IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)	
Title	**TG3 LB19 security comment resolution**	
Date Submitted	[11 September, 2002]	
Source	[John R. Barr] [Motorola] [1303 E. Algonquin Road Schaumburg, IL 60196]	Voice: [847-576-8706] Fax: [847-576-6758] E-mail: [John.Barr@Motorola.com]
Re:	[802.15.3 D11]	
Abstract	[This document is a record of security comment resolutions for LB19.]	
Purpose	[To provide a record of the security comment resolution for LB19.]	
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. Security Comment Resolution, Monterey

1.1 Tuesday, September 10, 2002

404 - ACCEPT IN PRINCIPLE. Add "The DEV shall set the secure frame counter to 0 whenever it receives a new key." to the end of clause 7.2.8.2.

110 - ACCEPT

5 - ACCEPT IN PRINCIPLE. Change "it shall verify that the beacon number is greater than the MACPIB_CurrentBeaconNumber, that the SECID matches the MACPIB_PNCSECID stored in the MAC PIB and that the integrity code passes. If all of these checks succeed, the DEV shall set the MACPIB_CurrentBeaconNumber to the received beacon number value and set the MACPIB_ValidBeacon to valid. If the beacon number is greater than the MACPIB_CurrentBeaconNumber, but the SECID does not

match the MACPIB_PNCSECID, the device may set the MACPIB_CurrentBeaconNumber to the value in the beacon and send a key request command to the PNC to obtain the new key."

to

"it shall verify that the beacon number in the beacon is greater than the LastKnownGoodBeaconNumber, that the SECID matches the MACPIB_PNCSECID and the integrity code passes. If all of these checks succeed, accept the beacon number in the beacon as the LastKnownGoodBeaconNumber. If the beacon number in the beacn is greater than the LastKnownGoodBeaconNumber, but the SECID does not match the MACPIB_PNCSECID, the device may set the LastKnownGoodBeaconNumber to the value in the beacon and send a key request command to the PNC to obtain the new key."

Delete "stored in the MACPIB_CurrentBeaconNumber in the MAC PIB" from line 16 on page 221.

On page 220, line 41, Change "greater than the CurrentBeaconNumber and less than the CurrentBeaconNumber + aMaxBeaconChange." to "greater than the LastKnownGoodBeaconNumber and less than the LastKnownGoodBeaconNumber + aMaxBeaconChange."

6 - ACCEPT IN PRINCIPLE. Move the definition of public-key object type from 7.5.2.1 to 7.4.15. Replace line 16 on page 128 with lines 1-11 on page 134. Replace lines 1-11 on page 134 with "The public-key object type field specifies the type of public key specified in the public-key object {xref 7.4.15}."

403 - REJECT. To maintain proper synchronization of keying material, the SECID is required. It is the only way a DEV can determine that it is out of sync.

113 - ACCEPT

99 - ACCEPT IN PRINCIPLE. See resolution of CID 6 which did this.

114 - ACCEPT IN PRINCIPLE. On line 30 change "and security manager" to "and security manager of the piconet ". On line 31 change "security manager acts as the central security point for all DEVs to obtain keying material for the piconet." to "piconet security manager authenticates DEVs for membership in the piconet and provides the broadcast payload protection key for the piconet." On line 37, change "all piconet data." to "data using the broadcast key.".

78 - ACCEPT

82 - REJECT. The PublicKeyObjectLength for ECC and RSA certificates can vary. Table 10 on page 43 incorrectly states that PublicKeyObjectLength is defined by the security suite. Change "Defined by the security suite, Clause 10." to "May be constant or variable as defined by the security suite, Clause 10."

83 - ACCEPT IN PRINCIPLE. Remove OID and OIDLength from 6.3.7.5 and 6.3.7.6. And update Figure 146 in 9.8.3 to reflect this change.

79 - ACCEPT

306 - ACCEPT

402 - ACCEPT

371 - ACCEPT IN PRINCIPLE. Change Pub_D to Pub_key_D. Change Pr_D to Pr_key_D. Change Pub_SM to Pub_key_SM. Change Pr_SM to Pr_key_SM. Change Keys_D to Sym_keys_D. Change Keys_G to Sym_keys_G. Change BH to SBH and add SCH for secure command header. Beacon and com-

mand shouldn't be lumped together. Add CD for command Data to separate it from BD. Use these identifiers as a guideline and update tables, text and figures in clause 9 as required.

432 - ACCEPT

107 - ACCEPT IN PRINCIPLE. Reference changed to clause where correction is to be made. Add BADBEACON-NUMBER to Table 14, page 54, line 49 since it is referenced in clause 9.2.8 on page 220, line 33.

382 - ACCEPT

241 - ACCEPT IN PRINCIPLE. Change "failure" on line 45 to "ChallengeResponse generation failure".

239 - ACCEPT IN PRINCIPLE. Change "Failure" to "Challenge verification failure".

86 - ACCEPT IN PRINCIPLE. The EncryptedSeed should be changed to Key and the IntegrityCode should be removed from the MLME-REQUEST-KEY.response. Change "with an encrypted version of therequested seed" to "with the requested key" in line 4.

90 - ACCEPT

20 - ACCEPT IN PRINCIPLE. Change "EncryptionSeed" on line 32 to "Key". Delete "in an encrypted format" from line 26.

89 - ACCEPT

88 - ACCEPT

87 - ACCEPT

1.2 Thursday September 12, 2002