Changes in 802.16e Working Document for SS Authorization via EAP Framework

IEEE 802.16 Presentation Submission Template (Rev. 8.3)

Document Number:

IEEE S802.16e-03/63r1

Date Submitted:

2003-11-13

Source:

Ae Soon Park, Sun Hwa Lim, Seokheon Cho, Young Jin Kim, Jee Hwan Ahn
ETRI,
161, Gajeong-Dong, Yuseong-Gu
Daejeon, Korea, 305-350

Voice: +82-42-860-5172
Fax: +82-42-860-5471
E-mail: aspark@etri.re.kr

Venue:

802.16e Session #28

Base Document:

IEEE C802.16e-03/63r1) and URL <http://ieee802.org/16/C80216e-03_63r1.pdf>

Purpose:

The document is submitted for review by Handoff/Sleep Mode Ad Hoc Group and/or by 802.16 Working Group Members

Changes in 802.16e Working Document for SS Authorization via EAP Framework

IEEE C802.16e-03/63r1.

2003. 11

ETRI
한국전자통신연구원

Contents

- Introduction
- Problem Statements
- Contribution in 802.16e
- Changes and Additions
- Conclusion

Introduction

- **Motivation**
  - **Need a device authentication or user authentication for mobile service (roaming or handoff service)**
  - **Interworking services between wireless networks have been increased recently.**
  - **The interworking is especially important in hot-spot area, where the coverage areas of multiple networks overlap each other, in order to authenticate mobile stations of other networks.**
  - **When IEEE 802.16 network interworks with other wireless networks (e.g. IEEE 802.11 a/b), it is difficult to accept the authentication framework that is provided in other wireless networks because IEEE 802.16 privacy sub-layer is a private protocol.**
  - **Using the open API may be an efficient way to authenticate mobile stations because if open API based authentication mechanism is provided in IEEE 802.16 network, the network is able to accept mobile stations of heterogeneous wireless network.**

    For Example, 802.1x introduces the EAP framework as an open API.

Introduction

Objective

- Propose SS authentication mechanism based on EAP framework
  - by adding IEEE 802.16 privacy sub-layer
  - define additional MAC messages for transferring EAP payload.

- To transfer EAP payload on MAC layer
  - Added to PKM Messages
    - EAP Transfer Request and EAP Transfer Reply

Introduction

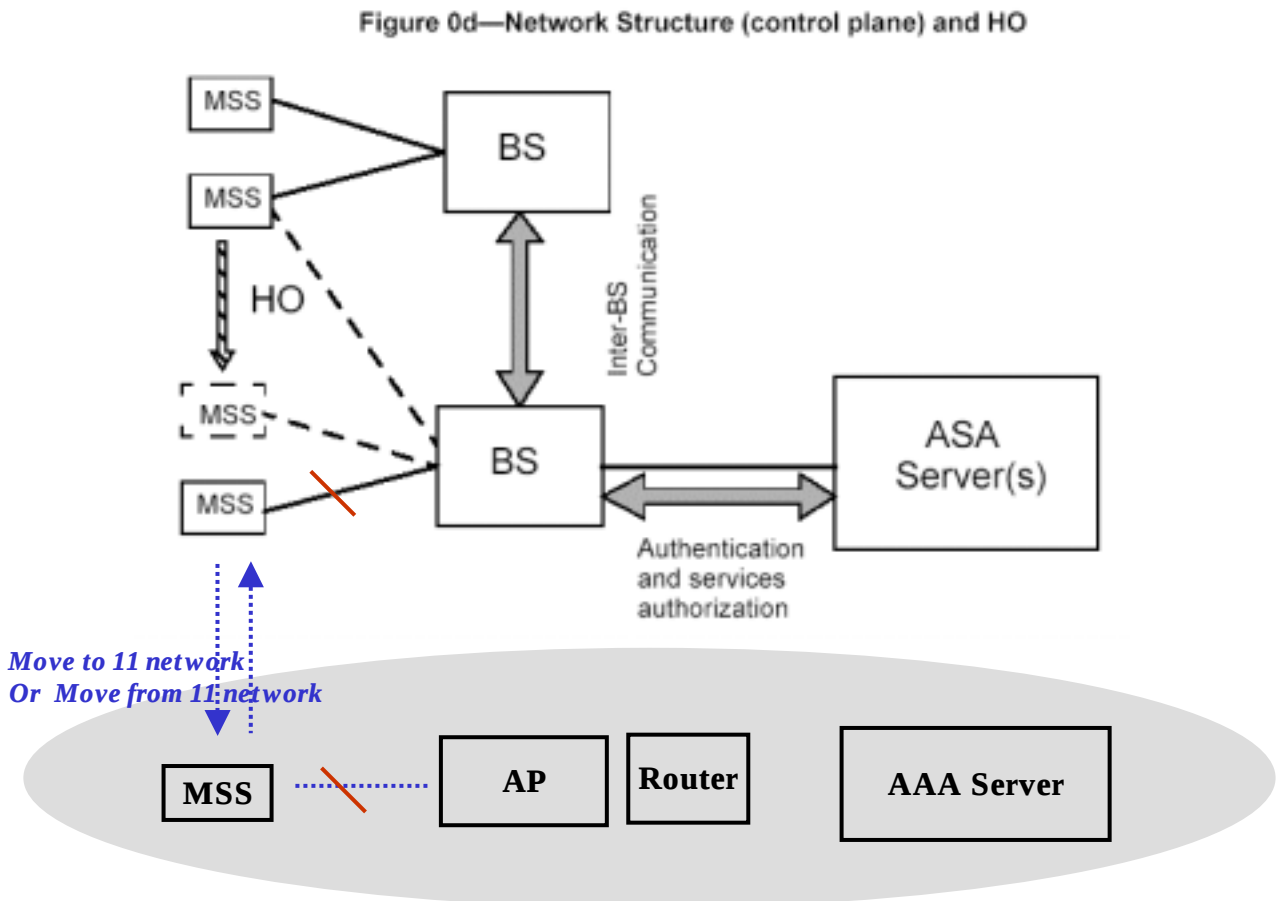
- **Advantage**
  - **To provide device and user authentication**
  - **Interworking with other wireless networks**
    - **e.g., 802.11 a/b**
  - **can provide and support of various authentication mechanism on an application layer**

Problem Statements I – device and user authentication for mobility service

ISSUE		Existing authorization policy	Proposed policy (open authorization policy)
Basic Authentication	Device (Terminal) Authentication	OK	OK
	User authentication	NOT OK	OK

Problem Statements II – roaming and handoff between heterogeneous networks

- **Interworking Problem**
  - **not compatible**



Problem Statements II – roaming and handoff between heterogeneous networks

- **Our contribution to solve this problem**
  - **MSS and BS supports Open API (based on EAP framework)**
  - **BS and ASA interface protocol is commercial protocol**
    - **RADIUS or Diameter**
    - **So, BS can interwork with any AAA server**
  - **Can solve by minor addition**
    - **using the same authentication framework**
    - **added to an message for the EAP**

Contribution in IEEE 802.16e

- The following are the main issues
  - PKM messages types added to on current MAC message
    - EAP Transfer Request
    - EAP Transfer Reply
  - Attribute definition of EAP Transfer Request message
  - Attribute definition of EAP Transfer Reply message
  - TLV definition of each attribute

Contribution in IEEE 802.16e - Added to an PKM Message

- **EAP Transfer Request, EAP Transfer Reply**

[Add the following rows to table 25]

Code	PKM Message Type	MAC Message Type
0-2	Reserved	
3	SA Add	PKM-RSP
4	Auth Request	PKM-REQ
5	Auth Reply	PKM-RSP
6	Auth Reject	PKM-RSP
7	Key Request	PKM-REQ
8	Key Reply	PKM-RSP
9	Key Reject	PKM-RSP
10	Auth Invalid	PKM-RSP
11	TEK Invalid	PKM-RSP
12	Auth Info	PKM-REQ
13	**EAP Transfer Request**	**PKM-REQ**
14	**EAP Transfer Reply**	**PKM-RSP**
15 ~ 255	reserved	

Contribution in IEEE 802.16e – EAP Transfer Request

- *Add to table 27b*

Attribute	Contents
Security-Capabilities*	Describes requesting SS's security capabilities
SAID*	Security Association ID, being equal to the Basic CID
SS's Public Key(Optional)*	As AK generated by BS, otherwise omitted.
EAP Payload	Contains the EAP-TLS Data, not interpreted in the MAC

- **Security-Capabilities, SAID, SS's Public Key Attributes**
  - **include only the 1'st EAP Transfer Request.**
- **SS's Public Key Attribute**
  - **AK can be generated by a BS or an AAA server. If AK is generated by the BS, the BS has to know SS's public key to encrypt AK.**
  - **Otherwise AK is generated by the AAA server, this attribute is omitted.**
- **EAP Payload Attribute**
  - **is not interpreted in this MAC layer, which contains a data payload for EAP-TLS or EAP-TTLS.**

Contribution in IEEE 802.16e – EAP Transfer Reply

- ***Add to table 28b***

Attribute	Contents
EAP Result Code*	Describes success or failure
Error Code*	Error code identifying reason for rejection or failure of authorization request
AUTH-Key(Optional) *	An AK encrypted with the SS's public key in case of generating by BS
Key Sequence Number*	Authorization key sequence number
Key Life Time*	Authorization key life time
SA Descriptor*	Specifies an SA ID and additional properties of the SA
EAP Payload	Contains the EAP-TLS or EAP-TTLS Data, not interpreted in the MAC

- *** means that attributes are included only the last EAP Transfer Reply.**

Contribution in IEEE 802.16e – added TLV

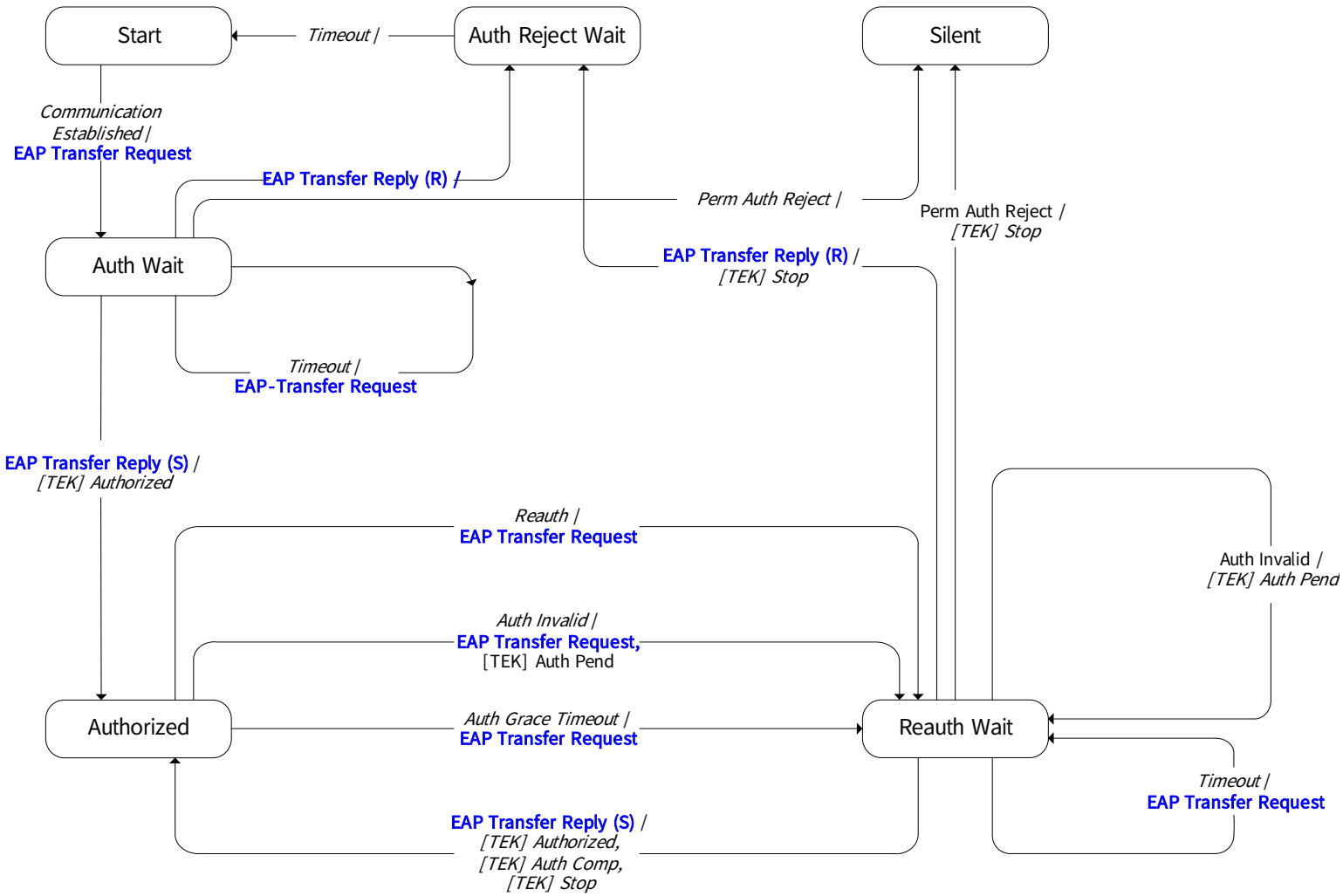
- *Add 11.2.20 EAP Payload*
  - **The EAP Payload attribute is not interpreted in this MAC layer, which contains a data payload for EAP-TLS or EAP-TTLS.**
  - **This attribute uses only an EAP Transfer Request and an EAP Transfer Reply.**

Type	Length	Value (string)
128	n	EAP payload data

- *Add 11.2.21 EAP Result Code*
  - **The EAP Result Code attribute indicates the error status, is included in an EAP Transfer Reply.**

Type	Length	Value (string)
129	1	0 : Success 1 : Failure

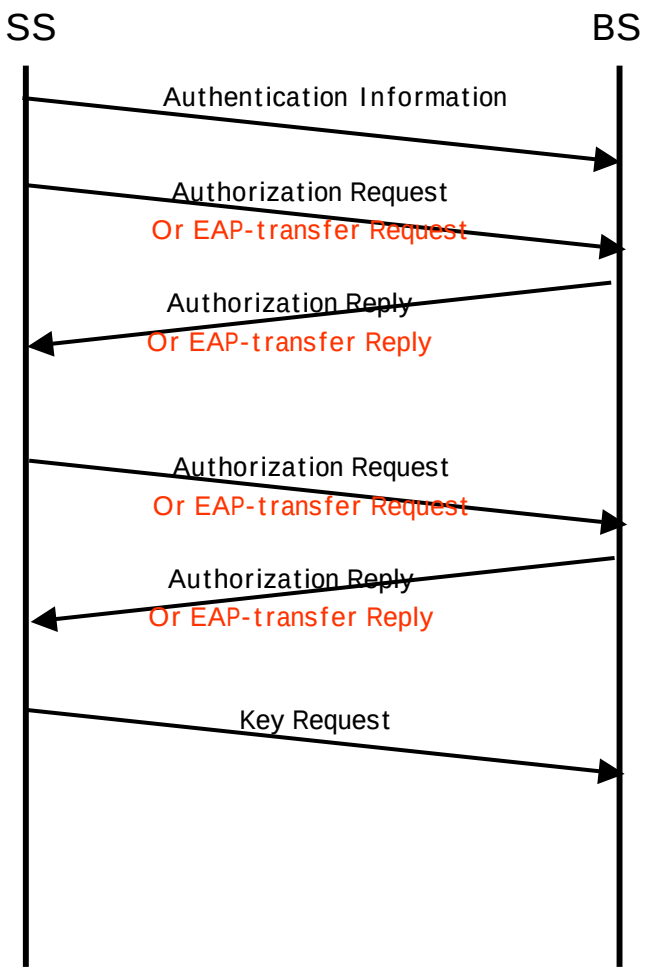
Contribution in IEEE 802.16e – Flow Diagram



Contribution in IEEE 802.16e – State Diagram

State Event or Rcvd Message	(A) Start	(B) Auth Wait	(C) Authorized	(D) Reauth Wait	(E) Auth Reject Wait	(F) Silent
(1) Communication Established	Auth Wait					
(2) Auth Reject or **EAP-Trans Reply (R)**		Auth Reject Wait		Auth Reject Wait		
(3) Perm Auth Reject		Silent		Silent		
(4) Auth Reply or **EAP-Trans Reply (S)**		Authorized		Authorized		
(5) Timeout		Auth Wait		Reauth Wait	Start	
(6) Auth Grace Timeout			Reauth Wait			
(7) Auth Invalid			Reauth Wait	Reauth Wait		
(8) Reauth			Reauth Wait			

Contribution in IEEE 802.16e - AK Management in BS and SS



Changes and Addition in IEEE P802.16-REVd/D1

- *Changes 6.2.2.3.9.2 to the followings*

6.2.2.3.9.2 Authorization Request (Auth Request) message

6.2.2.3.9.2.1 Auth Request message

***Code:* 4**

Attributes are shown in Table 27.

….

An SAID attribute contains a Privacy SAID. In this case, the provided SAID is the SS's Basic CID, which is equal to the Basic CID assigned to the SS during initial ranging.

6.2.2.3.9.2.2 EAP Transfer Request message

Code : 13

Attributes are shown in Table 27b.

Changes and Addition in IEEE P802.16-REVd/D1

- *Changes 6.2.2.3.9.3 to the followings*

6.2.2.3.9.3 Authorization Reply (Auth Reply) message

6.2.2.3.9.3.1 Auth Reply message

Sent by the BS to a client SS in response to an Authorization Request, the Authorization Reply message contains an Authorization Key,

…

6.2.2.3.9.3.2 EAP Transfer Reply message

Sent by BS to a client SS in response to an EAP Ttransfer Request, the EAP Transfer Reply message contains an EAP Result Code(success or failure), Error Code, the key's life time, sequence number, and a list of SA-Descriptors identifying the Primary and Static SAs. The requesting SS is authorized to access and one's particular properties(e.g., type, cryptographic suite). The SA Descriptor list shall include a descriptor for the Basic CID reported to the BS in the corresponding EAP Transfer Request. The SA-Descriptor list may include descriptors of Static SAIDs which are used for the SS authorization. The EAP Payload contains a data payload for EAP-TLS or EAP-TTLS.

Code :14

Attributes are shown in Table 28b

Changes and Addition in IEEE P802.16-REVd/D1

- ***Changes 7 to the followings***

Privacy provides subscribers with privacy across the fixed *or mobile* broadband wireless network.

- ***Changes 7.1 to the followings***

a) An encapsulation protocol for encryption packet data across the fixed *or mobile* broadband wireless access network

Changes and Addition in IEEE P802.16-REVd/D1

- ***Changes 7.1.2 to the followings***

An SS uses the PKM protocol or the EAP protocol to obtain authorization and traffic keying material from the BS, and to support periodic reauthorization and key refresh. The key management protocol for the PKM protocol uses X.509 digital certificates [IETF RFC 2459], the RSA public-key encryption algorithm [PKCS #1], and strong symmetric algorithms to perform key exchanges between SS and BS. ***On the other hands, the key management protocol for the EAP protocol uses EAP-TLS or EAP-TTLS based on a EAP framework.***

….

In 802.16 Existing Policy mode, **A BS authenticates a client SS during the initial authorization exchange. Each SS carries a unique X.509 digital certificate issued by the SS's manufacturer. The digital certificate contains the SS's Public Key and SS MAC address. When requesting an Authorization Key, an SS presents its digital certificate to the BS. The BS verifies the digital certificate, and then uses the verified Public Key to encrypt an Authorization Key, which the BS then sends back to the requesting SS**

All SSs shall have factory-installed RSA private/public key pairs or provide an internal algorithm to generate such key pairs dynamically. If an SS relies on an internal algorithm to generate its RSA key pair, the SS shall generate the key pair prior to its first Authorization Key (AK) exchange, described in 7.2.1. All SSs with factory-installed RSA key pairs shall also have factory-installed X.509 certificates. All SSs that rely on internalalgorithms to generate an RSA key pair shall support a mechanism for installing a manufacturer-issued X.509 certificate following key generation.

In Open Policy mode, an AAA server authenticates a client SS during the initial authorization exchange process using EAP data. Each SS carries a EAP payload. The EAP payload contains the EAP-TLS or EAP-TTLS Data. MAC data contains EAP payload with a MAC header. MAC message consists of general MAC Header and PKM header. A PKM message contains optionally the SS's Public key attribute. The Public key can be used to encrypt an AK which is generated by BS, otherwise this attribute will be omitted.

Changes and Addition in IEEE P802.16-REVd/D1

- ***Add Under 7.2.1***

7.2.1.1 Existing Authorization Policy Mode

7.2.1.2 Open Authorization Policy Mode

An SS begins authorization by sending an EAP Transfer Request message to its BS. The EAP Transfer Request message contains the Security-Capabilities, SAID, and EAP Payload.

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 EAP Transfer Request includes

a) EAP payload

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 one indicates a particular pair 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

d) SS's Public Key is used when AK is generated by BS and is optional.

In response to an EAP Transfer Request message, a BS through AAA server validates the requesting SS's identity, determines the encryption algorithm and protocol shared with the SS, activates an AK for the SS, optionally encrypts it with the SS's public key, and sends it back to the SS in an EAP Transfer Reply message. Otherwise an AK key shares between SS and BS by Upper Layer Security Protocol based on EAP framework such as EAP-TLS or EAP-TTLS. The EAP Transfer Reply includes:

a) EAP Result code

b) Error Code, if EAP Result Code is failure

c) an AK encrypted with the SS's public key, according to key distribution mechanism

d) a 4-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 SS is authorized to obtain keying information for

g) EAP Payload

While the EAP Transfer Reply shall identify Static SAs in addition to the Primary SA whose SAID matches with the requesting SS's Basic CID, the EAP Transfer Reply shall not identify any Dynamic SAs.

The BS, in responding to an SS's EAP Transfer Request, shall determine whether the requesting SS, whose identity can be verified via the EAP framework, is authorized for basic unicast services, and what additional statically provisioned services (i.e., Static SAIDs) the SS's user has subscribed for.

An SS shall periodically refresh its AK by reissuing an EAP Transfer Request to the BS. Reauthorization is identical to authorization with the exception that the SS does not send any other messages during reauthorization.

Changes and Addition in IEEE P802.16-REVd/D1

❑ *Changes 7.2.3 to the followings*

As part of their authorization exchange, the SS provides the BS with a list of all the cryptographic suites (pairing of data encryption and data authentication algorithms) the SS supports. The BS selects from this list a single cryptographic suite to employ with the requesting SS's primary SA. The Authorization Reply *or EAP Transfer Reply* the BS sends back to the SS includes a primary SA descriptor which, among other things, identifies the cryptographic suite the BS selected to use for the SS's primary SA. A BS shall reject the authorization request *or EAP Transfer Request* if it determines that none of the offered cryptographic suites are satisfactory.

The Authorization Reply *or EAP Transfer Reply* also contains an optional list of static SA descriptors; each static SA descriptor identifies the cryptographic suite employed within the SA. The selection of a static SA's cryptographic suite is typically made independent of the requesting SS's cryptographic capabilities. A BS may include in its Authorization Reply *or EAP Transfer Reply* static SA descriptors identifying cryptographic suites the requesting SS does not support; if this is the case, the SS shall not start TEK state machines for static SAs whose cryptographic suites the SS does not support.

Changes and Addition in IEEE P802.16-REVd/D1

- ***Changes 7.2.4 to the followings***

d) State transitions (i.e., the lines between states) are labeled with <what causes the transition>/<messages and events triggered by the transition>. So "timeout/Auth Request *or EAP Transfer Request*" means that the state received a "timeout" event and sent an Authorization Request *or EAP Transfer Request* ("Auth Request", *"EAP Transfer Request"*) message. If there are multiple events or messages before the slash "/" separated by a comma, any of them can cause the transition. If there are multiple events or messages listed after the slash, all of the specified actions shall accompany the transition.

Changes and Addition in IEEE P802.16-REVd/D1

- ***Changes 7.2.4.1 to the followings***

b) Authorize Wait (Auth Wait): The SS has received the "Communication Established" event indicating that it has completed basic capabilities negotiation with the BS. In response to receiving the event, the SS has sent both an Authentication Information and an Auth Request message *or EAP Transfer Request* to the BS and is waiting for the reply.

c) Authorized: The SS has received an Auth Reply *or last EAP Transfer Reply* message which contains a list of valid SAIDs for this SS. At this point, the SS has a valid AK and SAID list. Transition into this state triggers the creation of one TEK FSM for each of the SS's privacy-enabled SAIDs.

d) Reauthorize Wait (Reauth Wait): The SS has an outstanding reauthorization request. The SS was either about to expire (see Authorization Grace Time in Table 119) its current authorization or received an indication (an Authorization Invalid message from the BS *or an EAP Transfer Reply (R) from the BS*) that its authorization is no longer valid. The SS sent an Auth Request *or EAP Transfer Request* message to the BS and is waiting for a response.

e) Authorize Reject Wait (Auth Reject Wait): The SS received an Authorization Reject (Auth Reject) *or EAP Transfer Reply (R)* message in response to its last Auth Request *or EAP Transfer Request*. The Auth Reject's *or EAP Transfer Reply's* error code indicated the error was not of a permanent nature. In response to receiving this reject message, the SS set a timer and transitioned to the Auth Reject Wait state. The SS remains in this state until the timer expires. In response ..

f) Silent: The SS received an Auth Reject *or EAP Transfer Reply (R)* message in response to its last Auth Request *or EAP Transfer Request*. The Auth Reject's *or EAP Transfer Reply's(R)* error code indicated the error was of a permanent nature. This triggers a transition to the Silent state, where the SS is not permitted to pass subscriber traffic. The SS shall, however, respond to management messages from the BS issuing the Perm Auth Reject.

Changes and Addition in IEEE P802.16-REVd/D1

- ***Changes 7.2.4.2 to the followings***

Note that the message formats are defined in detail in 6.2.2.3.9.

Authorization Request (Auth Request *or EAP Transfer Request*): Request an AK and list of authorized SAIDs. Sent from SS to BS.

Authorization Reply (Auth Reply *or EAP Transfer Reply*): Receive an AK and list of authorized, static SAIDs. Sent from BS to SS. The Authorization Key is encrypted with the SS's public key *or securely transferred with the upper layer security protocol based on EAP framework (e.g., EAP-TLS, EAP-TTLS)*.

Authorization Reject (Auth Reject *or EAP Transfer Reply(R)*): Attempt to authorize was rejected. Sent from the BS to the SS.

Authorization Invalid (Auth Invalid *or EAP Transfer Reply(R)*): The BS may send an Authorization Invalid message to a client SS as follows:

Changes and Addition in IEEE P802.16-REVd/D1

- ***Changes 7.2.4.5 to the followings***

Actions taken in association with state transitions are listed by <event> (<rcvd message>) --> <state> below:

1-A Start (Communication Established) → Auth Wait

(a) send Authent Info message to BS, and send Auth Request message to BS

(b) or send EAP Transfer Request message to BS

(c) set Auth Request retry timer to Auth Wait Timeout

2-B Auth Wait (Auth Reject, *EAP Transfer Reply*) → Auth Reject *or EAP Transfer Reply(R)* Wait

b) set a wait timer to Auth Reject *or EAP Transfer Reply(R)* Wait Timeout

2-D Reauth Wait (Auth Reject, *EAP Transfer Reply*) → Auth Reject Wait

c) set a wait timer to Auth Reject *or EAP Transfer Reply(R)* Wait Timeout

4-B Auth Wait (Auth Reply *or EAP Transfer Reply*) → Authorized

b) decrypt and record AK delivered with Auth Reply *or delivered with EAP Transfer Reply*

4-D Reauth Wait (Auth Reply *or EAP Transfer Reply*) → Authorized

b) decrypt and record AK delivered with Auth Reply *or delivered with EAP Transfer Reply*

c) start TEK FSMs for any newly authorized SAIDs listed in Auth Reply or EAP Transfer Reply (provided the SS supports the cryptographic suite that is associated with the new SAID) and issue TEK FSM Authorized event for each of the new TEK FSMs

5-B Auth Wait (Timeout) → Auth Wait

(a) send Authent Info message to BS, and send Auth Request message to BS

(b) or send EAP Transfer Request message to BS

(c) set Auth Request retry timer to Auth Wait Timeout

5-D Reauth Wait (Timeout) → Reauth Wait

a) send Auth Request *or EAP Transfer Request* message to BS

6-C Authorized (Auth Grace Timeout) → Reauth Wait

a) send Auth Request *or EAP Transfer Request* message to BS

7-C Authorized (Auth Invalid) → Reauth Wait

b) send Auth Request *or EAP Transfer Request* message to BS

8-C Authorized (Reauth) → Reauth Wait

b) send Auth Request *or EAP Transfer Request* message to BS

Changes and Addition in IEEE P802.16-REVd/D1

- ***Changes 7.5.5 to the followings***

7.5.5 Public-key Encryption of AK Key ***Encryption of authorization key***

7.5.5.1 Existing Authorization Policy Mode

AKs in Auth Reply …., MGF1 with SHA-1 for the mask-generation function, and the empty string for the encoding parameter string.

7.5.5.2 Open Policy Mode

AK in EAP Transfer Reply messages shall be transferred by EAP framework protocol using the upper layer security protocol (e.g., EAP-TLS, or EAP-TTLS), or shall be a RSA public-key encrypted using the SS's public key, according to key generation mechanism. The AK can be generated by AAA server or BS. In the 1'st case, the AK encrypted by EAP framework, and in the 2'nd case, the AK encryption mechanism has the same mechanism with the existing policy mode.

Conclusion – comparison table

Function	Existing authorization policy	Open authorization policy
MAC Message	Authentication Information Authorization Request Authorization Reply	EAP Transfer Request EAP Transfer Reply
Key Exchange (AK)	16 dependent protocol	EAP-TLS or EAP-TTLS, etc. based on EAP framework security protocol
Authentication Scheme	Terminal Authentication	User authentication (If need a terminal auth then available)
Support SA Set	Authorization(X.509 Digital Certificate) Encryption (DES, 3-DES) Message Hash(HMAC-SHA1)	Authorization (Safe Security Protocol) Encryption (Same, or more various algorithm)) Message Hash(HMAC-MD5, HMAC-SHA1, etc.,)
AK key size	160 Bits	same (support flexible size)
TEK Key Size and Generation	64 bits, generated by BS	Same(support flexible size)
IV	64 bits	Same(support flexible size)
Authentication Server	ASA (out of scope in this spec)	Commercial Product
Protocol Between BS and ASA	out of scope in this spec.	Commercial Product (RADIUS or Diameter)
Scalability	Weak	Good
Compatibility (with heterogeneous network)	weak	YES
Interworking (between heterogeneous network)	NO	YES

Conclusion

- New authorization mechanism adaptation by two messages addition
  - EAP Transfer Request, EAP Transfer Reply
- Compatibility with IEEE 802.16e by minor changes
  - two PKM Message Addition for transferring EAP protocol
- To provide User Authentication functionality
- Efficiency for interworking with heterogeneous wireless networks
- Enhanced security level
  - for replay attack or man-in-middle attack
  - Can support the secure channel for authentication by EAP framework