| | |
|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** |
| Title | **Pre Authentication extension** |
| Date Submitted | **2005-03-09** |
| Source(s) | Yigal Eliaspur, Avishay Shraga, Sanjay Bakshi, David Ayoun, Ilan Zohar<br><br>**Intel Corporation** |
| | yigal.eliaspur@intel.com avishay.shraga@intel.com sanjay.bakshi@intel.com david.ayoun@intel.com<br><br>Voice +972-54-7884877 |
| Re: | IEEE P802.16e/D6 |
| Abstract | Pre authentication support for legacy EAP |
| Purpose | Adoption of proposed changes into P802.16e /D6 |
| 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 (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing the standard."<br><br>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:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>. |

# Pre-authentication extension

*Yigal Eliaspur, Avishay Shraga, Sanjay Bakshi, David Ayoun,*
*Rosner Gedon*
*Intel Corporation*

## 1 Overview

Pre authentication is a useful feature in many network architecture models.
The standard already includes optional pre-authentication messages. However these messages are based on EAP framework draft and cannot be used in legacy EAP architecture.
This proposal proposes an alternative (optional) pre authentication framework which can be used with legacy EAP architecture.

### 1. Details

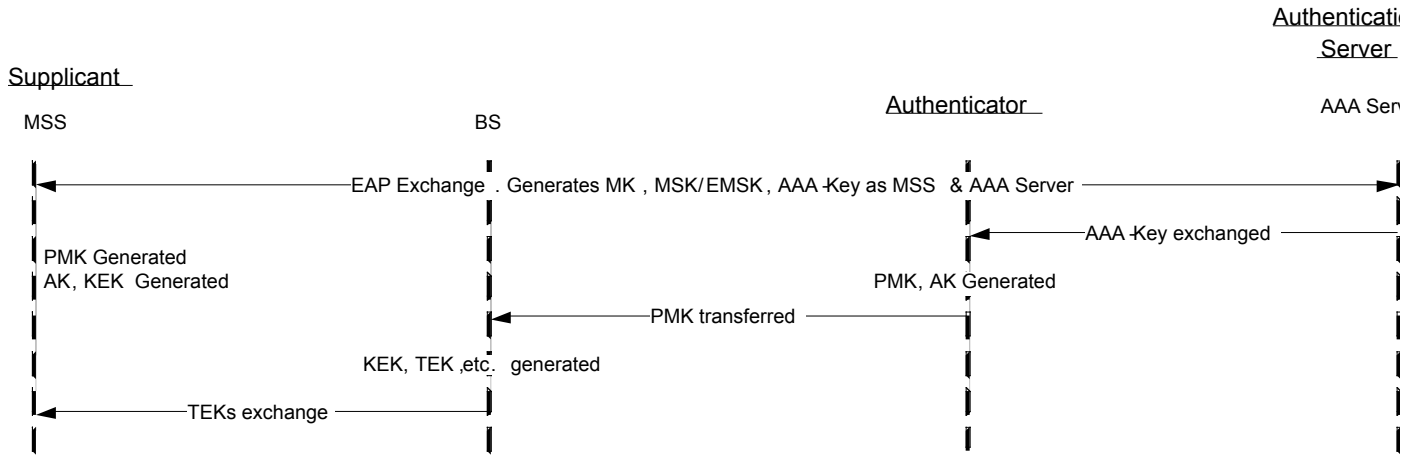
In order to achieve this goal, this contribution defines the following:

a) Two MAC management messages are added: PKMR-REQ and PKMR-RSP for Privacy Key Management Remote. These messages are similar to PKM-REQ and PKM-RSP respectively but the serving BS when receiving them will simply reroute its data forward the message to the target BS's authenticator.
b) A capability bit for the MSS to determine if a target BS supports pre-authentication.
c) An authentication zone identifier on each BS in NBR-ADV message – specifying if pre-auth is required.

**Key Usage Refresher**

**Figure 1**

## 1.1 Summary of the solution




Note: the authenticator may be colocated in the BS or maintained in a separate entity.

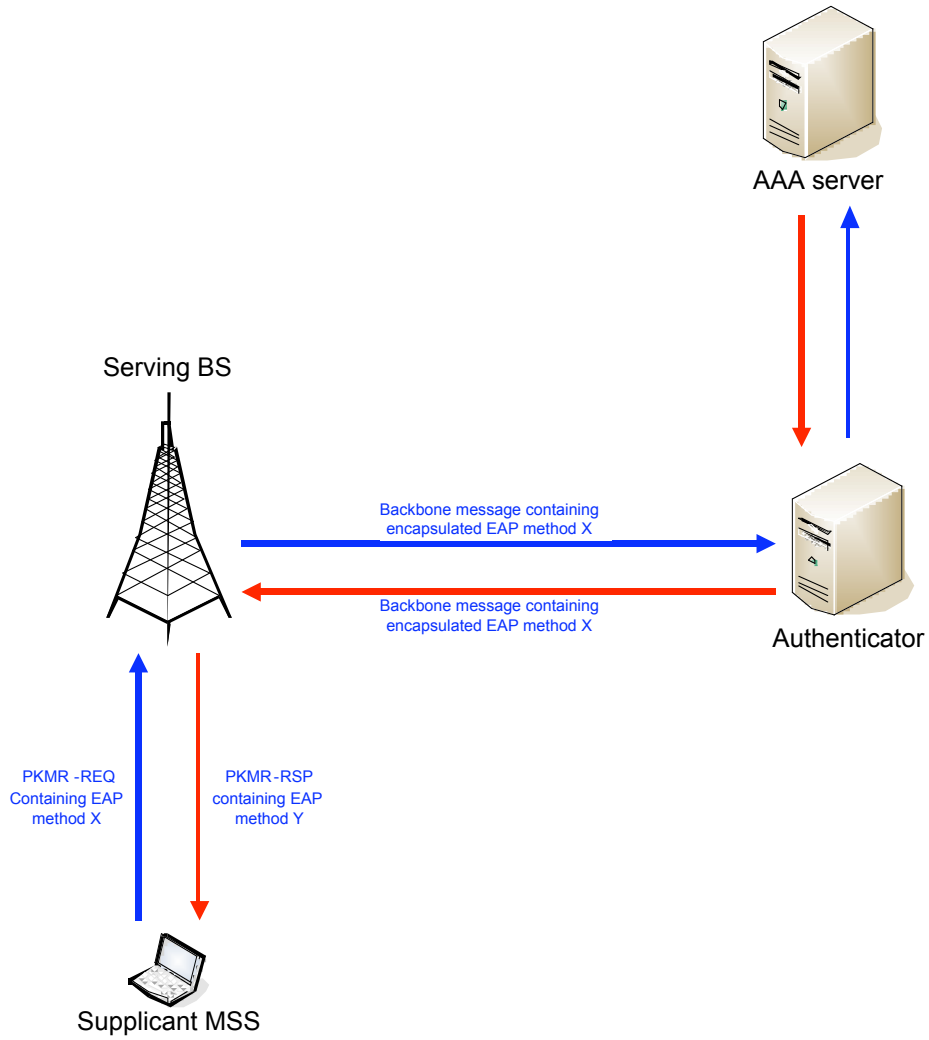

AAA server
Serving BS
Backbone message containing encapsulated EAP method X
Backbone message containing encapsulated EAP method X
Authenticator
PKMR -REQ Containing EAP method X
PKMR-RSP containing EAP method Y
Supplicant MSS

**Figure 1**

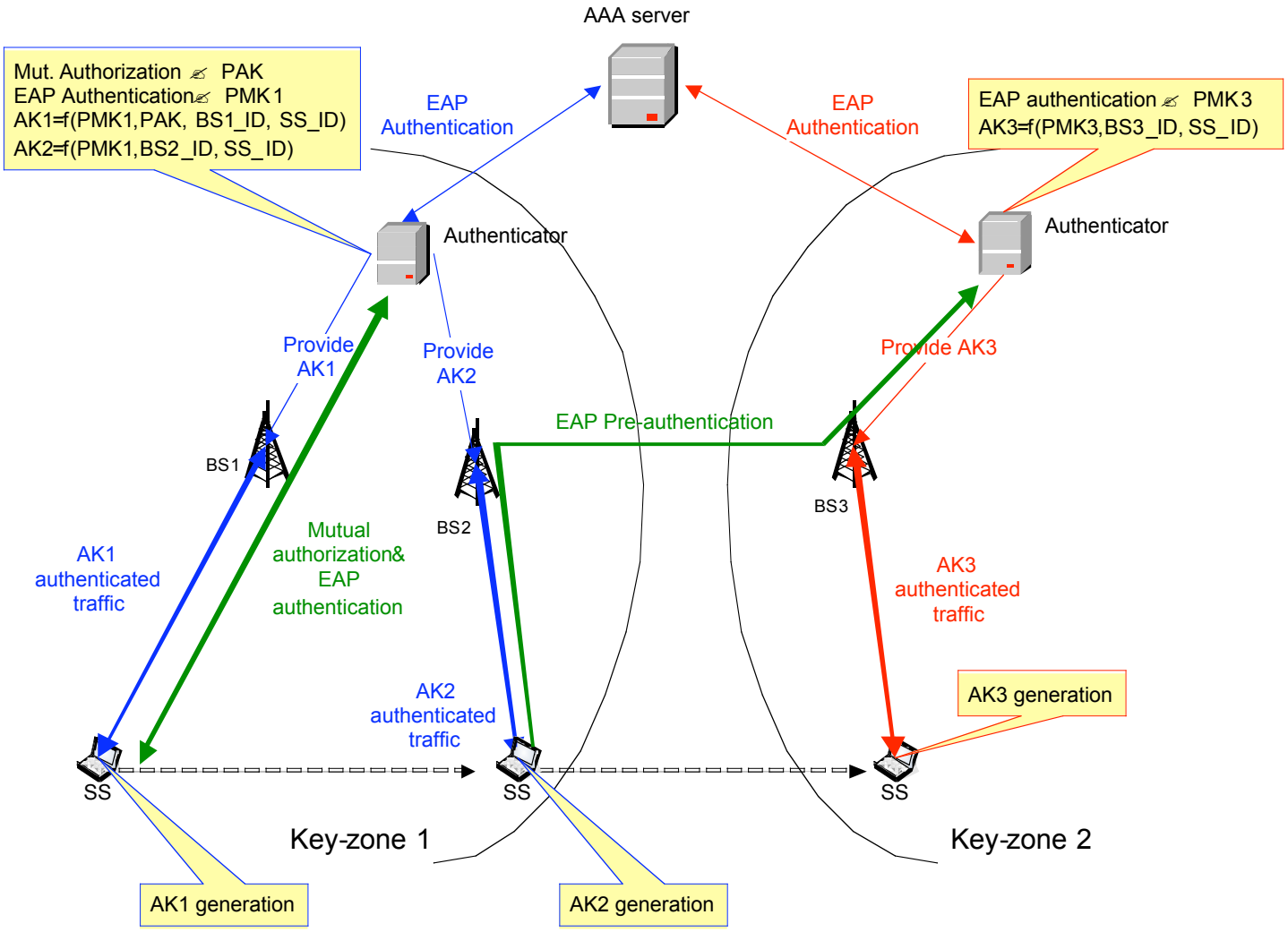



**Figure 3**

## 2 Text Change

*[In IEEE P80216e_D6 modify table 26 – PKM message codes]*

**Table 26—PKM message codes**

| Code | PKM message type | MAC Management message name |
|---|---|---|
| 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 | PKM-REQ/PKM-RSP |
| 14 | EAP-Establish-Key Request | PKM-RSP |
| 15 | EAP-Establish-Key Reply | PKM-REQ |
| 16 | EAP-Establish-Key Reject | PKM-REQ |
| 17 | EAP-Establish-Key Confirm | PKM-RSP |
| ~~18~~ | ~~Pre-Auth-Request~~ | ~~PKM-REQ~~ |
| ~~19~~ | ~~Pre-Auth-Reply~~ | ~~PKM-RSP~~ |
| ~~20~~ | ~~Pre-Auth-Reject~~ | ~~PKM-RSP~~ |
| 18-20 | *reserved* | — |
| 21 | PKMv2 Auth-Request | PKM-REQ |
| 22 | PKMv2 Auth-Reply | PKM-RSP |
| 23 | Key Update Command | PKM-RSP |
| 24-255 | *reserved* | — |

*[Delete sections '6.3.2.3.9.16 Pre-Auth-Request message', '6.3.2.3.9.17 Pre-Auth-Reply message' and '6.3.2.3.9.18 Pre-Auth-Reject message']*

*[In 6.3.2.3.47 add entries to table 106d as follows]*

**Table 106d— MOB_NBR-ADV Message Format**

| Syntax | Size | Notes |
|---|---|---|
| MOB_NBR-ADV_Message_Format() { | | |
| **Management Message Type = 53** | 8 bits | |
| **Skip-Optional-Fields bitmap** | 8 bits | Bit [0]: if set to '1', omit Operator ID field<br>Bit [1]: if set to '1', omit NBR BS ID field<br>Bit [2]: if set to '1', omit HO process optimization field<br>Bit [3]: if set to '1', omit QoS related fields<br>Bit [4]-[7]: *reserved* |
| **…** | | |
| if (Skip-Optional-Fields[2]=0) { | | |
| **HO Process Optimization** | 8 bits | HO Process Optimization is provided as part of this message is indicative only. HO process requirements may change at time of actual HO. For each Bit location, a value of '0' indicates the associated reentry management messages shall be required, a value of '1' indicates the reentry management message may be omitted.<br>Regardless of the HO Process Optimization TLV settings, the target BS may send unsolicited SBC-RSP and/ or REG-RSP management messages<br>Bit #0: Omit SBC-REQ/RSP management messages during current re-entry processing<br>Bit #1: Omit PKM-REQ/RSP management message during current re-entry processing<br>Bit #2: Omit REG-REQ/RSP management during current re-entry processing<br>Bit #3: Omit Network Address Acquisition management messages during current reentry processing<br>Bit #4: Omit Time of Day Acquisition management messages during current reentry processing<br>Bit #5: Omit TFTP management messages during current re-entry processing<br>Bit #6: Full service and operational state transfer or |

| | | |
|---|---|---|
| | | sharing between serving BS and target BS (ARQ, timers, counters, MAC state machines, etc…)<br>Bit #7: *Reserved* |
| if (HO Process Optimization bit [1] is Set) { | | Authentication Optimization bit |
| **Authentication Zone** | 12 bits | Authentication zone Identifier for the BS |
| **Pre-authentication Support** | 1 bit | Capability bit for target BS |
| *Reserved* | 3 bits | Shall be set to zero |
| } | | |
| } | | |
| … | | |

*[In section 6.3.2.3.47, Add following text after "Available Radio Resource" text]*

**Authentication Zone**
Specifies the authentication zone to which the neighbor BS belongs
**Pre-authentication Support**
This field specifies whether neighbor BS support pre-authentication capability. If this bit is set, then the MSS can do pre-authentication with the neighbor BS and generate a PMK for the authentication zone.

*[In 6.3.2.3.51 add entries to table 106j as follows]*

**Table 106j—MOB_BSHO-REQ message format**

| Syntax | Size | Notes |
|---|---|---|
| MOB_BSHO-REQ_Message_Format() { | | |
| **Management Message Type = 56** | 8 bits | |
| **Network Assisted HO supported** | 1 bit | Indicates that the BS supports Network Assisted HO |
| **Mode** | 3 bits | 0b000: HHO request<br>0b001: SHO/FBSS request: Anchor BS update with CID update<br>0b010: SHO/FBSS request: Anchor BS update without CID update<br>0b011: SHO/FBSS request: Active Set update with CID update<br>0b100: SHO/FBSS request: Active Set update without CID update<br>0b101: SHO/FBSS request: Active Set update with CID update for newly added BS<br>0b110: : SHO/FBSS request: Active Set update with CID update and CQICH allocation for newly added BS<br>0b111: *reserved* |
| If (Mode == 0b000) { | | |
| **N_Recommended** | 8 bits | |
| For (j=0 ; j<N_Recommended ; j++) { | | Neighbor base stations shall be presented in an order such that the first presented is the one most recommended and the last presented is the least recommended. |
| **Neighbor BSID** | 48 bits | |
| **Service level prediction** | 8 bits | |
| **MSS Authenticated** | 1 bit | 0: MSS must perform authentication with target BS<br>1: Target BS holds a valid PMK and according to the circumstances may hold a valid AK context |
| } | | |
| } | | |
| else if (Mode == 0b001) { | | |
| **TEMP_BSID** | 3 bits | TEMP_BSID of the recommended Anchor BS |
| .<br>.<br>. | | |

*[In section 6.3.2.3.51, Add following text after "Service level prediction" text]*

**MSS Authenticated**

0: MSS must do full authentication even if a valid AK exists.1: Informs the MSS that there is no need to perform authentication and that AK may be derived from the existing PMK that the MSS and BS share or that an AK context already exists according to the circumstances.

*[Insert text and tables as follows]*

### 6.3.2.3.59 Privacy key management – remote (PKMR) messages (PKMR-REQ/PKMR-RSP)

PKMR employs two MAC message types: PKMR Request (PKMR-REQ) and PKMR Response (PKMR-RSP), as described in Table xx1.

**Table xx1—PKMR MAC messages**

| Type Value | Message Name | Message Description |
|---|---|---|
| ?? | PKMR-REQ | Privacy Key Management – Remote Request [MSS→ BS] |
| ?? | PKMR-RSP | Privacy Key Management – Remote Response [BS→ MSS] |

These MAC management message types distinguish between PKMR requests (SS–to–BS) and PKMR responses (BS–to–SS). Each message encapsulates one EAP message in the Management Message Payload.

PKMR protocol messages transmitted from the SS to the BS (PKMR-REQ) shall use the form shown in Table xx2. They are transmitted on the MSSs Primary Management Connection.

**Table xx2—PKMR request (PKMR-REQ) message format**

| Syntax | Size | Notes |
|---|---|---|
| PKMR-REQ message format { | | |
| **Management Message Type = ??** | 8 bits | |
| **Target BSID** | 24 bits | Least significant 24 bits of the target BS ID |
| **Code** | 8 bits | |
| **PKMR identifier** | 8 bits | |
| **TLV Encoded Attributes** | *variable* | TLV specific |
| **OMAC/HMAC Tuple** | 23/16 | According to agreement in capabilities phase. This signature is calculated from keys used with the serving BS and will be verified by the serving BS |
| } | | |

PKMR protocol messages transmitted from the BS to the SS (PKMR-RSP) shall use the form shown in Table xx3. They are transmitted on the SSs Primary Management Connection.

**Table xx3—PKMR response (PKMR-RSP) message format**

| Syntax | Size | Notes |
|---|---|---|
| PKMR-REQ message format { | | |
| **Management Message Type = ??** | 8 bits | |
| **Source BSID** | 24 bits | Least significant 24 bits of the source BS ID |
| **Code** | 8 bits | |
| **PKMR identifier** | 8 bits | |
| **TLV Encoded Attributes** | *variable* | TLV specific |

| | | |
|---|---|---|
| **OMAC/HMAC Tuple** | 128 or 184 | According to agreement in capabilities phase. **This signature is for the serving BS and not the target BS** |
| } | | |

The parameters shall be as follows:

**Code**

The Code is one byte and identifies the type of PKMR packet. When a packet is received with an invalid Code, it shall be silently discarded. The code values are defined in Table xx4.

**PKMR Identifier**

The Identifier field is one byte. An SS uses the identifier to match a BS response to the SS's requests.

The SS shall increment (modulo 256) the Identifier field whenever it issues a new PKMR message. A "new" message is a PKMR-REQ that is not a retransmission being sent in response to a Timeout event. For retransmissions, the Identifier field shall remain unchanged.

The Identifier field in a BS's PKMR-RSP message shall match the Identifier field of the PKMR-REQ message the BS is responding to.

On reception of a PKMR-RSP message, the SS associates the message with a particular state machine (EAP stack for EAP messages).

**Attributes**

PKMR attributes carry the specific authentication, authorization, and key management data exchanged between client and server. Each PKMR packet type has its own set of required and optional attributes. Unless explicitly stated, there are no requirements about the order of attributes within a PKMR message. The end of the list of attributes is indicated by the LEN field of the MAC PDU header.

**Table xx4— PKMR message codes**

| Code | PKMR message types | MAC management message name |
|---|---|---|
| 0-12 | *Reserved* | - |
| 13 | EAP transfer | PKMR-REQ/PKMR-RSP |
| 24 | EAP start | PKMR-REQ |
| 25-255 | *Reserved* | - |

Formats for each of the PKMR messages are described in the following subclauses. The descriptions list the PKMR attributes contained within each PKMR message type. The attributes themselves are described in 11.9. Unknown attributes shall be ignored on receipt and skipped over while scanning for recognized attributes.
The BS shall silently discard all requests that do not contain ALL required attributes.

### 6.3.2.3.59.1 EAP Transfer message

When an MSS has an EAP message received from an EAP method for transmission to a remote BS or when a remote BS has an EAP message received from an EAP method for transmission to the MSS, it encapsulates it in an EAP Transfer message.

Code: 13

Attributes are shown in Table xx5.

**Table xx5 – EAP transfer attributes**

| Attribute | Contents |
|---|---|
| EAP protocol | Contains the EAP authentication data, not interpreted in the MAC |

The EAP Payload field carries data in the format described in section 4 of RFC2284bis

#### 6.3.2.3.63.2 EAP Start message

When an MSS has to initiate an authentication process with a BS, it sends an EAP start message.

Code: 24

This message has no attribute.

*[Add following two new MAC management messages in section 6.3.2.3]*

#### 6.3.2.3.60 Query HO context HO-BS-QRY

HO-BS-QRY is sent from MSS to BS before initiating HO in order to determine the current HO_Security_Context for the neighbor BS that is maintained by the serving BS.

| Syntax | Size | Notes |
|---|---|---|
| HO-BS-QRY{ | | |
| Management Message Type = ? | 8 bits | |
| Neighbor BSID | 48 bits | |
| HMAC/OMAC Digest | | Message Digest calculated using HMAC_KEY or OMAC_KEY |
| } | | |

Neighbor BSID : Identifies the BS for which HO_Security_Context information is being queried.

#### 6.3.2.3.61 Query HO context HO-BS-INF

HO-BS-INF is sent from BS to MSS in response to a HO-BS-QRY and contains the current HO_Security_Context for the neighbor BS that is maintained by the serving BS.

| Syntax | Size | Notes |
|---|---|---|
| HO-BS-INF{ | | |
| **Management Message Type = ?** | 8 bits | |
| **Neighbor BSID** | 48 bits | |
| **Authentication Zone** | 12 bits | Authentication zone Identifier for the BS |
| **Pre-authentication Support** | 1 bit | Capability bit for target BS |
| **MSS Authenticated** | 1 bit | Bit 0 : MSS Authenticated |
| *Reserved* | 2 bits | Must be zero |
| **HMAC/OMAC Digest** | | Message Digest calculated using HMAC_KEY or OMAC_KEY |
| } | | |

**Neighbor BSID**

Identifies the BS to which the information in HO_Security_Context belongs.

**Authentication Zone**

Specifies the authentication zone to which the neighbor BS belongs. The authentication zone of the neighbor may be the same as the serving BS transmitting this message.

**Pre-Authentication Support**

Specifies whether the neighbor BS supports the pre-authentication capability. If this bit is set, the MSS can do pre-authentication with the neighbor BS and generate a PMK for the authentication zone.

**MSS Authenticated**
0: MSS must do full authentication even if a valid AK exists.
1: Informs the MSS that there is no need to perform authentication and that AK may be derived from the existing PMK that the MSS and BS share or that an AK context already exists according to the circumstances.