierarchy for keys derived from ECC generated PMK will follow key hierarchy for keys derived from RSA certificates.

The Authorization Key (AK) is used to derive other keys:

- Key Encryption Key (KEK)
- Transmission Encryption Key (TEK)
- Cipher-based Message Authentication Code (CMAC) key

After AK derivation, key agreement may be performed to verify the newly created AK and exchange other required security parameters.

Alternatively ranging procedure may used to exchange nonce and other required security parameters.

KEK derivation follows procedures as defined in reference system.

TEK is derived at MS and BS by feeding identity parameters into a key derivation function. Parameters such as AK, Security Association ID (SAID), NONCE, KEY_COUNT, BSID, MS MAC address can be used. NONCE is generated by BS and distributed to SS.. If more than one TEK is to be created for an SA, separate KEY_COUNTs are maintained for each TEK.

The CMAC key is derived locally by using the AK, the KEY_COUNT and SAID of SA concerned with control plane/management signaling, as well as other identity parameters.

TEK(s) and the CMAC keys shall be derived in the following situations:

- Initial authentication
- Re-authentication
- Key update procedure for unicast connection.
- Handover to target 802.16m BS
- Re-entry to new 802.16m BS after connection loss / uncoordinated HO / idle mode re-entry.

In the last three cases, KEY_COUNT value is incremented prior derivation.

Group AK (GAK) is randomly generated at the BS.

The GTEK is generated locally by using the GAK, the NONCE, the KEY_COUNT and other identity parameters.

New GTEK shall be derived in the following situations:

- MS enters to multicast group (derived only in MS side)
- Generation and transmission of new GAK
- Group key update procedure for multicast connection.

10.5.3.2 Key Exchange

The key exchange procedure is controlled by the security key state machine, which defines the allowed operations in the specific states. The key exchange state machine does not differ from reference system, except that instead of the exchanging the keys in reference system, a nonce is exchanged and used to derive keys locally.

Distribution mechanism for nonce is FFS. In IEEE 802.16m, the nonce used to derive and update TEK is sent from BS to MS during authorization phase.

The BS and the MS derive the TEK through the key derivation mechanism at each side respectively. Update mechanism for nonce is FFS.

The Nonce can be exchanged with the following messages:

- Key Request / Reply
- Key Agreement
- Ranging

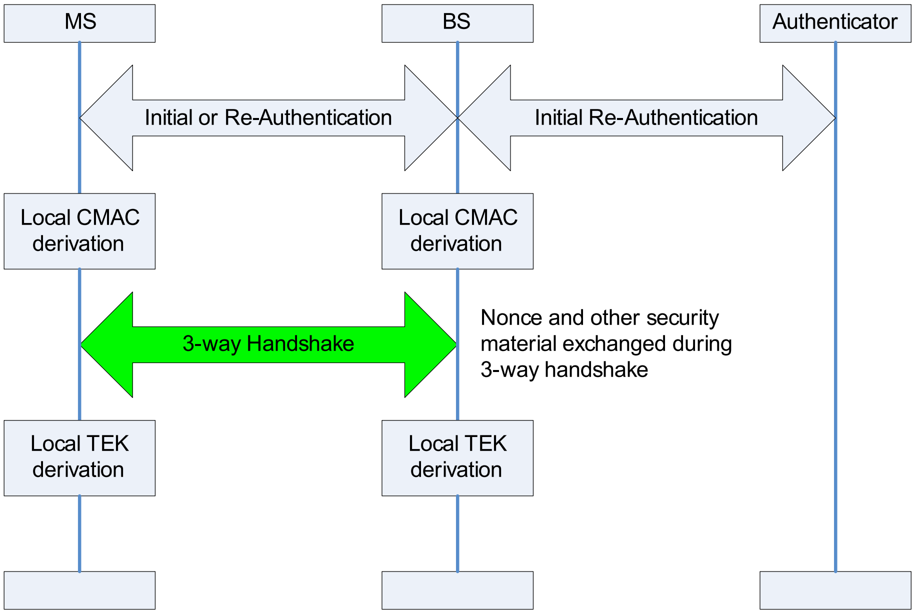
MS
BS
Authenticator
Initial or Re-Authentication
Initial Re-Authentication
Local CMAC derivation
Local CMAC derivation
3-way Handshake
Nonce and other security material exchanged during 3-way handshake
Local TEK derivation
Local TEK derivation

Figure 10.5.3.2-1: Initial or Re-authentication - Key Derivation and Exchange

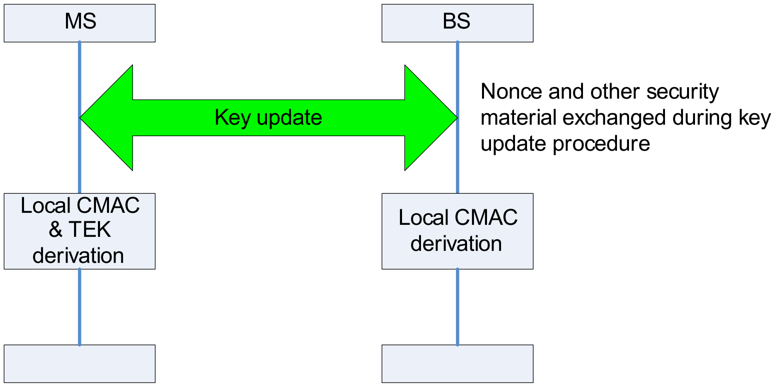
MS
BS
Key update
Nonce and other security material exchanged during key update procedure
Local CMAC & TEK derivation
Local CMAC derivation

Figure 10.5.3.2-2: Key Update Procedure

10.5.3.3 Key Usage

The TEK usage does not differ from 'Reference System'.

In encryption, used KEY_COUNT shall be identified by the receiver (MS or BS). EKS field carries the 2-bit key sequence of associated TEK. Alternative EKS design and usage is FFS.

10.5.4 Security Association Management

A security association (SA) is the set of information required for secure communication between BS and MSs. SA is identified using an SA identifier (SAID). In the reference system, the SA is applied to the respective flows once an SA is established.

IEEE 802.16m supports two types of basic SA management:

- Unicast SA (SA)
- Group SA (GSA)

Unicast SA is used to provide keying material to unicast transport connections. As in the case of the reference system, the data plane SA is applied to all messages exchanged within the same flow. Multiple flows may be mapped to the same unicast SA. Unicast SA can be static or dynamic. Static SAs are assigned by the BS. Dynamic SAs are mapped to a particular service flow, and are taken down when that service-flow is no longer in operation.

The unicast SA is used to provide keying material for management connections.

[Editor's Note: The header design is ongoing in 802.16m, the EC bit seems unlikely to remain in the standard. So, this text may need to be modified based on that decision.]
However, SA is not equally applied to the messages within the same flow. According to the value of MAC header fields (e.g. EC, EKS, Flow ID), the SA is selectively applied to the management connections.

When a service flow is established between the BS and the group of SS's, it is considered to be multicast and it is serviced by a Group SA (GSA).

If SS and BS decide "No authorization" as their authorization policy, no SAs will be established. In this case, Null SAID shall be used as the target SAID field in DSA-REQ/RSP messages. If authorization is performed but the MS and BS decide to create an unprotected service flow, the Null SAID may be used as the target SAID field in DSA-REQ/RSP messages.

10.5.5 Cryptographic Methods

Cryptographic methods specify the algorithms used in 802.16m for the following functions:

- User data and management data encryption/decryption methods and algorithms
- Key encryption/decryption methods and algorithms
- CMAC calculation algorithm for management message integrity protection

10.5.5.1 Encryption methods

MS and BS may support encryption methods and algorithms for secure transmission of MPDUs. AES algorithm is the only supported cryptographic method in 802.16m. The following AES modes are defined in 802.16m:

- AES-CCM mode - provides also integrity protection
- AES-CTR mode

10.5.5.1.1 AES in CCM mode

10.5.5.1.1.1 PDU payload format

The PN size is reduced in 802.16m from 4 bytes to 3 bytes. Further reduction in PN and supporting methods are FFS. The nonce construction for the CCM algorithm defined in IEEE 802.16e is used also for 802.16m.

10.5.5.2 Key encryption methods

Key encryption method NIST AES key wrap shall be used to encrypt a key, when cryptographic key(s) is needed to transmit from BS to MS.

10.5.5.3 Control Plane Signaling Protection

Contrary to the legacy systems that do not define the confidentiality protection over control plane signaling, IEEE 802.16m selectively protects the confidentiality of control plane signaling. The use of MAC (Message Authentication Code) in legacy systems only proves the originator of messages and ensures integrity of the messages.

10.5.5.3.1 Management Message Protection

IEEE 802.16m supports the selective confidentiality protection over MAC management messages. Through capability negotiation, MS and BS know whether the selective confidentiality protection is applied or not. If the selective confidentiality protection is activated, the negotiated keying materials and cipher suites are used to encrypt the management messages. Information required for selective confidentiality support is contained in FFS.

Figure 10.5.5.3-1 presents three levels of selective confidentiality protection over management messages in IEEE 802.16m.

- No authorization: If SS and BS decide “No authorization” as their authorization policy, then the management messages are neither encrypted nor authenticated. Management messages before the authorization phase also fall into this category.
- CMAC based integrity protection; CMAC Tuple TLV is included to the end of management message as a last TLV. CMAC integrity protects only payload, not header part. Actual management message is plain text.

AES-CCM based authenticated encryption; ICV field is included after encrypted payload and this ICV integrity protects both payload and MAC header part.

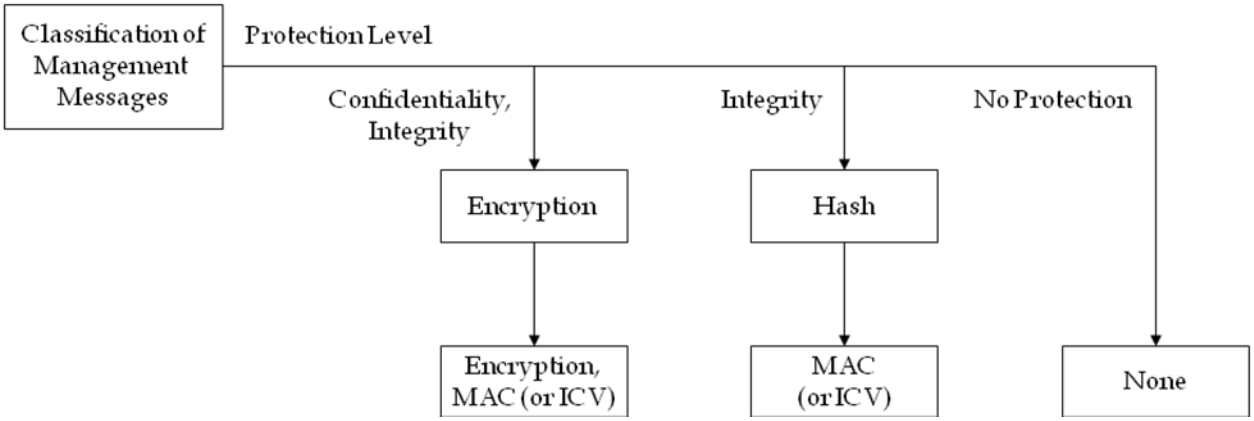

Figure 10.5.5.3-1. Flow of IEEE 802.16m Management Message Protection

10.5.5.3.3 Standalone Signaling Header Authentication

Integrity protection is applied to standalone MAC signaling header. Method for providing standalone signaling header protection is FFS.

10.5.6 Certificate Profile

[Editor’s Note: During RG discussion support for Authorization was removed. However, this text remains, as there was no specific comment submitted to address it. It would be appropriate to remove the following text in Section 10.5.6 to make it consistent with the removal of the other authorization text.]

This subclause describes the X.509 Version 3 certificate format and certificate extensions used in IEEE 802.16-compliant SSs. The X.509 Version 3 format is defined in IETF RFC 3280. ASN.1 encoding of algorithms object identifiers (OIDs) are also further described in IETF RFC 3279.

The basic X.509 Version 3 certificate format and set of ASN.1 encoded OIDs describing signature algorithms and public keys, is retained from the reference system for certificates used as credentials for RSA-based authorization (RSA signature algorithm and RSA public keys). RSA certificates will be based on keys that are no less than 1024 bits and no greater than 2048 bits.

ECC-based authorization requires credentials based on X.509 certificates that specify use of Elliptic Curve Digital Signature Algorithm (ECDSA) as the signature algorithm, define a set of elliptic curve domain parameters, and a public key generated from the set of domain parameters.

The elliptic curve domain parameters can be generated according to procedures defined in Section A.3 of ANSI X9.62-2005. Example parameters sets of parameters can be found in FIPS 186-3 and ANSI X9.63-2001. Domain parameters sets that are selected will produce keys of no less than 160 and no greater than 224 bits in length.

10.5.7 Mobility & Backward Compatibility

[Editor's Note: Text for this section is dependent upon work of other Rapporteur Groups.]

10.5.8 MBS Security

[Editor's Note: Text for this section is dependent upon work of MBS RG.]

[--End of Text Proposal--]