### IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Detailed text proposal on Trigger, BA, BAR Protection | | | | |
| Date: 2024-12-04 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  |  |
| Ido Ouzieli |  |  |  |
| Danny Alexander |  |  |  |
| Danny Ben-Ari |  |  |  |
| Johannes Berg |  |  |  |
| Laurent Cariou |  |  |  |
| Alfred Asterjadhi | Qualcomm |  |  |  |
| Abhisehek Patil |  |  |  |
| Liwen Chu | NXP |  |  |  |
| Li-Hsiang Sun | Mediatek |  |  |  |
| Nehru Bhandaru | Broadcom |  |  |  |
| Yanjun Sun | Apple |  |  |  |
| Jarkko Kneckt |  |  |  |

Abstract

The authors prepared this document to give a better view of the different proposals on Control frame protection in text format. The authors look forward to working with all interested participants to prepare an official proposal for specification text on Trigger, BA, BAR protection.

Revisions:

* Rev 0: Initial version of the document.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbn Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbn Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbn Editor: Editing instructions preceded by “TGbn Editor” are instructions to the TGbn editor to modify existing material in the TGbn draft. As a result of adopting the changes, the TGbn editor will execute the instructions rather than copy them to the TGbn Draft.***

***TGbn editor: Add new acronyms in 3.4 as follows:***

**3.4 Acronyms and abbreviations**

CIGTK control integriy group temporal key

***TGbn editor: Modify 9.3.1.7.1 as follows: (Track change on)***

* BlockAckReq frame format
* Overview

The frame format of the BlockAckReq frame is defined in Figure 9-46 (BlockAckReq frame format).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Frame  Control | Duration | RA | TA | BAR  Control | BAR  Information | Control MIC | Padding | FCS |
| Octets: | 2 | 2 | 6 | 6 | 2 | variable | 0 or 22 | variable | 4 |
| * BlockAckReq frame format | | | | | | | | | |

  The Duration field value is set as defined in 9.2.5 (Duration/ID field (QoS STA)).

The RA field of the BlockAckReq frame is the address of the recipient STA.

The TA field(#3522) is the address of the STA transmitting the BlockAckReq frame or a bandwidth signaling TA. In a BlockAckReq frame transmitted by a VHT STA or an HE STA(11ax) in a non-HT or non-HT duplicate format and where the scrambling sequence carries the TXVECTOR parameter CH\_BANDWIDTH\_IN\_NON\_HT, the TA field(#3522) is a bandwidth signaling TA.

The BAR (for block acknowledgment request) Control field is shown in Figure 9-47 (BAR Control field format(11ax)).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | B0 | | B1 B4 | B5 | B6 | B7 B11 | B12 B15 |
|  | | Reserved | | BAR Type | Protected Control | Key ID | Reserved | TID\_INFO |
| Bits: | | 1 | | 4 | 1 | 1 | 5 | 4 |
|  |  | | * BAR Control field format(11ax) | | | | | |

 (11ax)The BAR Type subfield indicates the BlockAckReq frame variant, as defined in Table 9-36 (BlockAckReq frame variant encoding(11ax)).

|  |  |
| --- | --- |
| * BlockAckReq frame variant encoding(11ax) | |
| BAR Type | BlockAckReq frame variant |
| 0 | Reserved |
| 1 | Extended Compressed |
| 2 | Compressed |
| 3 | Multi-TID |
| 4–5 | Reserved |
| 6 | GCR |
| 7–9 | Reserved |
| 10 | GLK-GCR |
| 11–15 | Reserved |

DMG STAs use only the Compressed BlockAckReq variant and the Extended Compressed BlockAckReq variant.

If protection for control frame is negotiated, the Protected Control subfield is set to 1 if the BlockAckReq frame contains information that has been processed with a message integrity check algorithm and is set to 0 if the BlockAckReq frame does not contain information that has been processed with a message integrity check algorithm. Otherwise, the Protected Control subfield is reserved.

The Protected Control subfield is reserved in all BlockAckReq variants except for Compressed BlockAckReq and Multi-TID BlockAckReq (TBD whether allowed for other variants). When the Protected Control subfield is equal to 1, the BlockAckReq is protected utilizing the message integrity check algorithm as defined in clause 12.5.X (Control frame integrity protocol (CIP).

The Key ID subfield contains the key ID when the Protected Control subfield is 1. Otherwise, the Key ID subfield is reserved.

The meaning of the TID\_INFO subfield of the BAR Control field depends on the BlockAckReq frame variant type. The meaning of this subfield is explained within the subclause for each of the BlockAckReq frame variants.

The meaning of the BAR Information field of the BlockAckReq frame depends on the BlockAckReq frame variant type. The meaning of this field is explained within the subclause for each of the BlockAckReq frame variants.

NOTE—Reference to “a BlockAckReq” frame without any other qualification from other subclauses applies to any of the variants, unless specific exclusions are called out.

The Control MIC field provides integrity protection for the BlockAckReq frame. The Control MIC field is present if the Protected Control subfield is equal to 1; Otherwise, the Control MIC field is not present.

The format of the Control MIC field is shown in Figure 9.XY (Control MIC field format).

|  |  |  |
| --- | --- | --- |
|  | PN | MIC |
| Octets: | 6 | 16 |

Figure 9-XY----Control MIC field format

The PN subfield contains the PN corresponding to the integrity key indicated by the Key ID subfield.

The MIC subfield contains a message integrity check calculated over the BlockAckReq frame as defined in 12.5.x (Control frame integrity protocol (CIP)).

The Padding field is optionally present in the BlockAckReq frame to extend the frame length to give the recipient STA enough time to perform message integrity check and to prepare the response for transmission a SIFS after the frame is received and validated.

***TGbn editor: Modify 9.3.1.8.1 as follows: (Track change on)***

**9.3.1.8.1 Overview**

(texts to include key ID, PN, MIC, and padding)

……

The BA Control field is defined in Figure 9-53 (BA Control field format(11ax)(11ay)).

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0 | | B1 B4 | | B5 | B6 | B7 B8 | B9 | B10 | B11 | B12 B15 |
|  | Reserved | | BA Type | | Protected Control | Key ID | Reserved | No Memory Kept | Memory Configuration Tag | Management Ack | TID\_INFO |
| Bits: | 1 | | 4 | | 1 | 1 | 2 | 1 | 1 | 1 | 4 |
|  | |  | | * BA Control field format(11ax)(11ay) | | | | | | | |

(11ax)The BA Type subfield in the BA Control field indicates the BlockAck frame variant, as defined in (#6291) Table 9-37 (BlockAck frame variant encoding(11ax)).

|  |  |
| --- | --- |
| * BlockAck frame variant encoding(11ax) | |
| BA Type | BlockAck frame variant |
| 0 | Reserved |
| 1 | Extended Compressed |
| 2 | Compressed |
| 3 | Reserved(#6599) |
| 4–5 | Reserved |
| 6 | GCR |
| 7(11ay) | EDMG Multi-TID |
| 8(11ay) | EDMG Compressed |
| 9(11ay) | Reserved |
| 10 | GLK-GCR |
| 11 | Multi-STA |
| 12–15 | Reserved |

NOTE—Reference to “a BlockAck” frame without any other qualification from other subclauses applies to any of the variants, unless specific exclusions are called out.

The GCR BlockAck frame is used in response to a GCR BlockAckReq frame, and the GLK-GCR BlockAck frame is used in response to a GLK-GCR BlockAckReq frame.(11ax)

If protection for control frame is negotiated, the Protected Control subfield is set to 1 in a Multi-STA BlockAck frame to indicate that the frame is protected and is set to 0 in a Multi-STA BlockAck frame to indicate that the frame is not protected. Otherwise the Protected Control subfield is reserved.

The Key ID subfield in a Multi-STA BlockAck frame with Protected Control subfield equal to 1 indicates the Key being used to protect the Multi-STA BlockAck frame. Otherwise the Key ID subfield is reserved.

……

***TGbn editor: Modify 9.3.1.8.6 as follows: (Track change on)***

**9.3.1.8.6 Multi-STA BlockAck variant**

(texts to include key ID, PN, MIC, and padding)

……

If the AID11 subfield of the AID TID Info subfield is neither 2045, 2009, nor 2010, then the Per AID TID Info subfield has the format shown in Figure 9-60 (Per AID TID Info subfield format if the AID11 subfield is neither 2045(11ax), 2009, nor 2010).

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | AID TID Info | Block Ack Starting Sequence Control | Block Ack Bitmap |
| Octets: | 2 | 0 or 2 | 0, 4, 8, 16 or 32 |
| * Per AID TID Info subfield format if the AID11 subfield is neither 2045(11ax), 2009, nor 2010 | | | |

If the AID11 subfield of the AID TID Info subfield is equal to 2009, then the Per AID TID Info subfield has the format shown in Figure 9-XX (Per AID TID Info subfield format if the AID11 subfield is equal to 2009). The Per AID TID Info field with the value in AID11 subfield equal to 2009 is after other Per AID TID Info fields in the Multi-STA BlockAck frame with AID11 not equal to 2010. The Starting Sequence Number subfield of the Block Ack Starting Sequence Control subfield is reserved. The Fragment Number subfield of the Block Ack Starting Sequence Control subfield follows the indication of the Block Ack Bitmap subfield length in Table 9-40 (Fragment Number subfield encoding for the Multi-STA BlockAck variant) to indicate the length of the PN And MIC subfield.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | AID TID Info | Block Ack Starting Sequence Control | PN And MIC |
| Octets: | 2 | 2 | 32 |

Figure 9-XX----Per AID TID Info subfield format if the AID11 subfield is equal to 2009

The PN And MIC subfield has the format shown in Figure 9-XX (PN And MIC subfield format).

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | PN | MIC | Reserved |
| Octets: | 6 | 16 | 10 |

Figure 9-XX----PN And MIC subfield format

If the AID11 subfield of the AID TID Info subfield is equal to 2010, then the Per AID TID Info subfield has the format shown in Figure 9-XX (Per AID TID Info subfield format if the AID11 subfield is equal to 2010). The Per AID TID Info field(s) with the value in AID11 subfield equal to 2010 is after other Per AID TID Info field in the Multi-STA BlockAck frame with AID11 not equal to 2010. The Starting Sequence Number subfield of the Block Ack Starting Sequence Control subfield is reserved. The Fragment Number subfield of the Block Ack Starting Sequence Control subfield follows the indication of the Block Ack Bitmap subfield length in Table 9-40 (Fragment Number subfield encoding for the Multi-STA BlockAck variant) to indicate the length of the Padding subfield.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | AID TID Info | Block Ack Starting Sequence Control | Padding |
| Octets: | 2 | 2 | 0, 4, 8, 16, or 32 |

Figure 9-XX----Per AID TID Info subfield format if the AID11 subfield is equal to 2010

If the AID11 subfield is not 2045, then the context and the presence of each optional subfield in a Per AID TID Info subfield in a Multi-STA BlockAck frame is defined in Table 9-39 (Context of the Per AID TID Info subfield and presence of optional subfields if the AID11 subfield is not 2045(11ax)).

|  |  |  |  |
| --- | --- | --- | --- |
| * Context of the Per AID TID Info subfield and presence of optional subfields if the AID11 subfield is not 2045(11ax) | | | |
| Ack Type subfield values | TID subfield values | Presence of Block Ack Starting Sequence Control subfield and Block Ack Bitmap subfields | Context of a Per AID TID Info subfield in a  Multi-STA BlockAck frame |
| 0 | 0–7 | Present | Block acknowledgment context:  Sent as an acknowledgment to QoS Data frames that solicit a BlockAck frame response or to a BlockAckReq frame. |
| 1 | 0–7 | Not present | Acknowledgment context:  Sent as an acknowledgment to a QoS Data or QoS Null frame that solicits an Ack frame response. |
| 0 or 1 | 8–13 | N/A | Reserved |
| 0 | 14 | N/A | Reserved |
| 0 | Reserved | Present | PN and MIC context if AID11 subfield is equal to 2009  Padding context if AID11 subfield is equal to 2010 |
| 1 | 14 | Not present | All ack context:  Sent as an acknowledgment to an A-MPDU that contains an MPDU that solicits an immediate response and all MPDUs contained in the A-MPDU are received successfully. |
| 0 | 15 | N/A | Reserved |
| 1 | 15 | Not present | Management/PS-Poll frame acknowledgment context:  Sent as an acknowledgment to a Management or PS-Poll frame. |
| NOTE 1—Additional rules for acknowledgment, block acknowledgment and the all ack context are defined in 26.4.2 (Acknowledgment context in a Multi-STA BlockAck frame) for a multi-TID A-MPDU.  NOTE 2—As HE STAs do not use HCCA (see 10.23.1 (General)), TID values from 8 to 15 are not used in QoS Data frames. | | | |

NOTE – To preserve backward compatibility, when the AID11 subfield is equal to 2009 or 2010, the reserved TID subfield that is used in the future to indicate other values can not indicate a value more than 7.

……

***TGbn editor: Modify 9.3.1.22.1 as follows: (Track change on)***

* **Trigger frame format(11ax)**
* **General**

A Trigger frame allocates resources for and solicits one or more HE TB PPDU transmissions. The Trigger frame also carries other information required by the responding STA to send an HE TB PPDU.

The format for the Trigger frame is defined in Figure 9-90 (Trigger frame format(11ax)(#1097)).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | | |  |  |  |  |
|  | Frame Control | Duration | RA | TA | Common Info | User Info List | Padding | FCS |
| Octets: | 2 | 2 | 6 | 6 | 8 or more | variable | variable | 4 |
| * **Trigger frame format(11ax)(#1097)** | | | | | | | | |

The Duration field is set as defined in 9.2.5 (Duration/ID field (QoS STA)).

The RA field is set as follows:

* For a Trigger frame that is not a GCR MU-BAR, NFRP or MU-RTS Trigger frame, and that has one User Info field and the AID12 subfield of the User Info field contains the AID of a non-AP STA, the RA field is set to the address of that STA
* For a Trigger frame that has at least one User Info field with the AID12 subfield that allocates an RA-RU, the RA field is set to the broadcast address
* For a Trigger frame that is not a GCR MU-BAR Trigger frame and that has more than one User Info field, the RA field is set to the broadcast address
* For a Trigger frame that is an NFRP Trigger frame or MU-RTS Trigger frame, the RA field is set to the broadcast address
* For a Trigger frame that is a GCR MU-BAR Trigger frame, the RA field is set to the MAC address of the group for which reception status is being requested

The TA field is the address of the STA transmitting the Trigger frame if the Trigger frame is addressed to STAs that belong to a single BSS. The TA field is the transmitted BSSID if the Trigger frame is addressed to STAs from at least two different BSSs of the multiple BSSID set. The rules for setting of the TA field are defined in 26.5.2.2.4 (Allowed settings of the Trigger frame fields and TRS Control subfield).

The Common Info field is defined in Figure 9-91 (Common Info field format(11ax)).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0    B3 | B4   B15 | B16 | B17 | B18 B19 | B20   B21 | B22 | B23                B25 |
|  | Trigger Type | UL Length | More TF | CS Required | UL BW | GI And HE-LTF Type | MU-MIMO HE-LTF Mode | Number Of HE-LTF Symbols And Midamble Periodicity |
| Bits: | 4 | 12 | 1 | 1 | 2 | 2 | 1 | 3 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | B26 | B27 | B28   B33 | B34   B35 | B36 | B37    B52 | B53 | B54    B62 |
|  | UL STBC | LDPC Extra Symbol Segment | AP Tx Power | Pre-FEC Padding Factor | PE  Disambiguity | UL Spatial Reuse | Doppler | UL HE-SIG-A2 Reserved |
| Bits: | 1 | 1 | 6 | 2 | 1 | 16 | 1 | 9 |

|  |  |  |
| --- | --- | --- |
|  | B63 |  |
|  | Reserved | Trigger Dependent Common Info |
| Bits: | 1 | variable |
| * **Common Info field format(11ax)** | | |

The Trigger Type subfield identifies the Trigger frame variant and its encoding is defined in Table 9-47 (Trigger Type subfield encoding(11ax)).

|  |  |
| --- | --- |
| * **Trigger Type subfield encoding(11ax)** | |
| **Trigger Type subfield value** | **Trigger frame variant** |
| 0 | Basic |
| 1 | Beamforming Report Poll (BFRP) |
| 2 | MU-BAR |
| 3 | MU-RTS |
| 4 | Buffer Status Report Poll (BSRP) |
| 5 | GCR MU-BAR |
| 6 | Bandwidth Query Report Poll (BQRP) |
| 7 | NDP Feedback Report Poll (NFRP) |
| 8(11az) | Ranging |
| 9–15 | Reserved |

The UL Length subfield of the Common Info field indicates the value of the L-SIG LENGTH field of the solicited HE TB PPDU.

….

If protection for control frame is negotiated, the Protected Control subfield is set to 1 if the Trigger frame contains information that has been processed with a message integrity check algorithm and is set to 0 if the Trigger frame does not contain information that has been processed with a message integrity check algorithm. Otherwise, the Protected Control subfield is reserved. The Protected Control field is present in the UHR variant Common Info field. TBD whether the Protected Control field is present in other variants of the Common Info field.

The Protected Control subfield is reserved in all variants of the Common Info field contained in a Trigger frame that is sent by a STA that does not support protected control frames. When the Protected Control subfield is equal to 1, the Trigger frame is protected utilizing the message integrity check algorithm as defined in clause 12.5.X (Control frame integrity protocol (CIP).

The Key ID subfield contains the key ID when the Protected Control subfield is 1. Otherwise, the Key ID subfield is reserved.

The location of the Protected Control and Key ID subfields in the UHR Common Info field is TBD.

The Control MIC field provides integrity protection for the Trigger frame. The Control MIC field is present if the Protected Control subfield is equal to 1; Otherwise, the Control MIC field is not present. The location and the encoding of the Control MIC field in the Trigger frame is TBD (i.e., it is TBD as to whether the Control MIC field is carried within multiple User Info fields or within the Padding field of the Trigger frame.).

The format of the Control MIC field is shown in Figure 9.XY (Control MIC field format).

|  |  |  |
| --- | --- | --- |
|  | PN | MIC |
| Octets: | 6 | 16 |

Figure 9-XY----Control MIC field format

The PN subfield contains the PN corresponding to the integrity key indicated by the Key ID subfield.

The MIC subfield contains a message integrity check calculated over the Trigger frame as defined in 12.5.x (Control frame integrity protocol (CIP)).

***TGbn editor: Add new clause at the end of 12.5 as follows:***

**12.5.x Control frame integrity protocol (CIP)**

**12.5.x.1 Overview**

CIP provides integrity and replay protection for the following control frames:

* Individually and group addressed Trigger frame
* Individually and group addressed Multi-STA BA frame
* Individually addressed Compressed BAR frame
* Individually addressed Multi-TID BAR frame
* Other variants of BAR frames to be protected are TBD

GMAC-256 is used for CIP.

If CIP is used, then GCMP-256 shall be used as the pairwise cipher for individually addressed data and management frame. Also, TBD most significant bits of PN for protecting individually addressed data and management shall not be set to all 1.

CIP uses TK to compute the MIC of individually addressed control frame that are defined to be protected.

CIP uses CIGTK delivered by the AP to compute MIC of group addressed Control frames that are defined to be protected. In a multiple BSSID set, all APs in the multiple BSSID set deliver the same CIGTK. An UHR STA shall only use a protected Multi-STA BA to provide acknowledgement of an individually addressed frame that solicits an acknowledgement to another UHR STA if the UHR STAs have negotiated protection for control frame that are defined to be protected.

**12.5.x.2 Encapsulation format**

To provide integrity and replay protection, CIP utilizes 1 bit Key ID field, 6 bytes PN field, and 16 bytes MIC field in the control frame that are defined to be protected.

The frame format is described in 9.3.1.22 (Trigger frame format), 9.3.1.7 (BlockAckReq frame format), and 9.3.1.8 (BlockAck frame format).

**12.5.x.3 CIP AAD construction**

The CIP Additional Authentication Data (AAD) is constructed from the control frame header. AAD construction is performed as follows without any bits masked out:

* Frame Control field
* Duration field
* RA field
* TA field

Figure 12-xx (CIP AAD construction) depicts the format of the AAD.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Frame Control | Duration | RA | TA |
| Octets: | 2 | 6 | 6 | 6 |

Figure 12-xx—CIP AAD construction

**12.5.x.4 Replay counters and packet numbers**

When CIP is negotiated between an AP MLD and a non-AP MLD:

* each non-AP STA affiliated with the non-AP MLD and each AP affiliated with the AP MLD shall maintain a PN for protecting individually addressed control frame. The PN shall be implemented as a 48-bit strictly increasing integer by each non-AP STA affiliated with the non-AP MLD independently and by each AP affiliated with the AP MLD independently. TBD most significant bits of the PN are set to all 1.
* each non-AP STA affiliated with the non-AP MLD and each AP affiliated with the AP MLD shall maintain a 48-bit replay counter to check replay of individually addressed control frame that are defined to be protected
* each AP affiliated with the AP MLD shall maintain a PN for each CIGTK. The PN shall be implemented as a 48-bit strictly increasing integer, initialized to 1 when the corresponding CIGTK is initialized. A single PN space is maintained for all APs in a multiple BSSID set.
* each non-AP STA affiliated with the non-AP MLD shall maintain a 48-bit replay counter for each CIGTK.

**12.5.x.5 Transmission**

When a STA transmits a control frame that is defined to be protected, it shall

1. Select the TK (if the control frame is individually addressed) or CIGTK (if the control frame is group addressed) currently active for transmission of individually addressed control frames or group addressed control frames
2. The Key ID field set to the corresponding key ID. The PN field set to the corresponding PN. The nonce, i.e., the initialization vector, shall be a concatenation of TA field and the non-negative integer inserted into the PN field.
3. Compute AAD as specified in 12.5.x.3 (CIP AAD construction).
4. Compute an integrity value over the concatenation of AAD and contents after TA field and before MIC field. Insert the output into the MIC field.
5. Transmit the frame.

**12.5.x.6 Reception**

When a STA receives a control frame that is defined to be protected, it shall

1. Identify the appropriate TK (if the control frame is individually addressed) or CIGTK (if the control frame is group addressed) and associated state based on the Key ID field. If no such TK or CIGTK exists, silently discard the frame and terminate CIP processing for this reception.
2. Perform replay protection on the received frame. The receiver shall interpret the PN field as a 48-bit unsigned integer. The receiver shall compare the PN to the value of the corresponding replay counter identified by the Key ID field. If the value from the received PN field is

less than or equal to the replay counter value, the receiver shall discard the frame

and increment the dot11RSNACIPStatsReplays counter by 1.

1. The nonce, i.e., the initialization vector, shall be a concatenation of TA field and the non-negative integer inserted into the PN field.
2. Compute AAD as specified in 12.5.x.3 (CIP AAD construction).
3. Extract and save the received MIC value, and compute a verifier over the concatenation of AAD and contents after TA field and before MIC field. If the computed verifier does not match the received MIC value, then the receiver shall discard the frame, increment the dot11RSNAStatsCIPMICErrors counter by 1, and terminate CIP processing for this reception.
4. Update the corresponding replay counter identified by the Key ID field with the value of the PN field.