IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)
Title	**TG3 LB12 St. Louis comment resolution**
Date Submitted	[8 July, 2002]
Source	[James P. K. Gilb] [Appairent Technologies] [9921 Carmel Mountain Rd. #247, San Diego, CA 92129] Voice: [858-538-3903] Fax: [858-538-3903] E-mail: [gilb@ieee.org]
Re:	[]
Abstract	[This document is a record of comment resolutions for LB17.]
Purpose	[To provide a record of the comment resolution for LB17.]
Notice	This document has been prepared to assist the IEEE P802.15. 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 acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15.

1. Comment resolution in Vancouver

1.1 MLME policy

— Change MLME-CREATE-CTA parameters to pass only those things needed to verify the functioning of the standard. Since the channel time parts are not going to be verified, only that a CTA.

1.2 Channel time management (CTM/Async*, CTM/Isoch*)

IDs: 15, 16, 34, 368, 813, 370, 614, 195, 906, 652, 914, 907, 917, 155, 20, 21, 411, 364, 366, 120, 410.

For asynchronous data, initial command comes from FCSL via MAC SAP with the MAC-ASYNC-DATA.request. Then the DEV MLME decides if it needs more time (hexagon decision). If so, it sends the frame over the air. The PNC MLME decides what to do and in the case of rejection responds with channel time status command, otherwise it is a beacon. Neither the PNC DME nor the DEV-2 DME are involved.

Asyncrhonous termination: Do we allow the destination to terminate. PNC is allowed to terminate and the source is allowed to terminate (this simply means that it sets the request to zero).

Now we don’t need MLME-CREATE-CTA.indication or MLME-CREATE-CTA.response, just let the PNC MLME do the response over the air.

Note: Perhaps we want to rename MLME-xxx-CTA to be MLME-xxx-STREAM?

For the ResultCodes on negative actions, allow timeout but do not refer to it as unsuccessful. 20, 21, 411. But should apply also to disassociation and deauthentication.

Beacon confirmation of synchronous request. Suggest stream creation information element. IDs 123, which really is a reference to [06] in 02/276r0. Asked for straw poll, do we require ACK before building the beacon, result was 4/1/5 (y/n/a). So action is for WMS to create new text in 8.5.1.1, page 175, line 50 that indicates this and send it to the reflector by COB 10 July 2002.

Resolution for 123: Accept in principle: Don’t use new IE, other edits that will be made are (based on 02/276r0 notation):

8.5 Channel Time management, <Page 175, line 3, TR> Accept as written

8.5.1 Isochronous Stream management, <Page 175, line 13-15, Editorial> Accept as written.

<Page 175, line 19-20, TR> (needs work, but seems like the right direction)

<Page 175, line 24, Ed> Accept as written.

8.5.1.2 Isochronous stream modification, <change two last bullets , TR>

Change to implement:

— The CTR type field shall be set to the same value as in the original request for that stream index.
— All the other channel time request command parameters are set to appropriate values as defined in 7.5.5.1.
— ~~Minimum number of TUs field is set to either the original value requested or a new value if the DEVs requirements have changed.~~

- ~~Desired number of TUs field is set to a value that is greater than or equal to the minimum number of TUs.~~

Note: This allows a DEV to change from every beacon to subrate and vice-versa. Does this cause enough problems that we should require a tear-down and re-establishment?

<page 177, line 46, TR> Accept as written.

Figure 115 – MSC for modifying a stream <revert to old, TR> Accept as written

8.5.1.3 Isochronous stream termination, <Page 179, line 40-42, TR > Withdraw this issue.

Figure 117 – MSC of source DEV-2 requesting termination of its stream <TR>: Withdraw this issue.

New issue: Make sure that we mention somewhere that only the source or the PNC of a broadcast or multicast stream shall be able to terminate the stream. Page 179, line 30, Add text “In the case of multicast or broadcast streams, only the source DEV or the PNC may terminate the stream.”

Figure 118 – MSC for a target DEV-2 disassociating causing a source DEV-3 stream termination <delete whole MSC, TR>. Accept as written, also delete lines 23-24 on page 180. Add text that says “When either the source or destination of a stream is disassociated from the network the streams are terminated as indicated in {xref disassociation}.

8.5.2.1 Asynchronous channel time creation and modification reservation <Page 181, line 26, TR> Accept as written.

<Page 181, line 37, TR> Change “and the same destination” to be “and the same source”

<Page 181, line 40, E> JPKG to check grammar, otherwise it is probably OK.

<Page 181, line 49, E> Accept as written.

Figure 119 – MSC for reserving asynchronous data channel time. Discussed earlier, new MSC is below:

8.5.2.1 Asynchronous GTS termination: Change it to only allow the source and PNC to terminate.

Change “Only the PNC, the originating DEV, or the target DEV shall be able to” to be “Only the PNC or the originating DEV may

1.3 Child/neighbor handover (

1.4 Transmission sequence resync

Duh, delete it. Resolves comments from Gilb, Heberling and Shvodian IDs ???.

2. Status at closing in Vancouver

a) Ballot resolution committee formed, members are:
b)

.

Table 1—Ballot resolution as of close of St. Louis meeting

Type	LB17	Unresolved as of 12 July, 2002
T (technical)	131	?
TR (Technical required)	444	?
T and TR	575	?
E (editorial)	622	?
Total	1197	?

3. Suggested resolutions from JPKG

3.1 Clause 6 comments.

Comment (TR): (Clause 6, multiple locations) When the device is operating in security modes 1, 2 or 3, the MLME needs to be able to indicate to the DME what type of protection is used on a given received frame so that the DME can decide whether or not to accept the frame. This is important because some devices may want to choose to send unprotected frames to certain other devices and the DME needs to be able to determine whether its policy allows it to accept those frames. An indication needs to be added to each MLME.indication and each MLME.confirm in Clause 6, which indicates that a frame is received from another DEV, specifying whether the frame had security turned on and whether the frame came from a device in the ACL.

Author’s note: The interfaces for the above described MLME messages should add the following entries to the semantics tables:

```
MLME-XXX.indication (or .confirm)    (
                                     SecurityUse,
                                     ACLEntry
                                     )
```

Author’s note: The following table entries should be added to the above described MLME messages.

Table 2—MLME-XXX.indication (or MLME-XXX.confirm) parameters

Name	Type	Valid Range	Description
SecurityUse	Boolean	TRUE or FALSE	This indicates to the DME if the received data frame had the security suite applied to it.
ACLEntry	Boolean	TRUE or FALSE	This indicates to the DME if the sender was found in the ACL.

Comment (TR): (Clause 6, multiple locations) Devices need to have the capability of choosing when to send frames with security and when not to. The decision for when to send a frame with security and what key to use should be determined by the DME. An indication needs to be added to each MLME.request and MLME.response in Clause 6, which cause the DEV to send a frame to another DEV, specifying whether that frame should be protected by security.

Author’s note: The interfaces for the above described MLME messages should add the following entry to the semantics tables:

```
MLME-XXX.request (or .response)    (
                                   KeySelection
                                   )
```

Author’s note: Insert the following entry into Table 61 on page 86:

Table 3—MLME-GTS.request parameters

Name	Type	Valid Range	Description
KeySelection	Enumeration	PICONET-MGMT, PICONET-DATA, PEER-MGMT, PEER-DATA, NONE	Specifies the key that shall be used to protect the outgoing frame or that security shall not be used on the frame.

Comment (TR): (Clause 6) When devices are running in a secure mode, they need to be able to indicate to the DME when frames received or frames being sent cause security operation failures. These security operation failures could be caused by not having the specified key or by a failed integrity check or some other cryptographic failure.

Author’s note: The following sub-clause should be added to Clause 6 to support the above comment.

3.1.1 Security management primitives

These primitives define how the MLME communicates security related events to the DME.

3.1.1.1 MLME-SECURITY-ERROR.indication

This primitive allows the MLME of any DEV to indicate a failed security processing operation to the DME.

3.1.1.1.1 Semantics of the service primitive

This primitive shall provide the following interface:

```
MLME-SECURITY-ERROR.indication (
                                    SrcID,
                                    DestID,
                                    SECID,
                                    ReasonCode
                                    )
```

Table 4 specified the parameters for the MLME-SECURITY-ERROR.indication primitive.

Table 4—MLME-SECURITY-ERROR.indication parameters

Name	Type	Valid Range	Description
SrcID	Integer	Any valid DEVID as defined in 7.2.3{xref}	The DEVID of the entity from which the frame causing the error originated.
DestID	Integer	Any valid DEVID as defined in 7.2.3{xref}	The DEVID of the device that the frame was intended for.
SECID	Octet string	Any valid security session identifier.	Specifies the unique security session identifier for the key that was used on the incoming frame or that was requested to be used on the outgoing frame.
ReasonCode	Enumeration	UNAVAILABLE-KEY, FAILED-SECURITY-CHECK, BAD-TIME-TOKEN	The reason for the security error.

3.1.1.1.2 When generated

This primitive is issued by the MLME when it receives an MLME.request message from a higher layer that requires security to be applied to a frame, but it is unable to find an appropriate key in the ACL or fails to be able to apply security to the frame. This primitive is also issued by the MLME when it receives a validly formatted frame from another device that induces a failed security check according to the security suite or for which the device is unable to find the designated key in the ACL. This primitive is also issued by the MLME when the time token received in a frame does not correspond to the current time token known by the DEV or if the last beacon was not valid.

3.1.1.1.3 Effect on receipt

On receipt of this primitive, the DME is notified of a security error and the reason for the security error.

Author’s note: End of added text for that comment.

Comment (E): (Table 11, pg. 41) The entries for ChallengeType and ChallengeLength should be removed as they are not used any longer.

Comment (T): (6.3.8.1, pg. 46) The use of the SECID in the MLME-REQUEST-KEY.request and MLME-REQUEST-KEY.indication implies that the requesting device knows the SECID of the key it is requesting. This will be true for piconet-wide keys because the SECID will be included in the beacon, but for peer-to-peer keys, the DEV may not know the SECID of the current key, in which case it perhaps should be allowed to request the key without knowing its SECID.

Comment (E): (Table 31, pg. 84) The SECID, sequence numbers and time token should have lengths 2, 4 and 6 respectively.

Comment (T): (Table 31, pg. 84) There should be two SECIDs, one for the management key and one for the data key. Recommend inserting an additional entry for MACPIB_PNCManagementSECID that indicates the SECID of the management key. The MACPIB_PNCSECID should be called the MACPIB_PNCDataSECID and correspond to the data key only.

Comment (T): (Table 32, pg. 85) Each entry in the access control should be able to support keys shared with that particular device. For each access control list table, there should be ManagementKeyInfo, Management-SECID, DataSECID, DataKeyInfo, SMSeqNum and DEVSeqNum entries. Recommend adding these field to the table.

3.2 Clause 7 comments

Comment (TR): (Clause 7.3) A 2-byte secure frame counter needs to be added to the secure frame formats in Figure 10, Figure 12, Figure 17 and Figure 19. The entry should be called “Secure frame counter” and should be added directly after the Time token in each figure. Similarly, the following entry should be added to Table 38:

Table 5—Beacon frame body

Information element	Sub clause	Note	Present in beacon
Secure frame counter	{xref}	The secure frame counter used by the PNC in this superframe, which is used to ensure uniqueness of the nonce.	As needed

Comment (TR): (Clause 7.3.2) A secure delayed ACK frame should be specified. The same conventions used with the other frames should be implemented.

Comment (TR): (Clause 7.4) The 2-byte secure frame counter needs to be added as an information element. Insert the following text for the secure frame counter:

3.2.1 Secure frame counter

The secure frame counter is used to guarantee that the nonce used for CCM security in a given frame is unique. The secure frame counter information element shall be formatted as illustrated in Figure 1.

Figure 1—Secure frame counter information element format

octets: 2	1	1
Secure frame counter	Length (=2)	Element ID

The secure frame counter represents the number of times the selected key has been used during that superframe. This counter shall be included in the CCM nonce.

Author’s note: End of added text for this comment

Comment (TR): (Clause 7.5) In each of the commands, the DME should control whether the SEC field is set to 1 or 0. In each case in which the SEC field is mentioned, the word “shall” should be changed to should or the sentence should be removed. For example, in 7.5.1.1, remove the second sentence or change it to “The SEC field in the frame control field should be set to 0.”

Comment (T): (Clause 7.5.1.2) It appears that if the length of the OID is variable, it may not be possible to unambiguously parse the association response command. Recommend adding the length of the OID before the OID to make this unambiguous.

Comment (TR): (Clause 7.5.2.1) The RSA security suite should be added to the document and the following entries should be added to the list of public-key object types:

5 -> RSA 1024-1 key
6 -> RSA X.509 certificate

Comment (TR): (Clause 7.5.2.5-7.5.2.9) The sequence number in the request key, request key response, distribute key, distribute key response, and de-authenticate commands are not necessary, as the general format for commands specified in 7.3.3.2 includes the sequence number in the command already. The sequence number should be removed from all of these commands.

Comment (TR): (Clause 7.5.2.6-7.5.2.8) The security session ID (SECID) should be included before the Encrypted Seed (where the sequence number currently resides) in the request key response, distribute key request and distribute key response commands. This value is needed to uniquely identify the key that is being transmitted in the protocol. Note that the SECID should not be included in the request key command since the requesting party may not know the SECID of the key being requested. Recommend adding the following text to each of the three commands:

The SECID is the unique identifier for the seed (and corresponding key) that is being transported in this protocol.

3.3 Clause 8 comments

Comment (T): Many of the operational requirements used in clause 8 describe what the DME has to do in order to perform certain operations. The responsiveness of a DEV to operations performed by other devices tends to be based on what the DME does, but the standard doesn’t really have any control over the DME.

Should the “shall” statements in clause 8 be made into “should” statements since they aren’t actually requirements on the MAC layer itself? If so, clause 8 should be changed accordingly to indicate that the requirements in this clause are only optional.

3.4 Clause 9 comments

Comment (T): (Clause 9.3) The security policies described in clause 9.3 are policies that must be implemented by the DME in order to provide the security intended by the security architecture. As such, they cannot be requirements that are placed on the DME. Recommend changing the text in clause 9.3 to:

Security policies determine the actions taken to preserve the security of the piconet. In general, these security policies are implemented by the DME and are thus outside the scope of this standard. However, proper implementation of the security policies is imperative to providing the security services and operational functionality claimed in this standard. It is therefore strongly recommended that implementers ensure that the DME implements the following security policies accurately.

Comment (T): (Clause 9.3) In order to help implementers clearly understand the security processes defined in this document, a description of the processes for implementing security should be included in the standard.

Author’s note: The following text should be added to clause 9 in the security policies sub-clause.

3.4.1 Secure frame generation

When a DEV wishes to send a secure frame, it shall obtain the appropriate keying material from the MAC PIB depending on the key indicated by the DME. If the DME indicates that the PICONET-MGMT key shall be used, the DEV shall use the key from the MACPIB_ManagementKeyInfo entry from the MAC PIB piconet security group parameters. If the DME indicates that the PICONET-DATA key shall be used, the DEV shall use the key from the MACPIB_DataKeyInfo entry from the MAC PIB piconet security group parameters. If the DME indicates that the PEER-MGMT key shall be used, the DEV shall use the key from the MACPIB_ManagementKeyInfo entry from the corresponding MAC PIB access control list group parameters table. If the DME indicates that the PEER-DATA key shall be used, the DEV shall use the key from the MACPIB_DataKeyInfo entry from the corresponding MAC PIB access control list group parameters table. If the DEV is unable to find the corresponding key that is to be used, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to UNAVAILABLE-KEY and shall not transmit the requested frame.

If the DEV is able to obtain the appropriate security suite and key from the MAC PIB, the DEV shall check to see if the last beacon was valid by obtaining the MACPIB_ValidBeacon value. If the last beacon was not valid, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to BAD-TIME-TOKEN and shall not transmit the requested frame. If the beacon was valid, the DEV shall apply the operations defined by the security suite using the key(s) to the frame. The time token included in the frame shall be the value found in the MACPIB_CurrentTimeToken and the SECID included in the frame shall be the value corresponding to the key being used.

The integrity code shall be computed on the entire frame up to the integrity code itself including the MAC header. The result of the integrity code computation shall be encrypted and placed in the integrity code field in the secure frame. The encryption operation shall be applied only to the integrity code, seeds that are being transmitted in a distribute key command or request key response command and the payload of data frames. The result of the encryption operation shall be inserted into the frame in the place of the data that was encrypted.

If any of the security operations fail, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to FAILED-SECURITY-CHECK and shall not transmit the requested frame.

If the security operations have been successfully performed and the payload field has been modified appropriately, the device shall then compute the FCS over the modified frame.

Comment (T): (Clause 9) The following table should be added at the end of the clause describing secure frame generation along with this text:

The key used to protect a particular frame depends on the purpose of the frame. In general, all secure commands between the PNC and other devices should be protected with the PNC management key. All secure data frames to or from the PNC, all secure broadcast frames and all secure beacons should be protected with the piconet group data key. For two DEVs that share a peer-to-peer security relationship, peer-to-peer management keys should be used for all secure commands and peer-to-peer data keys should be used for all secure data frames. If two DEVs in a secure piconet do not have a peer-to-peer security relationship, they may use the piconet group data key for secure commands and secure data frames transmitted between them. The following table summarizes which keys should be used for each type of frame.

Table 6—Key selection for secure frames

Frame type or command	None	PNC-DEV mgmt. key	Piconet group data key	Peer-to-peer mgmt. key	Peer-to-peer data key	Comment
Beacon frame			X			All secure beacon frames shall be protected by the group data key.
Immediate acknowledgement frame		X	X	X	X	Secure immediate acknowledgement frames should use the key used in the frame that is being acknowledged.
Delayed acknowledgement frame		X	X	X	X	Secure delayed acknowledgement frames should use the key used in the frame that is being acknowledged.
Data frame			X		X	Secure data frames between devices that share a peer-to-peer key shall use the peer-to-peer data key, otherwise they shall use the piconet group data key.
Association request	X					Association request commands shall not be secured with any key.
Association response	X					Association response commands shall not be secured with any key.
Disassociation request		X				
Disassocation response		X				

Table 6—Key selection for secure frames

Frame type or command	None	PNC-DEV mgmt. key	Piconet group data key	Peer-to-peer mgmt. key	Peer-to-peer data key	Comment
Authentication request	X					Authentication request commands shall not be secured with any key.
Authentication response	X					Authentication response commands shall not be secured with any key.
Challenge request	X					Challenge request commands shall not be secured with any key.
Challenge response	X					Challenge response commands shall not be secured with any key.
Request key		X		X		The management key for the relationship (peer-to-peer or PNC-DEV) shall be used for this command.
Request key response		X		X		The management key for the relationship (peer-to-peer or PNC-DEV) shall be used for this command.
Distribute key request		X		X		The management key for the relationship (peer-to-peer or PNC-DEV) shall be used for this command.
Distribute key response		X		X		The management key for the relationship (peer-to-peer or PNC-DEV) shall be used for this command.
De-authenticate				X		
New PNC announcement			X			
PNC handover		X				
PNC handover information		X				
PNC information request		X				
PNC information		X				
Probe		X	X	X		If the devices do not share an individual relationship, the piconet group data key shall be used. Otherwise, the management key (peer-to-peer or PNC-DEV) for the relationship shall be used.
Transmission sequence sync		X				

Table 6—Key selection for secure frames

Frame type or command	None	PNC-DEV mgmt. key	Piconet group data key	Peer-to-peer mgmt. key	Peer-to-peer data key	Comment
Channel time request		X				
Channel time status		X				
Channel status request		X	X	X		If the devices do not share an individual relationship, the piconet group data key shall be used. Otherwise, the management key for the relationship (peer-to-peer or PNC-DEV) shall be used.
Channel status response		X	X	X		If the devices do not share an individual relationship, the piconet group data key shall be used. Otherwise, the management key for the relationship (peer-to-peer or PNC-DEV) shall be used.
Remote scan request		X				
Remote scan response		X				
Transmit power change		X	X	X		If the devices do not share an individual relationship, the piconet group data key shall be used. Otherwise, the management key (peer-to-peer or PNC-DEV) for the relationship shall be used.
APS sleep request		X				
APS sleep response		X				
SPS change		X				
SPS configuration request		X				
SPS configuration response		X				
SPS inquiry		X				
SPS inquiry response		X				

3.4.2 Removing security from frames

When a DEV receives a secure frame, it shall obtain the appropriate keying material from the MAC PIB depending on the SECID and source address found in the frame. To find the correct key, the DEV shall first check the MAC PIB for an ACL entry that corresponds to a peer-to-peer relationship with the sending DEV and that has a MACPIB_DataSECID or MACPIB_ManagementSECID that matches the received SECID. If no peer-to-peer ACL entry matches the received frame, the DEV shall check the MACPIB_PNCDataSECID and MACPIB_ManagementSECID to determine if it matches the received SECID. If either of these entries gives a match, the DEV shall use the security suite in the corresponding MACPIB_SecuritySuite and the key corresponding to the SECID. If an appropriate entry in the ACL cannot be found, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to UNAVAILABLE-KEY and shall not perform any additional operations on the received frame.

If the DEV is able to obtain the appropriate security suite and key from the ACL, the DEV shall compare the received time token to the value in the MACPIB_CurrentTimeToken. If the frame is a beacon frame, the DEV shall determine if the received time token is greater than the MACPIB_CurrentTimeToken. If the frame is not a beacon frame, the DEV shall determine if the received time token is equal to the MACPIB_CurrentTimeToken. If either of these checks fail, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to BAD-TIME-TOKEN and shall not perform any additional operations on the received frame. If the time token matches, the DEV shall apply the operations defined by the security suite to the frame.

Before the security operations have been performed and the payload field has been modified, the DEV shall check the FCS. The DEV shall also check that the time token in the frame corresponds to the value in the MACPIB_CurrentTimeToken. If the time token does not match, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to UNAVAILABLE-KEY and shall not perform any additional operations on the received frame

The decryption operation shall be applied only to the integrity code, seeds that are being transmitted in a distribute key command or request key response command and the payload of data frames. The result of the decryption operation shall be replaced into the received frame in the place of the encrypted data. The integrity code shall be computed on the entire frame with the decrypted data replacing the encrypted data up to the integrity code itself including the MAC header.

If any of the security operations fail, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to FAILED-SECURITY-CHECK and shall not perform any additional operations on the received frame.

If the security operations have been successfully performed and the frame has been modified appropriately, the device may then continue to process the frame.

3.4.3 Joining a secure piconet

If a DEV wishes to join a secure piconet, it should associate with the PNC in order to be assigned a local DEVID and time slots to perform the authentication process. Since the device must be associated before the authentication process has taken place, the association command and response should have the SEC field in the frame control field set to 0.

Once the DEV is associated, the PNC should allocate an MTS to allow the DEV to proceed with the authentication protocol as described in 9.9.1{xref}. Before the authentication process is initiated, the DEV and PNC should ensure that they will be able to successfully implement the authentication protocol. Once the DEV is associated, the DEV or PNC may choose to send probe commands to each other to request or transmit public key objects or to request or transmit preferred OIDs. When a public key object is received in a probe command before authentication, the DEV may choose to determine whether that public key would be accepted in an authentication protocol and update its ACL if desired. The DEV and PNC may also exchange additional information before authentication if desired.

After the DEV has associated and exchanged the desired information with the PNC, the DEV should initiate the authentication protocol. The authentication and challenge commands are designed to be used with security turned off. In the authentication request command, the DEV should select either the security suite OID received in the association response or an OID received in a probe command after associating. Once the authentication protocol has been initiated, the DEV should follow the states and state transitions specified in 9.9.1.1 and 9.9.1.2 {xref}. While in the authentication process, the authentication commands should have the SEC field in the frame control field set to 0. If during the authentication process there is a security check failure of any kind, the DEV or PNC should return the appropriate error in the challenge response command or authentication response command respectively and exit from the authentication protocol.

3.4.4 Secure beacon processing

3.4.4.1 Generating secure beacons

A PNC in a piconet using security should send secure beacons protected with the piconet protection key stored in the MACPIB_DataKeyInfo field in the MAC PIB. For each superframe, the PNC should increment the time token stored in the MACPIB_CurrentTimeToken in the MAC PIB and transmit a secure beacon with the SEC field in the frame control field set to 1.

3.4.4.2 Receiving secure beacons

In order to maintain secure and reliable operations in the piconet, a DEV shall use the beacon to help maintain the current time token and the current key. When the DEV receives a secure beacon (a beacon with the SEC field in the frame control field set to 1), it shall verify that the time token is greater than the MACPIB_CurrentTimeToken, that the SECID matches the MACPIB_PNCSECID stored in the MAC PIB and that the integrity code passes. If all of these checks succeed, the DEV shall set the MACPIB_CurrentTimeToken to the received time token value and set the MACPIB_ValidBeacon to valid. If the time token is greater than the MACPIB_CurrentTimeToken, but the SECID does not match the MACPIB_PNCSECID, the device may set the MACPIB_CurrentTimeToken to the value in the beacon and send a key request command to the PNC to obtain the new key.

Comment (T): (Clause 9.4) The following descriptive text should be added to clause 9.4.

The security mode indicates in what manner a DEV shall utilize the entries in the MAC PIB piconet security group parameter and MAC PIB access control list group parameters. The security mode in use is determined by the MACPIB_SecurityOptionImplemented entry in the MAC PIB.

Comment (T): (Clause 9.4.1) The description of security mode 0 is not descriptive enough and should refer to a DEV operating in the mode, not a piconet operating in the mode. Recommend replacing the text in 9.4.1 with the following text:

A device operating in security mode 0 shall not utilize the ACL entries and shall not perform any security related operations on MAC frames. While in this mode, if the MAC receives a frame with the SEC field set to 1, the MAC shall discard the frame and the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layer with the ReasonCode set to UNAVAILABLE-KEY. If the MAC receives a frame with the SEC field set to 0, the MLME shall set the SecurityUse and ACLEntry fields to FALSE in the indication to the DME.

Comment (T): (Clause 9.4.2) The description of security mode 1 is not descriptive enough and should refer to a DEV operating in the mode, not a piconet operating in the mode. Recommend replacing the text in clause 9.4.2 with the following text:

Security mode 1 provides a mechanism for the MLME of a PNC to indicate to the DME if a received frame purportedly originated from a device in the ACL. The PNC may use this information as a criterion for allowing a device into the piconet. A device operating in security mode 1 shall not perform any security related operations on MAC frames. While in this mode, if the MAC receives a frame with the SEC field set to 1, the

MAC shall discard the frame and the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layer with the ReasonCode set to UNAVAILABLE-KEY. If the MAC receives a frame with the SEC field set to 0, the MLME shall set the SecurityUse field to FALSE and the ACLEntry field to TRUE or FALSE depending on if the sender is in the ACL in the indication to the higher layer.

Comment (T): (Clause 9.4.3) The description of security mode 2 is not descriptive enough and should refer to a DEV operating in the mode, not a piconet operating in the mode. Recommend replacing the text in clause 9.4.3 with the following text:

Security mode 2 provides a mechanism for a device to perform cryptographic security on frames transmitted in the piconet. DEVs operating in security mode 2 use public-key cryptography to verify the authenticity of other DEVs in the piconet and symmetric-key cryptography to protect frames using encryption and integrity. The cryptographic operations used for secure frames exchanged with the PNC and with other members of the piconet security group shall be performed as specified by the security suite indicated in the MACPIB_SecuritySuite in the MAC PIB piconet security group parameters. The cryptographic operations performed for secure frames exchanged with a peer DEV shall be performed as specified by the security suite indicated in the MACPIB_SecuritySuite entry associated with that peer security relationship in a MAC PIB access control list group parameters table. While in this mode, the MAC may accept frames with the SEC field in the frame control field set to 1 or 0 and shall set the SecurityUse in the MLME message to the DME to TRUE or FALSE respectively.

Comment (T): (Clause 9.4.4) The description of security mode 3is not descriptive enough and should refer to a DEV operating in the mode, not a piconet operating in the mode. Recommend replacing the text in clause 9.4.4 with the following text:

Security mode 3 provides a mechanism for a device to perform cryptographic security on frames transmitted in the piconet. DEVs operating in security mode 3 use public-key cryptography and public-key certificates to verify the authenticity of other DEVs in the piconet and symmetric-key cryptography to protect frames using encryption and integrity. The cryptographic operations used for secure frames exchanged with the PNC and with other members of the piconet security group shall be performed as specified by the security suite indicated in the MACPIB_SecuritySuite in the MAC PIB piconet security group parameters. The cryptographic operations performed for secure frames exchanged with a peer DEV shall be performed as specified by the security suite indicated in the MACPIB_SecuritySuite entry associated with that peer security relationship in a MAC PIB access control list group parameters table. While in this mode, the MAC may accept frames with the SEC field in the frame control field set to 1 or 0 and shall set the SecurityUse in the MLME message to the DME to TRUE or FALSE respectively.

3.5 Clause 10 comments

Comment (TR): (Clause 10.2.2) The mandatory to implement sub-suite should be less expensive and easier to implement than the current mandatory to implement sub-suite (ECIES-prime-256 raw 1). A security suite based on the RSA algorithm should be made mandatory.

Comment (TR): (Clause 10) The RSA-OAEP based security suite proposed in document {xref} should be inserted into the draft and made the mandatory to implement algorithm.

Comment (TR): (Table 82, pg. 259) The challenge response generation entry and the authentication response generation entry should add the following sentence at the end:

The secure frame counter used in the CCM nonce shall be the 2-byte string 0x0000.

4. Notes

Are sub-rate slots allowed to be pseudo-static?

Clarify 3 modes, 2 state (should already be comment).