| | | |
|---|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16> | |
| Title | **Security Zone Key management** | |
| Date Submitted | **2007-09-09** | |
| Source(s) | Sergey Seleznev, Hyoung Kyu Lim, Hyunjeong Kang, Jungje Son<br>Samsung Electronics<br>Rep. of Korea, Gyonggi-do, Suwon | Voice: +82312795968<br>E-mail: s.sergey@samsung.com |
| Re: | IEEE 802.16j-07/019 | |
| Abstract | This contribution proposes text changes to clarify SZK management and message authentication in MR system. | |
| Purpose | Discuss and adopt proposed text changes. | |
| 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 | 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 | The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<br><http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and<br><http://standards.ieee.org/guides/opman/sect6.html#6.3>.<br>Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>. | |

# Security Zone Key management

*Sergey Seleznev, Hyoung Kyu Lim, Hyunjeong Kang, Jungje Son*
*Samsung Electronics*

## Introduction

The following security functionality is missing from the current draft:

1. Group key for the uplink: sometimes RS may need to modify relayed unicast messages (e.g. DSA-REQ), however security context required for this operation is not distributed to intermediate RSs.
2. Key update procedures for multi-hop is not defined.

The following security functionality is not correctly defined in the current draft:

1. SZK key can not be used as GKEK, SZK key is not GKEK.

This contribution intends to clarify group key hierarchy and management based on P802.16Rev2/D0b.

## Group key management

### *Key hierarchy and derivation*

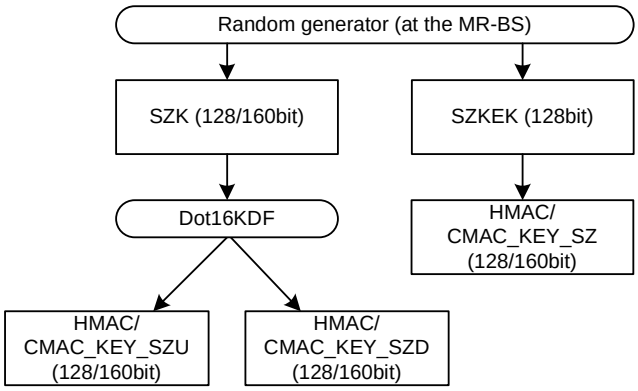


Fig.1: Security zone key hierarchy

To simplify Packet Number (PN) management two `keys are defined for message authentication: *_KEY_SZU and *_KEY_SZD for uplink (to BS) and downlink (from BS) message flows respectively. SZK is used for *_KEY_SZ* generation, and limits the number of key bits transmitted over the air interface. SZK Encryption Key (SZKEK) is used to encrypt SZK.

SZK_GN and SZKEK are randomly generated at the MR-BS. *_KEY_SZU, *_KEY_SZD and *_KEY_SZ are generated using Dot16KDF at the RS and MR-BS.

## *Key distribution and update*

Initial SZK and SZKEK have to be distributed during SA-TEK 3-way handshake. Consequent key updates can be performed using MBRA algorithm (with respect to P802.16Rev2/D0b) applied to multi-hop. Proposed text changes incorporate all the relevant procedures changes, mobile RS update mode, parameters and scenarios.

## *Proposed text*

[*Insert subclause 7.2.2.2.13*]

7.2.2.2.13 Security zone keys derivation

SZK and SKEK are randomly generated at the MR-BS. They are encrypted by RS's KEK using the same algorithms applied to AK encryption in a distributed security model, and transferred to RS during authorization phase, and updated periodically via relay multicast re-keying algorithm.

The security zone keys used for CMAC generation are derived as follows:

CMAC_KEY_SZU|CMAC_KEY_SZD<= Dot16KDF (SZK, "SECURITY_ZONE_KEYS", 256)

The security zone keys used for HMAC generation are derived as follows:

HMAC_KEY_SZU|HMAC_KEY_SZD<= Dot16KDF (SZK, "SECURITY_ZONE_KEYS", 320)

The CMAC_KEY_SZ used in SZK multicast update mode is derived as follows:
CMAC_KEY_SZ<= Dot16KDF (SZKEK, "SECURITY_ZONE_UPDATE_KEY", 128)

The HMAC_KEY_SZ used in SZK multicast update mode is derived as follows:
HMAC_KEY_SZ<= Dot16KDF (SZKEK, "SECURITY_ZONE_UPDATE_KEY", 160)

[*Change subclause 7.4.3*]

7.4.3 Security zone keys usage

The MR-BS shall generate, maintain and distribute relay security keys to RSs within a security zone. Relay security keys include Security Zone Key (SZK) and Security Zone Key Encryption Key (SZKEK). RS shall be capable to maintain two successive sets of relay security keys.

7.4.3.1 SZK usage

~~SZK is a group key shared by the MR-BS and a group of RS within the same security zone. The membership of the security zone (i.e., which security zone(s) a RS should be belong to) is determined by the MRBS The SZK is used to authenticate the MAC management messages transmitted over the relay links. The SZK is randomly generated by the MR-BS and used as the GKEK to compute the HMAC/CMAC as defined in section 7.2.2.2.9. SZK is distributed by the MR-BS to a RS after the RS gets authenticated during initial network entry, using the same key distribution procedure defined for the GKEK distribution.~~ SZK is used by the MR-BS and RS to derive security zone message authentication keys, i.e. HMAC/CMAC_KEY_SZU and HMAC/CMAC_KEY_SZD. SZK is updated periodically via relay multicast re-keying algorithm.

The MR-BS shall use HMAC/CMAC_KEY_SZD to generate MAC for the relay management messages (except for PKMv2 messages). The MR-BS shall use HMAC/CMAC_KEY_SZU to validate MAC of the relay management messages.

An RS shall use HMAC/CMAC_KEY_SZD to re-generate or validate MAC of the downlink relay management messages sent by the MR-BS (except for PKMv2 messages). An RS shall use HMAC/CMAC_KEY_SZU to re-generate or validate MAC of the relay management messages sent by this or other RS.

7.4.3.2 SZKEK usage

SZKEK shall be used by the MR-BS to encrypt SZK and authenticate PKMv2 Group-Key-Update-Command message in relay multicast re-keying algorithm SZK update mode. SZKEK is updated periodically via relay multicast re-keying algorithm.

SZKEK shall be used by the MR-BS and RS to derive a key for PKMv2 Group-Key-Update-Command message authentication in SZK update mode, i.e. HMAC/CMAC_KEY_SZ.

[*Insert the following subclause 7.5.2.6*]

7.5.2.6 Security zone keys encryption

SZK and SZKEK shall be encrypted with the cryptographic algorithm defined for TEK or AK encryption (dependent on the particular key length).

[*Delete subclause 7.2.2.2.9*]

~~7.2.2.2.9 Message authentication keys (HMAC/CMAC) and KEK derivation~~

~~MAC (message authentication code) keys are used to sign management messages in order to validate the authenticity of these messages. The MAC to be used is negotiated at SS Basic Capabilities negotiation. There is a different key for UL and DL messages. Also, a different message authentication key is generated for a multicast message (this is DL direction only) and for a unicast message.~~

~~In general, the message authentication keys used to generate the CMAC value and the HMAC Digest are derived from the AK.~~

~~The keys used for CMAC key and for KEK are as follows:~~

~~CMAC_KEY_U | CMAC_KEY_D | KEK <= Dot16KDF (AK, SS MAC Address | BSID | "CMAC_KEYS+KEK", 384)~~

~~CMAC_KEY_GD <= Dot16KDF(GKEK, "GROUP_CMAC_KEY",128) (Used for multicast MAC message such as a PKMv2 Group-Key-Update-Command message and downlink multicast MAC message sent from the MR-BS to the RSs within the same security zone)~~

~~The keys used for HMAC key and for KEK are as follows:~~

~~HMAC_KEY_U | HMAC_KEY_D | KEK <= Dot16KDF(AK, SS MAC Address | BSID |"HMAC_KEYS+KEK", 448)~~

~~HMAC_KEY_GD <= Dot16KDF(GKEK, “GROUP-HMAC-KEY”, 160) (Used for multicast MAC message such as a PKMv2 Group-Key-Update-Command message and downlink unicast MAC message sent between RSs within the same security zone)~~

~~HMAC_KEY_GU <= Dot16KDF (GKEK, "GROUP-HMAC-KEY", 128) (Used for uplink unicast MAC message sent between RSs within the same security zone).~~

~~Exceptionally, the message authentication keys for the HMAC/CMAC Digest included in a PKMv2 Authenticated- EAP-Transfer message are derived from the EIK instead of the AK. The keys used for CMAC key and for KEK are as follows:~~

~~CMAC_KEY_U | CMAC_KEY_D <= Dot16KDF (EIK, SS MAC Address | BSID | “CMAC_KEYS”, 256)~~
~~The keys used for HMAC key and for KEK are as follows:~~
~~HMAC_KEY_U | HMAC_KEY_D <= Dot16KDF (EIK, SS MAC Address | BSID | “HMAC_KEYS”, 320)~~

[*Insert the following subclause 7.8.4*]

7.8.4 Relay multicast re-keying algorithm

The relay multicast re-keying algorithm shall be used to update security zone keys on a multiple RSs.

The initial SZK and SZKEK distribution is performed by using the PKMv2 SA-TEK 3-way handshake. Once an RS shares the traffic keying material with the MR-BS, the MR-BS updates and distributes the traffic keying material periodically by sending PKMv2 Group-Key-Update-Command messages.

The MR-BS manages the SZK Grace Time. This parameter means time interval (in seconds) starting at the point when any UL or DL PN of a relay group key reached $PN_{lim}$. Length of a SZK Grace Time shall be shorter than time required for complete exhaustion of relevant packet number space.

The MR-BS manages the SZKEK Grace Time. This parameter means time interval (in seconds) before the estimated expiration of an old distributed GTEK.

The MR-BS distributes updated group key material by sending PKMv2 Group-Key-Update-Command messages before old distributed key is expired. Two message types are distinguished according to the included Key Push Modes.

The MR-BS transmits the PKMv2 Group-Key-Update-Command message for the SZKEK update mode in order to distribute the new SZKEK. Moreover, the MR-BS transmits the PKMv2 Group-Key-Update-Command message for the SZK update mode in order to distribute the new SZK.

In general, the SZKEK lifetime corresponds to the n (integer being bigger than 1) times of the SZK updates (i.e. the SZKEK shall be updated once while the SZK is updated n times). The MR-BS transmits the PKMv2 Group-Key-Update-Command message for the SZKEK update mode to each RS in a security zone before the current SZKEK expires and the last SZK Grace Time of the corresponding current SZKEK starts. The purpose of the PKMv2 Group-Key-Update-Command message for the SZKEK update mode is to distribute the SZKEK. The

PKMv2 Group-Key-Update-Command message for the GKEK update mode is carried on the Primary Management connection. The MR-BS intermittently transmits the PKMv2 Group-Key-Update-Command message for the SZKEK update mode to each RS in order to reduce the MR-BS's load in refreshing group key material. The SZKEK is needed to encrypt the new SZK.

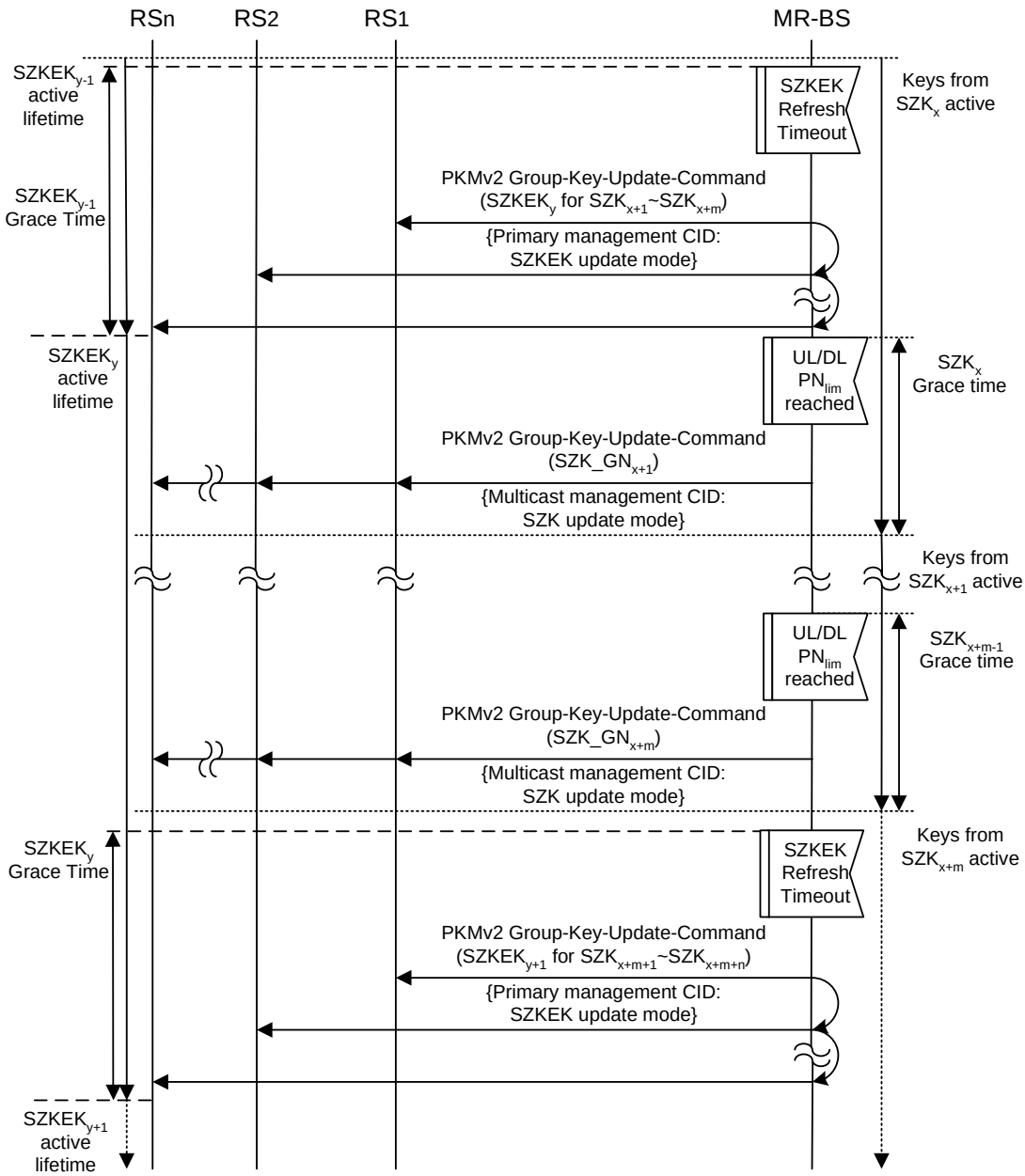


Figure ### - Relay multicast re-keying algorithm

The MR-BS transmits the PKMv2 Group-Key-Update-Command message for the SZK update mode carried on the multicast connection after the each SZK Grace Time starts. The aim of the Key Update Command PKMv2 Group-Key-Update-Command message for the GTEK update mode is to distribute new SZK to all RSs within a security zone.

If UL or DL PN at the RS expires and RS did not receive new SZK it shall perform reauthentication.

[*Insert the following subclause 7.8.4.1*]

7.8.4.1 MRS re-keying algorithm

In case a RS (i.e. MRS) leaves the security zone, security zone keys shall be updated. In order to avoid SZEK update mode in relay multicast re-keying algorithm, the MR-BS may not include SZKEK parameters during the PKMv2 SA-TEK 3-way handshake with MRS. If SZKEK parameters are omitted, the MR-BS shall always send the PKMv2 Group-Key-Update-Command in SZK update mode on primary management CID of MRS.

[*Insert the following subclause 7.8.1.1*]

7.8.1.1 PKMv2 SA-TEK-Response for RS

The PKMv2 SA-TEK-Response for RS shall also include security zone SAID and associated security zone keys. The SZK and SZKEK attributes contain all of the keying material corresponding to a particular generation of a security zone SAID. This would include the SZK, the SZKEK, the SZK's key sequence number, the associated SZKEK sequence number and the SZKEK's remaining lifetime. The SZKEK should be identically shared within the same security zone. Unlike the PKMv2 Group-Key-Update-Command, the SZK and SZKEK are encrypted with the negotiated TEK encryption algorithm because they are transmitted as a unicast messages.

[*Insert the following text at the end of 6.3.2.3.9.20*]

In MR, PKMv2 SA-TEK-Response message sent to RS shall include the following TLVs:

**SA_SZK_Update (see 11.1.11)**

TLV which specifies a security zone SAID and corresponding SZK, and SZKEK parameters.

[*Insert the following subclause 11.1.10*]

11.1.11 SA_SZK_Update Tuple

Table Xx – SZ_SZK_Update

| Name | Type | Length | Value | Scope |
|---|---|---|---|---|
| SA-SZK-Update | TBD | *variable* | See Table Xx | PKM-RSP, REG-RSP |

Table Xx – SA_SZK_Update definition

| Field | Length (bits) | Note |
|---|---|---|
| SAID | 16 | Security zone Security Association Identifier |
| SZK-Parameters | *variable* | Security Zone Key related parameters |
| SZKEK-Parameters (optional) | *variable* | Security Zone Key Encryption Key related parameters |

[*Change Table 77 at subclause 6.3.2.3.9.26 as indicated*]

**Table 77—PKMv2 Group-Key-Update-Command message attributes**

| Attribute | Contents |
|---|---|
| Key Sequence Number | AK sequence number for GKEK/SZKEK update mode, GKEK/SZKEK sequence number for GTEK/SZK update mode |
| GSAID | Security association identifier |
| Key Push modes | Usage code of PKMv2 Group-Key-Update-Command message.<br>In MR, GTEK update mode corresponds to SZK update mode, and GKEK update mode corresponds to SZKEK update mode. |
| Key Push Counter | Counter one greater than that of older generation |
| GTEK/SZK-Parameters | "Newer" generation of GTEK-related parameters relevant to GSAID. The GTEK-Parameters is the TEK-Parameters for multicast, broadcast service, or MBS.<br>In MR, SZK-related parameters relevant to security zone SAID. |
| GKEK/SZKEK-Parameters | "Newer" generation of GKEK-related parameters for multicast, broadcast service, or MBS.<br>In MR, SZKEK-related parameters relevant to SAID for encrypting SZK. |
| HMAC/CMAC Digest | Message integrity code of this message |

[Insert the following subclause 11.9.40]

11.9.40 SZK-Parameters

This attribute is a compound attribute, consisting of a collection of sub-attributes. These sub-attributes represent all the security parameters relevant to a particular generation of SZK.

| Type | Length | Value |
|---|---|---|
| TBD | *variable* | The compound field contains the sub-attributes as defined in the Table Xx. |

**Table Xx—SZK-Parameters definition**

| Field | Length (bits) | Note |
|---|---|---|
| SZK | *variable* | Security Zone Key encrypted with KEK derived from AK |
| SZK Sequence Number | 4 | SZK Sequence Number |

[*Insert the following subclause 11.9.41*]

11.9.41 SZKEK-Parameters

This attribute is a compound attribute, consisting of a collection of sub-attributes. These sub-attributes represent all the security parameters relevant to a particular generation of SAID for encrypting SZK.

| Type | Length | Value |
|---|---|---|
| TBD | *variable* | The compound field contains the sub-attributes as defined in the Table Xx. |

**Table Xx—SZKEK-Parameters definition**

| | | |
|---|---|---|
| SZKEK | 128 | Security Zone Key Encryption Key |
| SZKEK Sequence Number | 8 | SZKEK Sequence Number |
| SZKEK Lifetime | - | SZKEK remaining lifetime |

SZKEK remaining lifetime is an integer *n*, which corresponds to a number of remaining SZK updates under this SZKEK.