IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)		
Title	**IEEE P802-15_TG3 D10 Security Related Comment Resolutions**		
Date Submitted	[August 13, 2002]		
Source	[Ari Singer, Daniel V. Bailey] [NTRU] [5 Burlington Woods Burlington, MA 01803 USA]	Voice: Fax: E-mail:	[+1 781 418-2515] [+1 781 418-2532] [asinger@ntru.com]
Re:	802.15.3 TG3 Letter Ballot Draft D10		
Abstract	[This document is offered as rolling recommended resolutions for security related ballot comments on 802.15.3 D10.]		
Purpose	[This document is offered as rolling recommended resolutions for security related ballot comments on 802.15.3 D10. It will be updated frequently to accommodate input and decisions by the working group as well as adding more proposed resolutions for other ballot comments.]		
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, Vancouver to Schaumburg

2. Resolved Comments

2.1 Monday, July 22, 2002

293 (Shvodian, TR) & 304 (Shvodian, TR) **Reject. These IEs are used for the probe command.**

494 (Gilb, TR) The SECID is listed as an octet string in some of these tables. Change the SECID to be 2 octets in all locations. Particularly, change tables 11, 12, 13 and 32. **Accept.**

2.2 Tuesday, July 23, 2002

460 (Gilb, T) There is no introductory text to describe this subclause. Text is also missing from 9.9.4 and 9.9.6. **Accept in principle.**

Text for clause 9.9.3 introduction: In a secure piconet or in a secure peer-to-peer relationship, the security manager may wish to update the current data protection key by initiating the distribute key protocol described here. For a change in the piconet group data key, the PNC sends the new piconet group data key to each authenticated DEV before changing the key using the distribute key protocol. For a change in a peer data key, the security manager in the relationship initiates the distribute key protocol.

Text for clause 9.9.4 introduction: In a secure piconet, if a DEV receives a frame or beacon with an unknown SECID, it may initiate the request key protocol described here in order to obtain the unknown key from the security manager of the relationship.

Text for clause 9.9.6 introduction: When a DEV transmits (or recieve) a secure data frame, the DEV shall protect (or verify) the frame using the data protection protocol described here.

630 (Gilb, T) The word "can" is use when it should be "may". **Accept.** Change "The only state a DEV can " to "The only state a DEV may "

482 (Gilb, TR) The PNCs DEV address is no longer in the beacon. Ensure that the DEV address of the PNC is available in some other manner to all DEVs to peform the required security processes. **Accept in principle.** Add text in Figure 149 "Store ID_SM as the DEV address of the SM for this authentication." On page 133, line 9 change "requesting DEV" to "security manager".

426 (Gilb, T) Missing definitions for the following acronyms: CCM, DER, ECQV, ECIES, CTR, CBC, CRL, SECID. Add the following definitions: CCM - counter-counter mode, DER - ?, ECQV - eliptic curve Qu-Vanstone, ECIES - eliptic curve ??, CTR - counter mode, CBC - ??, CRL - ??, SECID - security identifier. **Accept in principle.** CCM - CTR encryption + CBC-MAC, DER - Distinguished Encoding Rules, ECMQV - Elliptic Curve Menezes-Qu-Vanstone key establishment protocol, CTR - Counter mode, CBC - Cipher Block Chaining, CRL = Certificate Revocation List, SECID - Security Identifier, CBC-MAC = Cipher Block Chaining-Message Authentication Code

578 (Gilb, T) The comparison with TLS needs to be modified to indicate the use of CCM rather than HMAC with SHA-256 and CBC encryption. Change the comment after the first bullet to: The security suite specfication in this document specified the use of AES in CCM mode, which provides an AES CBC-MAC encrypted using AES CTR encryption. **Accept in principle.** Change "The security suite specification in this document specifies the use of HMAC with SHA-256." to "The security suite specifications in this document may specify other algorithms."

475 (Gilb, TR) Step 4 says to validate the content of ICU but does not specify how it is done. Provide the figure that was intended here and fix the xref. Otherwise, delete the sentence. **Accept in principle. This mechanism should be specified in the security suite, not in the general scheme. Struik will provide update to the implicit certificate methods and implicit certificate security sub-suite.**

474 (Gilb, TR) Figure 12 is not in the annex nor is it a valid cross reference. Specify how this validation is to be performed. Otherwise, delete the implicit certificate scheme. **Accept in principle. Struik will provide update to the implicit certificate methods and implicit certificate security sub-suite.**

2.3 Friday, July 26, 2002

62 (Heberling, TR) Please clarify what impact the Security parameters have upon aMaxFrameSize-4? Does the amount of useful data get reduced to maintain the aMaxFrameSize-4? Please add clarification to the indicated sentence. **Accept in principle.** Add following sentence to end of clause 7.2.7, page 106, line 4: "When the SEC bit is set to 1, additional fields included in the frame body for payload protection will reduce the number of actual information octets by 12."

862 (Shvodian, T) Initial Owner needs a definition. Definine initial owner. **Accept in principle.** Add the following to sub-clause 9.9. "For each protocol described in this sub-clause, tables are included to specify the requirements for the DEV and security manager to successfully implement the protocol. The setup table specifies the required data that must be stored by each device, denoted the initial owner, before the protocol is initiated. The capabilities table specifies the required functionality for each device to perform its respective role in the protocol."

930 (Shvodian, T), 885 (Shvodian, T), 886 (Shvodian, T), 887 (Shvodian, T), 892 (Shvodian, T): Defer to group resolution of 150.

463 (Gilb, TR), 847 (Shvodian, TR): **Accept in principle.** The term network byte order will be removed along with the need for the sequence counters.

870 (Shvodian, TR), 941 (Shvodian, T) **Accept in principle. Add the following text to clause 9.3 (related to text in 4.4 of 02/273r5): (This text is not yet approved)**

Changes in the piconet-wide group data key

When the PNC changes the piconet-wide group data key, the PNC shall transmit the new key to all of the currently authenticated DEVs using the {xref - distribute key command }. Once all of the authenticated DEVs have been informed of the change, the PNC can change the SECID in the beacon. When a DEV receives a valid {xref - distribute key} command from the PNC, the DEV shall use the new key for all outgoing secure frames that require the use of the piconet-wide group data key once it sees the corresponding SECID in the beacon. The DEV may continue to accept frames protected by the old piconet-wide group data key for up to{65,535 ms}.

If a DEV that is in the AWAKE state or entering the AWAKE state from the SLEEP state, {xref - 8.12}, receives a beacon with a time token greater than the last known time token, but with a SECID that does not match the SECID of the known key, the device shall send a key request command to the PNC to obtain the new key. While waiting to obtain the new key, the DEV may accept the new time token value and continue to transmit and accept frames with the last known piconet-wide group data key for up to {65, 535 ms-"the amount of time since the DEV last received a valid beacon with the known key"}.

224 (Gilb, TR), 846 (Shvodian, TR): **Accept in principle. Add following text to sub-clause 9.3 along with table to be added as part of resolution of comment 865.**

Selecting the SECID for new keys

For each management and data key used in the piconet, the security manager in the relationship shall select the 2-octet SECID that identifies the key. The first octet of the SECID for all keys except the piconet-wide group data key shall be set to the DEVID of the security manager in the relationship. The SECID for the piconet-wide group data key shall have the first octet set to the BcstID, {xref - 7.2.3}.The second octet shall designate a unique value for the key associated with the security relationship between the security manager and a DEV.

565 (Gilb, TR) 7.5.2.6-7.5.2.9: 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. Delete the SECID from the key request command. Change the name of the SECID field in the other three commands to be Key SECID. Add the following text to each of the three commands: The key SECID field is the unique identifier for the seed (and corresponding key) that is being transported in this protocol. **Accept. Make sure definition and use of ‘seed’ is well defined.**

938 (Shvodian, T) For all of the secure frame formats, we may need to add the SMID (security manage ID) to the secure header so that a receiving DEV knows which key to use. Add the 8 bit SMID to security frames to enable a DEV to know which key was used for the encryltion. **Accept in principle. See resolution to 846.**

843 (Shvodian, T) Add the ACKs to the figures unless it makes them unnecessarily complicated. Otherwise, leave it as is. Change from integrity protected ACK to Immediate ACK. **Accept.**

927 (Shvodian, T) Secure ACK is not needed. Remove the Secure ACK message authentication generation. **Accept.**

282 (Shvodian, TR) Remove Secure Immediate ACK. It serves no purpose and complicates the ACK frame by giving it a frame body. Delete Secure Imm-ACK frame. **Accept.**

457 (Gilb, TR) There are no ACKs shown in the overview figures. Add the ACKs to the figures unless it makes them unnecessarily complicated. Otherwise, leave it as is. **Reject. No ACKs are shown on the diagrams since they do not add value to understanding the protocol, but do clutter up the diagram.**

2.4 Tuesday, July 30, 2002

218 (Gilb, TR) 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. Change the MLMEs to indicate that a DEV is able to send the request key without knowing the SECID of the current key. Otherwise, perhaps the SECID can be deleted from the request command? **Accept in principle. Delete SECID from the request command.**

222 (Gilb, TR) The SMSeqNum and DEVSeqNum are no longer used. Delete all references to the sequence number in clause 6. **Accept.**

221 (Gilb, T) 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, ManagementSECID, DataSECID, DataKeyInfo entries. Adding these fields to the table. **Accept in principle.** Add Management-

KeyInfo, ManagementSECID, DataSECID, and DataKeyInfo entries in the MAC PIB access control list group parameters (Table 32). Delete MACPIB_SECID from Table 32.

221+ (Gilb, T) ACCEPT IN PRINCIPLE: Update Table 31 as well to include ManagementSECID and DataSECID in place of MACPIB_PNCSECID.

776 (Shvodian, TR) It is a waste to have a 6 octet time token in a secure beacon and a 4 octet beacon number in the piconet synchronization parameter. Are 6 octets really needed? Octets would roll over less than once per year with a 10 ms superframe. If 4 octets are sufficient, just use the beacon number. If 6 octets are needed, change the beacon number in the piconet synchronization parameter to 6 octets and delete the time token. **Accept in principle.** Delete Time token from Figure 10 on page 108. Update all references to time token to reference the beacon number. Delete Time token from Table 38 and 46 in section 7.4.20. Change the beacon number from 4 octets to 6 octets in Figure 23. (Note: determine if new name needed for the 6 octet version to allow 4 octet version to continue to be used as is. James)

780 (Shvodian, TR) Remove the Time token. This can be replaced by the beacon counter in the piconet synchronization IE. **Accept in principle. See resolution to 776.**

2.5 Wednesday, July 31, 2002

433 (Gilb, T) The SECID, time token and integrity code fields are not defined before they are first discussed. Add either a forward reference to the definitions of these fields or define them here or in 7.2 with a generic secure frame as an example. **Accept in principle. Add the following figure and text to clause 7.2.**

The frame body shall have the following format when the SEC bit is set to 1 in the frame control field.

8	variable	2	2
Integrity code	Payload	Secure frame counter	SECID

Figure 1—Secure frame body

Add the following sub-clauses to 7.2:

SECID field

The SECID field shall be included in the frame body of all secure frames. The SECID field contains a 2-octet identifier for the key that is being used to protect the frame. The SECID for a given key is selected by the security manager in the secure relationship as described in {xref - see resolution to 224 and 846}. The SECID for management keys is communicated to a DEV in a successful authentication protocol by the security manager in the challenge request command {xref - 7.5.2.3}. The SECID for data keys is communicated to a DEV by the security manager in a distribute key request command {and broadcast distribute key command pending resolution to Odman’s e-mail}, 7.5.2.7, or a request key response command, 7.5.2.6.

Secure frame counter (SFC) field

The secure frame counter field shall be included in the frame body of all secure frames. The secure frame counter field contains a 2-octet counter that is used to ensure the uniqueness of the nonce in a secure frame.

A DEV shall not reuse a frame counter with the same time token and key. The DEV may initialize the secure frame counter at 0 and increment it each time a secure frame is sent. When the time token is updated, the DEV may reset the secure frame counter to 0 if desired or allow the counter to roll over.

Integrity code field

The integrity code field shall be included in the frame body of all secure frames. The integrity code field contains an 8-octet encrypted integrity code that is used to cryptographically protect the integrity of the MAC header and MAC frame. The integrity code is computed as specified in {xref - 10.2.5}.

Update resolution to 62 to include SFC, but not FCS. Set the number of information octets reduced in secure frames to 12. See resolution from Friday, July 26 for corrected text.

865 (Shvodian, TR) It needs to be clear which commands use secure command format and which use non secure command format. **Accept in principle. Add the following table and text to clause 7 (need to determine best place).**

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 shall be protected with the PNC management key. All secure data frames to or from the PNC, all secure broadcast frames and all secure beacons shall be protected with the piconet group data key. For two DEVs that share a peer-to-peer security relationship, peer-to-peer management keys shall be used for all secure commands and peer-to-peer data keys shall 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 1—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					Immediate acknowledgement frames shall not be secured with any key.
Delayed acknowledgement frame	X					Delayed acknowledgement frames shall not be secured with any key.
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.

Table 1—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
Disassociation request		X				
Disassocation response		X				
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				

Table 1—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
PNC information		X	X			If the PNC information command is sent as a directed frame from the PNC to a DEV, the PNC-DEV management key shall be used. If the PNC information command is sent as a broadcast frame, the piconet group data key shall be used.
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				
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				

Table 1—Key selection for secure frames

Frame type or command	None	PNC-DEV mgmt. key	Pico-net group data key	Peer-to-peer mgmt. key	Peer-to-peer data key	Comment
SPS configuration request		X				
SPS configuration response		X				
SPS inquiry		X				
SPS inquiry response		X				

577 (Gilb, TR) There needs to be an explanation of what keys are used with which commands. clause 9 seems like a good place to put this. A table needs to be added to list the usage of the frames and the types of keys used for each frame (the table is in document 02/271r0). The following text should be added at the end of the clause describing secure frame generation: 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. **Accept in principle. See resolution to 865.**

387 (Heberling, TR) Insert a copy of table 38 into clause 7.3.1.2 just before Table 40 with these info elements for the secure beacon frame: Info Elements Present in beacon ChannelTimeAllocation In every beacon Piconet BSID In every beacon DevAssociation As needed StreamAnnouncement As needed PNCHandoverCount As needed Piconet parm change As needed Parent PNC DEV Address As needed Integrity code In every beacon. **Accept in principle. Resolution of comment 385 moved Table 38 to where the confusion between secure and non-secure frames is no longer present.**

296 (Shvodian, TR) Key number is no longer needed. This was added to let a DEV know when the group key changed. Since the SECID is in every beacon, DEVs will know when the key changes. Remove Key number for the beacon in figure 23 and remove the description from the text. **Accept.**

569 (Gilb, TR) Need to add a description on how to create and receive a secure beacon. Add the following text to the end of subclause 9.3 9.3.6 Secure beacon processing 9.3.6.1 Generating secure beacons A PNC in a piconet using security should send secure beacons protected with the piconet protection key stored. For each superframe, the PNC should increment the time token and transmit a secure beacon with the SEC field in the frame control field set to 1. 9.3.6.2 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, it shall verify that the time token is greater than the current time token, that the SECID matches the SECID for the piconet and that the integrity code passes. If all of these checks succeed, the DEV shall set the current time token to be the received time token value. If the time token is greater than the current time token, but the SECID does not match the current SECID, the

device may set the current time token to the value in the beacon and send a key request command to the PNC to obtain the new key. **Accept.**

Updated August 8th to:

Add the following text to the end of sub clause 9.3 9.3.6 Secure beacon processing 9.3.6.1 Generating secure beacons A PNC in a piconet using security shall send secure beacons protected with the current piconet protection key. For each superframe, the PNC shall increment the beacon number and transmit a secure beacon with the SEC field in the frame control field set to 1. 9.3.6.2 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 beacon number and the current SECID in the beacon. When the DEV receives a secure beacon, it shall verify that the beacon number is greater than the current beacon number, that the SECID matches the its last known SECID for the piconet and that the integrity code passes. If all of these checks succeed, the DEV shall set the current beacon number to be the received beacon number value. If the beacon number is greater than the current beacon number, but the SECID does not match the devices last know SECID for the piconet, the device may set the current beacon number to the value in the beacon and send a key request command to the PNC to obtain the key corresponding to the SECID sent in the beacon.

936 (Shvodian, T) An authenticated DEV can use the probe command. Can an unassociated DEV? If the PNC is checking the ACL to determine association privliges, a DEV could get refused from associating. Clarify if an associated DEV can do a probe. Split unauthenticated into two columns: unassociated and associated. **Accept in principle.** In Figure 151 on page 225 add "Unassociated state" between "Any state" and "Unauthenticated state D0.0". Transition from "Any state" to "Unassociated state" is the current D0.1. Add transition from "Unassociated state" to "Unauthenticated state D0.0" upon completion of association. In Table 58, page 226, line 8, change "Default state for the DEV" to "Default state for an associated DEV"

(Update from August 7) Remove the X in the Authenticated (if required) column for the Probe command in Table 48.

931 (Shvodian, TR) This raises an interesting question: "If the hash is not in the PIB, the public key is passed to the DME to establish trust by other means." Is the security function in the DME? The MLME_request.indication goes up to the SM's DME. So is the SM part of the DME? Need to clarify where the security function resides in the reference model of figure 3. Is it part of the DME? **Accept in principle.** The security manager operations, which consist of managing the keys for the relationship, reside in the DME. The DME also maintains the ACL, which is used for managing the keys. However, there currently is no mechanism for the DME to update the ACL and keying information that is required by the MAC when operating in the secure modes. Ari will create new MLMEs similar to those defined in Appendix G of the 802.15.1 standard to allow the DME to update required ACL and keying information. We should also determine whether more information than required is included in the MAC PIB access control list group (subclause 6.5.6 and table 32).

(From August 8) Change resolution to: **Accept in principle.** The security manager operations, which consist of managing the keys for the relationship, reside in the DME. The DME also maintains the ACL, which is used for managing the keys. The DME shall use the MLME-Get and MLME-Set commands to update contents of the MAC PIB access control list group.

2.6 Friday, August 2, 2002

758 (Shvodian, TR) Does the length field in the Tx length include security overhead? What is covered by the length field needs to be clarified. **Accept in principle.** Page 91, Line 10. Change “Length of the frame to be transmitted.” to “Length of the MAC frame to be transmitted {xref 7.2}.”

782 (Shvodian, TR) Frames with the SEC bit set to one use the secure frame format. Add the following text: Frames with the SEC bit set to one shall use the secure frame format. **Accept in principle.** Add the following at end of sub-clause 7.2.1.3 on page 103. “Frames with the SEC bit set to one shall use the secure frame format for that frame type, {xref - 7.3}.”

497 (Gilb, TR) Add the text required to implement 2 key CCM, indicating that it is an option. That way, if an attack is found, the standardized implementation is already written and implementers simply need to switch over to it. **Withdrawn.**

888 (Shvodian, TR) Is the secure frame counter 2 octets or 4? It looks like it is currently 2 octets in the data frames and 4 in the command frames. If this is the case, then a separate nonce is needed for command frames. Clarify the number of octets in the data, command and beacon secure frame counters. **Accept in principle.** See resolution to 433.

495 (Gilb, TR) Add a field, secure frame counter, to every secure frame. Make it 2 octets long. Add a new element called the "secure frame counter." to every secure frame. The secure frame counter basically counts the number of secure frames that a particular DEV has transmitted within that superframe. The secure frame counter shall have a length 2-bytes and go directly after the time token. This counter is used as an input to the nonce for payload protection. Add the requirement that a DEV shall not send two secure frames within the same superframe with the same secure frame counter. The simplest way to ensure this is that the beginning of each superframe, the value shall be set to 0 and it shall be incremented each time it is used within that superframe (which is any time you send a secure frame). **Accept in principle.** See resolution to 433.

891 (Shvodian, T) Can one secure frame counter be used for all transmission or is a separate on needed for all groups? Clarify if it is acceptible for one secure frame counter to be used for alll frames. **Accept in principle.** See resolution to 433.

223 (Gilb, TR) A 2-octet secure frame counter needs to be added to the secure frame formats in Figure 10, Figure 12, Figure 17 and Figure 19. The field should be called "Secure frame counter" and should be added directly after the time token in each figure. Add text to 7.3 that describes the secure frame counter field as follows: "The secure frame counter is used by the DEV for this frame to ensure uniqueness of the nonce." **Accept in principle.** Replace time token field with secure frame counter field (2 octets) in Figures 10, 12, 17, and 19. Add entry to Table 38: Secure Frame Counter, 7.2.x (see 433), “The secure frame counter is used by the DEV for this frame to ensure uniqueness of the nonce.”, As needed.

281 (Shvodian, TR) Secure Frame Counter (Data) or Sequence Counter (command) is missing. Not sure which one is used to protect the beacon. Add correct secure counter. **Accept in principle.** The secure frame counter should be included. See 433.

769 (Shvodian, TR) Padding for security is needed. Security encrypts blocks of 128 bits (16 octets). Need to add padding for security, plus a field to indicate how many pad octets there are. **Reject.** CCM mode does not require the use of any padding and the encrypted text need not be a multiple of 16 octets.

890 (Shvodian, TR) Padding needed to round up to 128 bit blocks. A mechanism is needed to pad the frame to a multiple of 16 octets and a way to indicate to the receiver how many octets of padding must be removed. May need a pad field in the secure frames. **Reject.** CCM mode does not require the use of any padding and the encrypted text need not be a multiple of 16 octets.

2.7 Tuesday, August 6, 2002

563 (Gilb, TR) 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. **Accept in principle.**

Add RSA security suite as defined in 02363r0 as an optional security suite in clause 10.

-Add three additional public key information element IDs to table 46 in 7.4. These shall be numbered consecutively in the table and represent segments of a public key object longer than 255 octets that will be formed by the sequential concatenation of the information elements. Modify sub-clause 7.4.14 to show long public keys segmented into multiple IEs with the highest element ID sent first in any single or multiple frame exchange. A DEV requesting a public key object IE, shall only request the lowest IE ID in the request.

-Update list of valid public-key object types in sub-clause 7.5.2.1 to be:

0-> NULL
1-> ECMQV Koblitz-283 key
2-> RSA-OAEP Raw 1024 key
3-> NTRUEncrypt 251-1 key
4-> ECMQV Koblitz-283 Implicit Certificate
5-> X.509 Certificate
6-255 -> Reserved

-Remove entries for "Auth Response" and "Challenge Response" from Table 81 in sub-clause 10.2.5.1. These entries will be added to each security suite individually.

-Remove the "Authentication response generation" and "Challenge response generation" entries from Table 82 in sub-clause 10.2.5.2. These entries will be added to each security suite individually.

-Remove the "Payload protection key derivation" entry from Table 82 in sub-clause 10.2.5.2. These entries will be added to each security suite individually.

-Change all occurrences of "EncryptedSeed" in the Request Key and Distribute Key commands with "Key". Change associated description of those entries to remove word "encrypted" where appropriate. Change all occurrences of "seed" with "key" where appropriate. All command frames including these keys shall always be protected by the management key associated with the SM relationship between the source and destination DEVs. An example of the entries that need to be changed are in 02363r0.

-Remove entries "Seed_D" and "Seed_G" from table 55.

-Change last sentence of 9.7.5 to read: "This key is the payload protection key that is generated by the security manager."

-Remove steps to generate "Keys_D" from "Seed_D" in figure 149 and replace text for obtaining the seed with the following text in clause 9.9.1 figure 149: "Performs operations on challenges to obtain shared key "Keys_D".

-Update "seed" with "Keys" where appropriate in table 64, figure 155, table 66, figure 157, table 72, and figure 166.

-Change the "Encrypted seed" entry in table 81 to Table 2 in doc 02363r0.

-Change the "Seed encryption operation" entry in table 82 to Table 3 in doc 02363r0 with the following description: "The key for key transport {in the key request, {xref - 9.9.4}, or distribute key, {xref - 9.9.3} protocols) shall be encrypted using CCM authentication and encryption using the management payload protection key {xref - 7.3.3.2}."

-Change the term "seed" to "key" in table C.1 of the security rationale appendix.

882 (Shvodian, T) Are suite OIDs ever used, or do we just need subsuite OIDs? Eliminate suited OIDs if they serve no purpose. **Reject.** The sub-suite OIDS a built off of the suite OID arcs. Since are defining these OIDs for the first time in this standard, they should be included in the draft. The suite OIDS are not used or transmitted by the DEVs.

484 (Gilb, TR) The sequence counter field is no longer needed. Delete the sequence counter field from this figure and delete all references to it in the draft. This includes deleting the MACPIB_SMSeqNum and MACPIB_DEVSeqNum. **Accept.**

290 (Shvodian, TR) sequence counter is missing. Add sequence counter. **Accept in principle.** The time token field has been replaced with the Secure Frame Counter field. (See comment 433)

848 (Shvodian, T) Why are the seq_nums 4 octets and SFDs 2 octets? Is it because management is more important than data? Many more data frames should be tranmitted than management. Prefer 2 octet for management sequence counter for overhead reasons if it is not a security problem. **Accept in principle.** Sequence counters have been replaced with a secure frame counter of 2 octets for both management and data frames. (See comment 433)

297 (Shvodian, TR), 284 (Shvodian, TR), 389 (Heberling, TR), 289 (Shvodian, TR), 390 (Heberling, TR), 435 (Gilb, TR), 392 (Heberling, TR), 305 (Shvodian, TR), 832 (Shvodian, T) **Accept in principle.** Time token has been removed and replaced with a beacon number which is 6 octets long. (See comment 776)

930 (Shvodian, T) **Accept in principle.** Clause 10.2.4.1 shall be removed and all bit ordering in clause 10 will be updated to be consistent with rest of the draft. (See comment 150)

885 (Shvodian, T), 886 (Shvodian, T), 887 (Shvodian, T), 892 (Shvodian, TR) **Accept in principle.** All bit ordering in clause 10 will be updated to be consistent with the rest of the draft. (See comment 150)

883 (Shvodian, T) Why no certs for NTRUEncrypt? Certs for NTRUEncrypt, may not be used, but should they be included int he standard for possible use? **Accept in principle. NTRUEncrypt is not supported in mode 3.**

1111 (Roberts, T), 1112 (Shvodian, T) A**ccept in principle.** Sequence counters have been removed, time token has been replaced by the beacon number, and secure frame counter is included in every secure frame. Specifically, remove "seq_num_D" and "seq_num_SM" from clause 9.9.4, replace TimeToken with Beacon Number, and update text in the figures to reflect the changes.

215 (Gilb, TR) 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. The following sub-clause should be added to Clause 6. 6.x.x Security management primitives These primitives define how the MLME communicates security related events to the DME. 6.x.x.x MLME-SECURITY-ERROR.indication This primitive allows the MLME of any DEV to indicate a failed security processing operation to the DME. The semantics of the primitive are as follows: MLME-SECURITY-ERROR.indication(SrcID, DestID, SECID, ReasonCode) The primitive parameters are defined in Table xx. Table xx - MLME-SECURITY-ERROR.indication parameters Name & Type & Valid Range & Description \\ SrcIDInteger & 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 for which the frame was intended. \\ 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. \\ 6.x.x.x.x 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. 6.x.x.x.x Effect on receipt On receipt of this primitive, the DME is notified of a security error and the reason for the security error. **Accept in principle.** Add new sub-clause as indicated to clause 6. Remove all references to time token and the Bad-Time-Token reason code since time token is no longer sent in each frame. Modify text according to other comment resolutions. Add parameter to MLME-SECURITY-ERROR.indication which contains the contents of the offending frame.

214 (Gilb, TR) 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. Add the following parameter to the primtive descriptions for frames sent over the air. MLME-XXX.request (or .response)(KeySelection) with this entry in the corresponding tables. 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. \\ **Reject.** Devices in a secure piconet should not be able to arbitrarily send an unsecured frame. This also adds unnecessary complexity to the MLME interface and implementation of the MAC. It may be appropriate to allow streams to be established which do not use data protection when the data is protected by a higher level encryption protocol. Given time the committee may include such an option.

213 (Gilb, TR) 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. The interfaces for the above described MLME messages should add the following entries to the semantics description: MLME-XXX.indication (or .confirm)(SecurityUse, ACLEntry) The following table entries should be added to the above described MLME messages. 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. \\ **Accept in principle.** Instead of adding parameters to .indicate and .confirm MLMEs, we recommend that the MLME generate an error indication and return a copy of the frame to the DME so it can take appropriate action. The MLME shall not perform any further processing on the frame.

571 (Gilb, T) 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. Replacing the first paragraph 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. **Accept in principle.** Replace first paragraph of 9.4.1 with: "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."

572 (Gilb, T) 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. Replacing the first paragraph in 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. **Accept in principle.** Mode 1 will be removed and informative text will be added to the association protocol description to describe how a DME could implement the required functionality without any additional support from the MAC.

573 (Gilb, T) 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. Replacing the first paragraph in 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. **Accept in principle.** Replace first paragraph of 9.4.3 with: "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 in use for this relationship. The cryptographic operations performed for secure frames exchanged with a peer DEV shall be performed as specified by the security suite associated with that peer security relationship. While in this mode, if the MAC receives a frame with the SEC field in the frame control field set to a value different than expected as defined in {xref Table 48}, the MLME shall generate a MLME-SECURITY-ERROR.indication with the ReasonCode set to INVALID-SEC-VALUE." (indicate the exceptions from text in clause 7 in Table 48)

574 (Gilb, T) The description of security mode 3 is not descriptive enough and should refer to a DEV operating in the mode, not a piconet operating in the mode. Replacing the first paragraph in 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. **Accept in principle.** Replace first paragraph of 9.4.4 with: "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 cryptogra-

phy 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 in use for this relationship. The cryptographic operations performed for secure frames exchanged with a peer DEV shall be performed as specified by the security suite associated with that peer security relationship. While in this mode, if the MAC receives a frame with the SEC field in the frame control field set to a value different than expected as defined in {xref Table 48}, the MLME shall generate a MLME-SECURITY-ERROR.indication with the ReasonCode set to INVALID-SEC-VALUE." (indicate the exceptions from text in clause 7 in Table 48)

2.8 Wednesday, August 7, 2002

310 (Shvodian, T) Authentication response command needs a response value of "DEV not a security manager" in case a DEV tries to associate with another DEV who is not a security manager. Add a "DEV is not a security manager" response code. **Accept.**

864 (Shvodian, T) All of these states need to specify that the DEV ignores Beacon integrity. **Accept in principle.** On page 226, line 1, add the following sentence: "During the process of authentication, the DEV shall not perform integrity checking on the beacon."

856 (Shvodian, T) Add association to the list of commands that the SM handles in startup state. **Accept in principle.** Clause 9.9 needs to be updated to segregate the security manager functions into specialized state machines for each major function. A top level state machine should be defined to handle security manager event handling to direct received security related MLME events to the proper state machine. For Table 60, the only MLME events that will be directed to this state machine will be the authentication request, challenge response, or timeout events. Association requests will never be directed to this state machine. Action Item for Dan and Ari: Modify clause 9.9 to segregate security manager functions and update tables for each of the functions to reflect only the MLME events that will be directed to them. This also includes updates to the state diagram figures in 9.9.

59 (Heberling, TR) Deauthentication cannot "fail". Both PNC and client shall regard a deauthenticate request as being completed when requested and proceed with the deauthentication procedure. The PNC needs to get back the DevID from the confirm in case it has deauthenticated several DEVs. The reasonCode is not needed since the request cannot fail, and even if it did there is no recovery./KO MLME_DEAUTHENTICATE.confirm <change text in line 7> This primitive reports the completion of a deauthentication. <Change parameter to MLME_DEAUTHENTICATE.confirm> MLME_DEAUTHENTICATE.confirm (DevID) <Change text in 6.3.10.3.1> This primitive is sent by the MLME after sending a deauthentication request command to a DEV and completeing the deauthentication procedure. The primitive shall be sent even if the deauthenticated DEV does not ACK the command frame. **Accept in principle.** Delete the last two sentences in clause 6.3.10.3.1 and replace with: "The result code shall be set to SUCCESS if an ACK was received, and to ACK-TIMEOUT if indicated time period expires." Add parameter to MLME-DE-AUTHENTICATE.confirm for DevID. DevID is the destination of the MLME-DE-AUTHENTICATE.request command causing this confirm. Action item for Dan and Ari: Update 9.9.5.8 to include necessary updates to authentication state information in the MAC required as a result of completing a de-authentication process both in the originating DEV and the receiving DEV. E.G. 6.3.10.1.2 and 6.3.10.2.2 are inconsistent. One indicates that the MLME securely deletes all keying material and the other indicates that the DME does this. This should be done in by the DME via internal updates or by commands to the MLME to update any security information associated with the secure relationship.

334 (Heberling, TR) What is a deauthentication acknowledgement? /KO Replace with Imm-ACK, unless a real frame is intended but missing in the frame formats. In that case insert that frame into clause 7. **Accept in principle. Replace with Imm-ACK.** Delete De-authentication acknowledgement transition from Figure 165. Note on information common to MLME and DME: The operation of the security commands will

update information in the MLME and the DME. When the DME issues a De-Authentication or Disassociation for a DEV request, the MLME will securely remove the keying information associated with the security relationship with that DEV. When the DME issues a Distribute-Key request, the MLME will securely update the keying information associated with the securely relationship with that DEV with the new keying information in the Distribute-Key request. When a Request-Key confirm is received, the DME will assume that the MLME has securely updated its keying information. When the DME receives a Distribute-Key indication, the DME will assume that the MLME has securely updated its keying information for that command. There is a difference with the way key updates are handled from the PNC. They are considered new keys and the old keys from the PNC are automatically depreciated based on when a new SECID was detected in the beacon. The old keys are not deleted until after the ATP period expires. When the DME receives an Authentication response, it will assume that the MLME knows that it is authenticated with the sending DEV SM. Until the DME provides the MLME with the management keying information, the MLME cannot generate or process any secure frames in the piconet. The DME shall use the MLME-KEYUPDATE command to provide the MLME with the management keying information obtained as part of the authentication process. The information in the MAC PIB (as updated by recent comments) will remain, but the MLME does not need to reference it during normal operation.

434 (Gilb, TR) The integrity code needs a secure frame counter to operate correctly. Add a secure frame counter, 2 octets, to all secure frames at the beginning of the frame, right after the time token. Add the definition to 7.3, "The secure frame counter represents the number of times the slected key has been used during that superframe. The use of the secure frame counter in the encryption and integrity protocol is described in {xref}". **Accept in principle.** Secure frame counter added to all secure frames as in comment 433. Update description of SFC field to require initialization to 0 for first frame sent in any superframe. New text is: "The secure frame counter field shall be included in the frame body of all secure frames. The secure frame counter field contains a 2-octet counter that is used to ensure the uniqueness of the nonce in a secure frame. A DEV shall not reuse a frame counter with the same time token and key. The DEV shall initialize the secure frame counter to 0 for the first frame sent in a superframe and increment it each time a secure frame is sent."

871 (Shvodian, T) This is unclear. Should be replaced by an MSC. **Accept in principle.** Figure 160 will be updated. See comment note following resolution comment 856.

336 (Heberling, TR) Figure 163 shows PNC handover using PNC information and PNC handover information (renamed to PNC handover CTRB). Non of these contains Authentication state. Consequently the new PNC has no way of knowing if a DEV is only associated, authenticated or in progress of authenticating. /KO SEC group needs to clarify. Appropriate information elements needs to be added to PNC information, 7.5.4.2, or a new SEC handover command frame needs to be specified. Since the PNC information can be a response to a DEV inquiry, probably a new frame is the preferred alternative. **Accept in principle.** Add AUTHENTICATED as the third state allowed in the DEV association info field and use the probe command to send the DEV Association IE from the departing PNC to the new PNC. This is already part of the PNC handover process.

468 (Gilb, TR) The scheme in Annex B talks about a general elliptic curve, but 802.15.3 has chosen a specific one. Add an item here that defines the elliptic curve parameters, D, with a cross reference (xref 10.3.1.2). Also, use the nomenclature of Annex B.2 here (i.e. Hash, UID, VID, CAID, etc.) to better align the definitions with annex B. Probably reformat this as a table as well. **Reject.** The suggested usage does not exist in D10. Please review new ECMQV security suite specification which is consistent.

216 (Gilb, TR) Since the DME is able to choose the keys used for a command (or no keys), the .confirm commands need to add "UNAVAILABLE_KEY" to all of the result codes. Change all .confirm MLMEs that send frames as indicated. **Accept in principle.** See resolution of comment 215. The MLME-SECURITY-ERROR.indication will return UNAVAILABLE_KEY as an error and a copy of the offending frame.

459 (Gilb, TR) There is no pending key state in the diagram. Change "... to is the "pending key" state." to be "... to is the startup mode state or secure mode state." **Accept in principle.** See comment 856. Clause 9.9 will be updated to handle this situation.

438 (Gilb, TR) We don't need most of the IEs listed for security purposes. Unless it can be shown that these are needed to respond to a probe command, we can delete the following: Public key object 7.4.17 Time token 7.4.20 Integrity code 7.4.21 I think we still need these, but we should verify that they are needed, else delete them: Security suite OID 7.4.18 Security session ID 7.4.19. **Accept in principle.** The public key object, security suite OID, and security session OID are needed for the probe command. The time token and integrity code IEs will be removed.

302 (Shvodian, TR) This is not an IE. It never is transmitted in a Beacon. It should be a command field. Change this from an information element into a frame field and put it into a frame field sub-clause. **Reject.** This will be used in the probe command.

225 (Gilb, TR) 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.' **Reject.** Devices in a secure piconet should not be able to arbitrarily send an unsecured frame. This also adds unnecessary complexity to the MLME interface and implementation of the MAC. It may be appropriate to allow streams to be established which do not use data protection when the data is protected by a higher level encryption protocol. Given time the committee may include such an option.

220 (Gilb, T) There should be two SECIDs, one for the management key and one for the data key. Add 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. **Accept in principle.** Update Table 31 as well to include ManagementSECID and DataSECID in place of MACPIB_PNCSECID.

783 (Shvodian, TR) The disassociation command requires authentication if authentication is required. Put and X in the Authenticated column of the Disassociation request command. **Accept**.

869 (Shvodian, TR) these states need to show an entry and exit. some only have one or the other. Show the state entry and exit. **Accept in principle.** Clause 9.9 is being updated and Figure 159 will be modified to have the required entry and exits.

805 (Shvodian, TR) There are many places in the draft that refer to things that an associated DEV can do. Unfortunately, with security turned on, many of these really require authentication. One solution would be to to say "associated or authenticated if required". the preferred way would be to have DEVs in mode 0 and 1 automatically authenticated in modes 0 and 1. Add text that associated DEVs are automatically authenticated in modes 0 and 1, and throughout the draft use authenticated instead of associated as appropriate. **Accept in principle.** Change appropriate text in draft from just "associated" to "associated and authenticated if required" when authentication is required when security is enabled.

570 (Gilb, T) Need some more descriptive text for 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. **Accept.**

431 (Gilb, TR) Need to identify which commands are sent with security under mode 2 and mode 3 scenarios.For example, in a secure relationship with the PNC, the disassociate command shall only be accepted if it is sent as a secure command frame. The probe command, however, may be responded to by the DEV. We need a list of all of the commands, like the table in clause 7 with 4 columns listing what to do with the

frames, 1) TX allowed when SM=PNC, 2) RX action when SM=PNC, 3) TX allowed when SM=DEV and 4) RX actio when SM=DEV. It is possible, in theory, to add these columns to the table in clause 7, but the table would be too large. **Accept in principle.** Change the text following Table 48 from: "Unless otherwise stated in the command descriptions, in all commands, the SEC bit shall be set to 0 when the piconet is operating in security modes 0 or 1 and shall be set to 1 when the piconet is operating in security modes 2 or 3. Also, the ACK request field shall be set to either Imm-ACK or implied-ACK for all commands unless otherwise stated in the command description." to "In all commands, the SEC bit shall be set to 0 when the piconet is operating in security mode 0 or 1 and shall be set to 1 when the piconet is operating in security modes 2 or 3 and the DEV must be authenticated if required in order to send that command. Also, the ACK request field shall be set to either Imm-ACK or implied-ACK for all commands unless otherwise stated in the command description."

Update to resolution of comment 936. Remove the X in the Authenticated (if required) column for the Probe command in Table 48.

303 (Shvodian, TR) This is not an IE. It is never sent in a beacon and there is no need to have type and length. Change this from an information element into a frame field and put it into a frame field sub-clause. **Reject.** This needs to be an information element for the Probe command.

443 (Gilb, TR) The OID field is variable and is potentially very long. Change every instance of OID in clause 7 (and where referenced in clause 8) to be OID encoding, a 1 octet field that maps approved OIDs to an octet value. Add to the OID table in clause 9 a column that provides OID mappings for the security suites, with 0x00 as the first suite, 0x01 as the second, etc. **Reject.** The OID is of manageable length and limiting the implementation to the known OIDs at the time the standard is written may prevent reasonable upgrades in the future.

442 (Gilb, TR) The security suite OID only supports reporting on OID type. Change the security suite OID IE to be able to report multiple OIDs or provide a mechanism by which a DEV responds to a probe with muliple OID IEs if if supports multiple security suites. Need to make sure that any time a DEV needs this information it gets the list instead of simply a single OID. This may impact the association response command as well. **Accept in principle.** The text on page 126, lines 1-3 already allows multiple OIDs to be returned in response to a probe command. However, it is up to the DEV to determine whether multiple OIDs are reported. The Association response only returns the preferred security suite OID. A DEV can use the probe command to determine if additional security suites are supported.

562 (Gilb, TR) It appears that if the length of the OID is variable, it may not be possible to unambiguously parse the association response command. Add the length of the OID before the OID to make this unambiguous. **Accept in principle.** Change Table 9. "PiconetSecurityOID" becomes "PiconetSecurityOIDIE". Next column is "As defined in 7.4.18"

441 (Gilb, TR) The OID in this command is unnecessary. In any event, we should use the mapping of authentication types in 7.5.2.1 instead of the entire OID. Delete the OID and its length from this command. If the identifier of the security relationship is required, put in the public key type field from 7.5.2.1 with an xref to where it is defined. Probably we don't need to send anything here. **Accept in principle.** Change the list of public-key object types on page 132, lines 5-10 to be ")->NULL, 1->Raw key, 2->X.509 Certificate, 3->Implicit Certificate, 4-255 -> reserved. Add an OID length and OID field to the authentication request command format in Figure 52 following Dev address. Change text on page 132, line 2 from "the current security suite" to "the security suite defined by the OID". Add text to page 133, line 4: "The symmetric algorithms to be used are as specified in the security manager's OID." In clause 7.4.17 on page 125, line 24, figure 41, change PublickeyObjectType to length 1 octet. Move the definition of the public-key object types from 7.5.2.1 to 7.4.17 replacing the reference to clause 10. Add reference to definitions in 7.4.17 in clause 7.5.2.1.

850 (Shvodian, T) Are the sequence counters and secure frame counters reset to zero every superframe or do they keep incrementing till they roll over? Clarify if these are reset every superframe or if they roll over. **Accept in principle.** See comments 433 and 434.

564 (Gilb, TR) The sequence number for the management keys was originally created to remove the need for devices to rely on the security of the group key and time token to provide freshness on management frames. However, since the techniques require that devices securely maintain a strictly increasing time token and since the devices cannot communicate without having a functioning beacon with an increasing time token, the sequence numbers are redundant and consume excess space. The sequence number should be removed from all of these commands. **Accept in principle.** All occurrences of "Sequence Number" used for freshness throughout the draft shall be removed. No longer required.

942 (Shvodian, TR) Do we really need a separate sequence number counter for mangement frames and one for data frames? Management frames should be relatively rare compared to data frames. Why don't we just have a single frame counter. Use a single frame sequence counter regardless of frame type (data, command, beacon). **Accept in principle.** All occurrences of "Sequence Number" used for freshness throughout the draft shall be removed. No longer required.

889 (Shvodian, T) Does the sequence nubmer increment for retransmission? Can it? Specify if the sequence number may or shall increment for retransmissions. **Accept in principle.** All occurrences of "Sequence Number" used for freshness throughout the draft shall be removed. No longer required.

631 (Gilb, T) The word "can" is used when it should be "may". Change "can" to "may". **Accept.**

855 (Shvodian, TR) PNC/SM should ignore all commands in startup state, not just security related commands. Change to: The security manager has not yet sent keys Security manager ignores all commands from the DEV except the following: **Accept in principle.** See comment 856.

867 (Shvodian, TR) Does the SM send new key to all DEVs, then update SECID in beacon and start using the new key? Need to explicitly show when the PNC/SM starts using the new key. **Accept in principle.** See comment 870.

874 (Shvodian, TR) Need to explain why SM rejects all commands while checking a message instead of queuing them. **Accept in principle.** See comment 856.

877 (Shvodian, TR) Need to explain why the security manager "may" send the desired OID, and not "shall". Explain why this is a may and not a shall or change to a shall. **Accept in principle.** Change line 23 on page 255 "may" to "shall" and update section for editorial clarity.

576 (Gilb, TR) The secure frame counter has not been established yet when the authentication process begins. 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. **Accept in principle.** Add the following sentence at the end of the challenge and authentication response entries: "The secure frame counter used in the CCM nonce shall be the 2-octet string 0x0000."

467 (Gilb, T) Broken xref. Add a bibilography cross reference here the PKIX-X509 document and add the corresponding bibligraphy entry. **Accept.**

2.9 Thursday, August 8, 2002

Update to 931 made.

566 (Gilb, TR) Need to have a desrciption of how to do the secure frame generation. Add the following subclause to 9.3 9.3.3 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, then 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, then 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 MLME-xxx.request command has an associated MLME-xxx.confirm, then the MLME shall also set the reason code for the .confirm to be UNAVAILABLE-KEY. If the DEV is able to obtain the appropriate security suite and key from the MAC PIB, the DEV shall use the current time token in the frame. 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. However, the DEV shall set the retry field in the frame control field of the MAC header to be 0 only for the purposes of the integrity calculation. This operation is done in order to allow a device to retransmit a frame without recomputing the integrity code. 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. **Accept in principle.**

Add the following sub clause to 9.3

9.3.3 Secure frame generation

"When a DEV wishes to send a secure frame, it shall use the keying material required for the type of frame and by the relationship between the sending DEV and the receiving DEV. For each relationship, there are two keys used to protect secure frames: a management key and a data key. All commands sent to the PNC shall use the PNC-DEV management key agreed on with the PNC during the authentication process. All commands sent to a device other than the PNC shall use the peer-to-peer management key associated with the peer-to-peer relationship with that DEV or the piconet-wide group data key if no peer-to-peer relationship exists. All data frames sent to a DEV shall use the peer-to-peer data protection key associated with the peer-to-peer relationship with that DEV or the piconet-wide group data key if no peer-to-peer relationship exists. All broadcast data frames shall use the piconet-wide group data key. {xref Table nn-Key selection for secure frames} provides a listing of which keys are to be used for protecting secure frames. 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 MLME-xxx.request command has an associated MLMExxx.confirm, then the MLME shall also set the reason code for the .confirm to be UNAVAILABLE-KEY.

If the DEV is able to obtain the appropriate keying material, the DEV shall use the current beacon counter and secure frame counter for the corresponding SECID to construct the CCM nonce used to protect the secure frame {xref Figure kk-CCM nonce format}. The SECID included in the frame shall be the value corresponding to the keying material being used. The integrity code shall be computed on the entire frame up to the integrity code itself including the MAC header. However, the DEV shall set the retry field in the frame control field of the MAC header to be 0 only for the purposes of the integrity calculation. This operation is done in order to allow a device to retransmit a frame without recomputing the integrity code. 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. The device shall then compute the FCS over the modified frame."

(modified by e-mail on 8/13 to) "When a DEV wishes to send a secure frame, it shall use the keying material required for the type of frame and by the relationship between the sending DEV and the receiving DEV. For each relationship, there are two keys used to protect secure frames: a management key and a data key. All commands sent to the PNC shall use the PNC-DEV management key agreed on with the PNC during the authentication process. All commands sent to a device other than the PNC shall use the peer-to-peer management key associated with the peer-to-peer relationship with that DEV or the piconet-wide group data key if no peer-to-peer relationship exists. All data frames sent to a DEV shall use the peer-to-peer data protection key associated with the peer-to-peer relationship with that DEV or the piconet-wide group data key if no peer-to-peer relationship exists. All broadcast data frames shall use the piconet-wide group data key. {xref Table nn-Key selection for secure frames} provides a listing of which keys are to be used for protecting secure frames. 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 MLME-xxx.request command has an associated MLMExxx.confirm, then the MLME shall also set the reason code for the .confirm to be UNAVAILABLE-KEY.

If the DEV is able to obtain the appropriate keying material, the DEV shall use the current beacon counter and secure frame counter for the corresponding SECID to construct the CCM nonce used to protect the secure frame {xref Figure kk-CCM nonce format}. The SECID included in the frame shall be the value corresponding to the keying material 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. The device shall then compute the FCS over the modified frame."

567 (Gilb, TR) Need to describe how to receive an incoming secure frame. Add the following section to the end of 9.3 9.3.4 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 pay-

load field has been modified, the DEV shall check the FCS. The DEV shall also check that the retry field in the frame control field of the MAC header is set to 0 and, if not, set it to 0. This operation is done in order to allow a device to retransmit a frame without recomputing the integrity code. 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. **Accept in principle.**

Add the following section to the end of 9.3

9.3.4 Secure frame reception

"When a device receives a secure beacon frame, the DEV shall determine if the received beacon number is greater than the CurrentBeaconNumber and less than the CurrentBeaconNumber + 6,553 {Please determine if this is the right number and how it should be represented, or even use at all.}. If not, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to BAD-BEACON-NUMBER and shall not perform any additional operations on the received beacon.

When a DEV receives a secure non-beacon frame or a secure beacon frame with a valid beacon number, it shall use the appropriate keying material depending on the type of frame, SECID and source address found in the frame. If the SECID in the frame does not correspond to known keying material in the receiving DEV, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the Reason-Code set to UNAVAILABLE-KEY and shall not perform any additional operations on the received frame.

If there are no previous security errors in the processing of the frame, 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 retry field in the frame control field of the MAC header is set to 0 and, if not, set it to 0. This operation is done in order to allow a device to retransmit a frame without recomputing the integrity code. The decryption operation shall be applied only to the integrity code, keys 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 replace the encrypted data in the received frame. 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."

(modified by e-mail on 8/13 to) "When a device receives a secure beacon frame, the DEV shall determine if the received beacon number is greater than the CurrentBeaconNumber and less than the CurrentBeaconNumber + 6,553 {Please determine if this is the right number and how it should be represented, or even use at all.}. If not, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to BAD-BEACON-NUMBER and shall not perform any additional operations on the received beacon. When a DEV receives a secure non-beacon frame or a secure beacon frame with a valid beacon number, it shall use the appropriate keying material depending on the type of frame, SECID and source address found in the frame. If the SECID in the frame does not correspond to known keying material in the receiving DEV, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the Reason-Code set to UNAVAILABLE-KEY and shall not perform any additional operations on the received frame.

If there are no previous security errors in the processing of the frame, 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 decryption operation shall be applied only to the integrity code, keys 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 replace the encrypted data in the received frame. 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."

Update resolution to 569.

868 (Shvodian, T) What is the purpose of the distribute Key response command? What does the PNC do if it fails? Try again? Disassociate the DEV? If the frame passed CRC the PNC would get an ACK and the key should be received correctly. Add text explaining the purpose of the distribute key response command. **Accept in principle.** Update 6.3.9.3.1 to be "This primitive is generated by the DME as a result of the receipt of an MLME-DISTRIBUTE-KEY.indication command from a peer DEV. It shall not be generated by the DME as a result of the receipt of an MLME-DISTRIBUTE-KEY.indcation command from the PNC."

388 (Heberling, TR) Please make these changes to the secure beacon frame format: MAC header|HCS|[SECID(fixedLnth)|FrameCounter(fixedLnth)]|... ...PiconetSynchParm(permanentfield)|... ...CTA-IEs(variableLnth)|PiconetBSID-IE(variableLnth)|... ...Other IEs(as needed)|Integrity code-IE| [] means optional fields. Please note that the TimeToken field has been removed as a seperate info element and can be subsumed by the Beacon count subfield in the PiconetSynchParm field. Again the rationale for placing the variable length fields after the fixed length fields is that it makes parsing the CTA-IEs more efficient. **Accept in principle.** Frame counter is not needed. Update 7.3.1.2, page 109, line 5 with the following fields: HCS+MAC header (12 octets)|SECID (2 octets)|Other IEs (as needed)|Integrity code (8 octets)|FCS.

781 (Shvodian, TR) What does the Integrity code protect? Only the IEs or the SECID and secure sequence number, too? Clarify what the integrity code protects. The most important header fields are part of the nonce and thus already protected. **Suggest accept in principle. Figure 154 and Table 82 specify how to protect the beacon. Recommend referencing one of these in 7.3.1.2. Recommend that the SECID and secure frame counter not be protected by the integrity. Recommend also adding the following tables and text to clause 10.2.5 and, if desired, separating the entries of table 82 and interspersing these tables to help clarify:**

(Add to the end of 10.2.4.5) Figure 2 specifies the format of the nonce that is input to the CCM algorithm. The source DEVID, destination DEVID, secure frame counter and fragmentation control field shall be included in the frame that is being protected. The beacon counter shall be the beacon counter from the beacon for this superframe.

3	**2**	**6**	**1**	**octets: 1**
Fragmentation control field	Secure frame counter	Beacon counter	Destination DEVID	Source DEVID

Figure 2—CCM nonce format

(Add the following figures and text after table 82) Figure 3 specifies the length information and data input to the CCM operation for secure beacons. The auth data length *l(a)* shall be set to the length of all of the protected data and the enc data length *l(m)* shall be set to 0. The data input to CCM shall be taken in the order it is received in the frame, omitting the HCS, FCS and integrity code.

Enc Data Length *l(m)*	**Auth Data Length *l(a)***
0	$14+L_1+...+L_{n-1}$

L_{n-1}	**...**	**L_1**	**2**	**2**	**Octets: 10**
Information element-(n-1)	...	Information element-1	Secure frame counter	SECID	Frame header

Figure 3—CCM input for secure beacons

Figure 4 specifies the length information and data input to the CCM operation for secure commands. For all commands except for the request key response command and distribute key request command, the auth data length *l(a)* shall be set to the length of all of the protected data and the length of encrypted data *l(m)* shall be set to 0. For the request key response command and distribute key request command, the auth data length *l(a)* shall be set to the length of all of the protected data minus 16 (the length of the key) and the enc data length shall be set to 16 (the length of the key). The data input to CCM shall be taken in the order it is received in the frame, omitting the HCS, FCS and integrity code.

Enc Data Length *l(m)*	**Auth Data Length *l(a)***
L_2	$18+L_1$

L_2	**L_1**	**2**	**2**	**2**	**2**	**Octets: 10**
Enc data	Auth data	Length $(=4+L_1+L_2)$	Command type	Secure frame counter	SECID	Frame header

Figure 4—CCM input for secure commands

Figure 5 specifies the length information and data input to the CCM operation for secure data frames. The auth data length *l(a)* shall be set to 14 and the length of encrypted data *l(m)* shall be set to the length of the data payload. The data input to CCM shall be taken in the order it is received in the frame, omitting the HCS, FCS and integrity code

Enc Data Length *l(m)*	**Auth Data Length *l(a)***
L_1	14

L_1	**2**	**2**	**Octets: 10**
Pre-encrypted data	Secure frame counter	SECID	Frame header

Figure 5—CCM input for secure data frames

873 (Shvodian, TR) It is not clear why the DEV would reject all commands while checking a message. Why wouldn't they be queued? Need to explain why commands are rejected. **Accept in principle.** See resolution for comment 856. The new diagrams will show queuing of commands where appropriate.

291 (Shvodian, TR) Need to show what the integrity code protects. Does it include SECID and sequence counter? **Accept in principle.** See comment 781.

935 (Shvodian, TR) I have been told that everything in the frame but the FCS is covered by the integrity check. There are some problems with this: HCS is not known during encryption so it cannot be part of integrity check. I recommended dropping HCS from the MAC andyway and keeping it in the PHY. A security wrapper is required to pad to a multiple of 16 octets. The calculation for this would have to include MAC overhead. Most of the important fields are protected by the nonce (SrcID, DestID, Fragmentation field, If possible, I think it is better if the integrity code does not cover the header. If it needs to, the covered fields need to made clear. HCS cannot be covered since it is generated at the PHY. **Accept in principle.** See comment 781 regarding what is covered and comment 769.

493 (Gilb, TR) The IC needs to be recalculated if the frame is re-tried. Declare the retry bit to be a mutable field, i.e. that before calculating the IC, set this bit to a known value, say one. This is both for transmission and reception. **Accept.** See comments 566 and 567.

429 (Gilb, TR) The security group 6.5.5 has way too many things in it that don't belong there because they change too rapidly or are not really management items. Delete the following items from the security group: MACPIB_PNCSECID MACPIB_SMSeqNum MACPIB_DEVSeqNum MACPIB_CurrentTimeToken MACPIB_ValidBeacon MACPIB_NewPNC Rename as follows: MACPIB_SecuritySuite - MACPIB_PiconetSecuritySuite. **Accept in principle.** Remove the following entries from Table 31: MACPIB_SecuritySuite, MACPIB_PNCPublicKeyInfo, MACPIB_SMSeqNum, MACPIB_DEVSeqNum, MACPIB_ValidBeacon, MACPIB_NewPNC. Remove the following entries from Table 32: MACPIB_SecuritySuite and MACPIB_PublicKeyInfo. Add the following entry to Table 31: MACPIB_ManagementSECID - 2 - The SECID for the keys agreed upon during authentication that are used for protecting commands. - Dynamic.

Add the following entries to Table 32: MACPIB_ManagementSECID - 2 - The SECID for the keys agreed upon during authentication that are used for protecting commands. - Dynamic, MACPIB_ManagementKeyInfo {duplication of entry in Table 31}, and MACPIB_DataKeyInfo {duplication of entry in Table 31}. Update all SECID entries to be of length 2 octets instead of 8 octets.

852 (Shvodian, T) Does SM check ACL after getting association request? Need a figure showing SM checking ACL after association. **Accept in principle.**

Mode 1 shall be removed from the draft. There already is a diagram showing the PNC receiving and responding to an association request. The following changes will be made to clarify how simple ACL functionality can be implemented with the current draft.

Change the last sentence on pg. 160 and first on pg. 161 in 8.3.1 from "The PNC needs some time to make sure that there are enough resources available to support another DEV on the piconet and to allocate a DEVID. After a decision is made regarding the association and the DEVID, the PNC sends an association response command to indicate the acceptance or rejection of the association." to the following text:

"The PNC needs some time to ensure that the device should be allowed in the piconet, to ensure that there are enough resources available to support another DEV on the piconet and to allocate a DEVID. The PNC may maintain an access control list (ACL) of 48-bit DEV addresses that shall be allowed to join the piconet. If the ACL is in use, when the PNC receives an association request command, the PNC shall consult the ACL to determine if the DEVID in the request is included in the ACL. If the DEV address is not in the ACL, the PNC shall send an association response command with the reason code set to 'Association denied', {xref - 7.5.1.2}, indicating that the device is not associated due it not being on the ACL. If the PNC determines that there are not enough resources available to support the new DEV, the PNC shall send an association response command with the reason code set to the appropriate value in {xref - 7.5.1.2}. If the PNC determines that the DEV shall be associated, the PNC shall send an association response command with the reason code set to 'Success', {xref - 7.5.1.2}."

Add the following entry to the reason code list in 7.5.1.2, pg. 130, line 40:

- 8 -> Association denied
- 9-255 -> reserved.

All references to mode 1 as the ACL mode, shall be removed from the draft and mode 2 shall become mode 1 and mode 3 shall become mode 2.